# Plaquette 4 – Anneaux : inversibles, diviseurs de zéro, nilpotents

## Structures algébriques — Prépa MPSI / MP2I (1re année)

Corrections détaillées

**Boîte à outils**

**Anneaux et sous-anneaux.**

— $(A, +, \times)$ est un **anneau** : $(A, +)$ groupe abélien, $\times$ associative, distributive sur $+$, avec un neutre $1_A$.

— **Sous-anneau** : $B \subset A$ avec

$$1_A \in B \quad \text{et} \quad \forall x, y \in B,\ x - y \in B \text{ et } xy \in B$$

— **Binôme** : si $ab = ba$, $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ et $a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}$.

— **Inversibles** : $A^\times$ est un **groupe** pour $\times$, avec $(ab)^{-1} = b^{-1}a^{-1}$.

— **Diviseur de zéro** : $a \neq 0$ tel qu'il existe $b \neq 0$ avec $ab = 0$ ou $ba = 0$. Un inversible n'en est jamais un. **Intègre** : commutatif, non nul, sans diviseur de zéro.

— **Nilpotent** : $a^n = 0$ pour un $n \geq 1$ ; alors $1 - a$ est inversible,

$$(1-a)^{-1} = 1 + a + \ldots + a^{n-1}$$

— **Idempotent** : $e^2 = e$.

— **Morphisme d'anneaux** : $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$ et $f(1_A) = 1_B$.

— **Corps** : anneau commutatif non nul où tout élément non nul est inversible. Un anneau intègre **fini** est un corps.

## Correction de l'exercice 1 – Reconnaître un sous-anneau

On applique la caractérisation, **sans oublier l'unité** :

$$1_A \in B \quad \text{et} \quad \forall x, y \in B,\ x - y \in B,\ xy \in B$$

— **a)** Stable par différence et produit, mais $1 \notin 2\mathbb{Z}$ : **non**.

— **b)** $1 = \frac{1}{10^0}$ ; $\frac{k}{10^n} - \frac{k'}{10^m} = \frac{k10^m - k'10^n}{10^{n+m}}$ et $\frac{k}{10^n} \times \frac{k'}{10^m} = \frac{kk'}{10^{n+m}}$ : **oui**.

— **c)** $1 \in \mathbb{Z}[\mathrm{i}]$, la différence est évidente et $(a + \mathrm{i}b)(c + \mathrm{i}d) = (ac - bd) + \mathrm{i}(ad + bc)$ : **oui** (anneau des **entiers de Gauss**).

— **d)** Stable, mais l'unité de $F(\mathbb{R}, \mathbb{R})$ est la fonction constante 1, qui ne s'annule pas en 0 : **non**.

— **e)** La constante 1 est continue, et différences et produits de fonctions continues le sont : **oui**.

— **f)** Stable par différence, mais pas par produit : $\sqrt[3]{2} \times \sqrt[3]{2} = \sqrt[3]{4}$. Si l'on avait $\sqrt[3]{4} = a + b\sqrt[3]{2}$ avec $a, b \in \mathbb{Q}$, en multipliant par $\sqrt[3]{2}$ :

$$2 = a\sqrt[3]{2} + b\sqrt[3]{4} = ab + \left(a + b^2\right)\sqrt[3]{2}$$

Comme $\sqrt[3]{2} \notin \mathbb{Q}$, on aurait $a + b^2 = 0$ et $ab = 2$, donc $-b^3 = 2$ : $b = -\sqrt[3]{2}$ serait rationnel. Absurde : **non**.

**Piège** : en a) et d), la partie est stable par toutes les opérations, et ce n'est pourtant pas un sous-anneau — c'est l'unité qui manque.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

**Réponse.** Sous-anneaux : b), c), e). Non : a) et d) (pas d'unité), f) (non stable par produit).

## Correction de l'exercice 2 – Calculer dans un anneau non commutatif

**a)** $AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = B$ et $BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

— $A + B = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ et $(A+B)^2 = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$.

— $A^2 + 2AB + B^2 = A + 2B + 0 = \begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix}$.

Les deux diffèrent : l'identité remarquable est **fausse** ici.

**b)** Par distributivité, sans jamais permuter les facteurs :

$$(a+b)^2 = a^2 + ab + ba + b^2$$

— on retrouve $a^2 + 2ab + b^2$ si et seulement si $ab + ba = 2ab$, soit $ba = ab$. Il faut que $a$ et $b$ **commutent**.

**c)** $N^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ et $N^3 = 0$. $I_3$ commute avec toute matrice, donc le binôme s'applique, et les termes d'indice $k \geq 3$ sont nuls :

$$(I_3 + N)^n = I_3 + nN + \binom{n}{2} N^2 = \begin{pmatrix} 1 & n & \frac{n(n-1)}{2} \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$$

— Pour $n = 10$ : $\binom{10}{2} = 45$, d'où la matrice de première ligne $(1, 10, 45)$, de deuxième ligne $(0, 1, 10)$, de troisième ligne $(0, 0, 1)$.

— Contrôle pour $n = 2$ : $(I_3+N)^2 = I_3 + 2N + N^2$, première ligne $(1, 2, 1)$, et $\frac{2 \times 1}{2} = 1$ ✓.

**Réponse.** $AB = B$, $BA = 0$, $(A+B)^2 \neq A^2 + 2AB + B^2$ ; il faut $ab = ba$ ; $(I_3+N)^{10}$ a pour lignes $(1, 10, 45)$, $(0, 1, 10)$, $(0, 0, 1)$.

## Correction de l'exercice 3 – Diviseurs de zéro

**a)** Si $a$ est inversible et $ab = 0$, on multiplie à gauche par $a^{-1}$ : $b = a^{-1}ab = 0$. De même $ba = 0 \Rightarrow b = 0$.

**b)** $f = 1_{\mathbb{R}_+}$ et $g = 1_{\mathbb{R}_-^*}$ ne sont pas nulles, mais en tout point l'une des deux vaut 0 : $fg = 0$. L'anneau $F(\mathbb{R}, \mathbb{R})$ n'est pas intègre.

**c)** Le calcul donne $A\hat{A} = \begin{pmatrix} 4-4 & -2+2 \\ 8-8 & -4+4 \end{pmatrix} = 0$. En général, pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et sa comatrice transposée $\hat{M} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ :

$$M\hat{M} = \hat{M}M = (ad - bc)\, I_2 = \det(M)\, I_2$$

— si $\det M \neq 0$, $M$ est inversible d'inverse $\frac{1}{\det M}\hat{M}$ ;

— si $\det M = 0$ et $M \neq 0$, alors $\hat{M} \neq 0$ (mêmes coefficients au signe et à la place près) et $M\hat{M} = 0$ : $M$ est diviseur de zéro.

**d)** Soit $\overline{k} \neq \overline{0}$ et $d = k \wedge n$. Si $d = 1$, $\overline{k}$ est inversible (Bézout). Si $d > 1$, on pose $m = \frac{n}{d}$, avec $0 < m < n$, donc $\overline{m} \neq \overline{0}$, et

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— $km = \frac{k}{d}n \equiv 0 \pmod{n}$ : $\overline{k}\overline{m} = \overline{0}$.

Pour $\overline{8}$ dans $\mathbb{Z}/12\mathbb{Z}$ : $d = 4$, $m = 3$ et $8 \times 3 = 24 \equiv 0$ ✓.

**Attention** : cette dichotomie n'est pas générale ; dans $\mathbb{Z}$, 2 n'est ni inversible ni diviseur de zéro.

**Réponse.** Inversible ⇒ non diviseur de zéro ; $1_{\mathbb{R}_+}1_{\mathbb{R}^*_-} = 0$ ; $A\hat{A} = 0$ ; dans $M_2(\mathbb{R})$ et $\mathbb{Z}/n\mathbb{Z}$, non nul = inversible ou diviseur de zéro ; $\overline{8} \times \overline{3} = \overline{0}$.

## Correction de l'exercice 4 – Éléments nilpotents

**a)** 1 et $a$ commutent, donc la factorisation de $1 - a^n$ s'applique :

$$(1-a)\left(1 + a + \ldots + a^{n-1}\right) = 1 - a^n = 1$$

— et de même dans l'autre ordre : $(1-a)^{-1} = 1 + a + \ldots + a^{n-1}$ (analogue de la série géométrique, qui s'arrête ici).

**b)** Soit $a^n = 0$ et $b^m = 0$. Comme $ab = ba$, on développe $(a+b)^{n+m-1} = \sum \binom{n+m-1}{k} a^k b^{n+m-1-k}$. Dans chaque terme, soit $k \geq n$ et $a^k = 0$, soit $k \leq n-1$ et alors $n + m - 1 - k \geq m$, donc $b^{n+m-1-k} = 0$. Tous les termes sont nuls.

**c)** $E_{12}^2 = E_{21}^2 = 0$, mais $E_{12} + E_{21} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ a pour carré $I_2$ : ses puissances valent $I_2$ ou elle-même, jamais 0.

**d)** Dans $\mathbb{Z}/8\mathbb{Z}$ : $8 \mid x^k \Leftrightarrow 2 \mid x$ ($8 = 2^3$). Les nilpotents sont $\overline{0}, \overline{2}, \overline{4}, \overline{6}$.

— Dans $\mathbb{Z}/12\mathbb{Z}$ : $12 = 2^2 \times 3$ divise une puissance de $x$ si et seulement si $2 \mid x$ et $3 \mid x$, soit $6 \mid x$ : nilpotents $\overline{0}$ et $\overline{6}$ ($6^2 = 36 \equiv 0$).

**e)** $\overline{3} = \overline{1} - a$ avec $a = -\overline{2}$, nilpotent ($a^3 = -\overline{8} = \overline{0}$). Donc

— $\overline{3}^{-1} = \overline{1} + a + a^2 = \overline{1} - \overline{2} + \overline{4} = \overline{3}$. Contrôle : $3 \times 3 = 9 \equiv 1 \pmod{8}$ ✓.

**Réponse.** $(1-a)^{-1} = \sum_{k<n} a^k$ ; somme de nilpotents nilpotente si $ab = ba$ ; $(E_{12} + E_{21})^2 = I_2$ ; nilpotents : $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ et $\{\overline{0}, \overline{6}\}$ ; $\overline{3}^{-1} = \overline{3}$.

## Correction de l'exercice 5 – Idempotents et anneaux de Boole

**a)** $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$ (1 et $e$ commutent), et $e(1-e) = e - e^2 = 0$.

**b)** On teste les carrés. Modulo 6 : $0, 1, 4, 9 \equiv 3, 16 \equiv 4, 25 \equiv 1$ ; idempotents $\overline{0}, \overline{1}, \overline{3}, \overline{4}$ (et $\overline{3} + \overline{4} = \overline{1}$ : ce sont $e$ et $1 - e$).

— Modulo 10 : $5^2 = 25 \equiv 5$ et $6^2 = 36 \equiv 6$ ; les autres carrés ne redonnent pas le nombre ; idempotents $\overline{0}, \overline{1}, \overline{5}, \overline{6}$.

— Dans un anneau intègre, $e^2 = e$ s'écrit $e(e-1) = 0$, donc $e = 0$ ou $e = 1$.

**c)** On développe avec $x^2 = x$ :

$$x + x = (x+x)^2 = x^2 + x^2 + x^2 + x^2 = 4x$$

— donc $2x = 0$, soit $x = -x$ : dans un anneau de Boole, tout élément est son propre opposé.

— $(x+y) = (x+y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx$, donc $xy + yx = 0$, puis $xy = -yx = yx$ : l'anneau est **commutatif**.

**d)** $A \cap A = A$ : tout élément est idempotent. Le neutre de $\Delta$ est $\varnothing$ (le « 0 »), celui de $\cap$ est $E$ (le « 1 »). Conformément à c), $A \,\Delta\, A = \varnothing$ ($2x = 0$).

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

**Lecture** : un idempotent $e \neq 0, 1$ « découpe » l'anneau : dans $\mathbb{Z}/6\mathbb{Z}$, $\overline{3}$ et $\overline{4}$ correspondent aux facteurs $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ du théorème chinois.

**Réponse.** $1-e$ idempotent, $e(1-e)=0$ ; $\{\overline{0},\overline{1},\overline{3},\overline{4}\}$ et $\{\overline{0},\overline{1},\overline{5},\overline{6}\}$ ; intègre : 0 et 1 ; Boole : $2x=0$ et commutatif ; $0=\varnothing$, $1=E$.

## Correction de l'exercice 6 – Le groupe des inversibles d'un anneau

**a)** $1 \in A^\times$. Si $a, b$ sont inversibles, $ab$ l'est, avec la règle de l'inverse d'un produit (ordre renversé) :

$$(ab)\left(b^{-1}a^{-1}\right) = a\left(bb^{-1}\right)a^{-1} = aa^{-1} = 1$$

— (et de même dans l'autre ordre). L'inverse $a^{-1}$ est inversible, d'inverse $a$. L'associativité est celle de $\times$ : $A^\times$ est un groupe.

**b)** L'unité de $A \times B$ est $(1_A, 1_B)$ ; $(a,b)(a',b') = (1_A,1_B)$ équivaut à $aa' = 1_A$ et $bb' = 1_B$ (et de même dans l'autre ordre). Donc $(a,b)$ est inversible si et seulement si $a$ et $b$ le sont.

**c)** $\mathbb{Z}^\times = \{-1, 1\}$ (si $ab=1$ dans $\mathbb{Z}$, $|a|=1$). Par b), $(\mathbb{Z}\times\mathbb{Z})^\times = \{(\pm1,\pm1)\}$, groupe de Klein. $f \in F(\mathbb{R},\mathbb{R})$ est inversible si et seulement si elle **ne s'annule pas** (inverse $\frac{1}{f}$).

**d)** Les entiers de 0 à 8 premiers avec 9 : $1, 2, 4, 5, 7, 8$, soit $\varphi(9) = 6$ éléments. Puissances de $\overline{2}$ :

— $2, 4, 8, 16 \equiv 7, 14 \equiv 5, 10 \equiv 1$ : $\overline{2}$ est d'ordre 6, donc $(\mathbb{Z}/9\mathbb{Z})^\times = \langle\overline{2}\rangle$ est **cyclique**, isomorphe à $\mathbb{Z}/6\mathbb{Z}$.

— En revanche, $(\mathbb{Z}/8\mathbb{Z})^\times = \{\overline{1},\overline{3},\overline{5},\overline{7}\}$ n'a que des éléments d'ordre $\leq 2$ : c'est le groupe de Klein, **non cyclique**.

**Réponse.** $A^\times$ groupe ; $(A\times B)^\times = A^\times \times B^\times$ ; $\{\pm1\}$, $\{(\pm1,\pm1)\}$, fonctions sans zéro ; $(\mathbb{Z}/9\mathbb{Z})^\times = \langle\overline{2}\rangle$ cyclique d'ordre 6, $(\mathbb{Z}/8\mathbb{Z})^\times$ Klein.

## Correction de l'exercice 7 – Les inversibles de Z[√2] et l'équation de Pell

**a)** Si $a + b\sqrt{2} = a' + b'\sqrt{2}$ avec $b \neq b'$, alors $\sqrt{2} = \frac{a-a'}{b'-b} \in \mathbb{Q}$ : absurde. Donc $b = b'$, puis $a = a'$ : $\sigma$ est bien défini.

— $\sigma$ respecte la somme et 1 ; pour le produit, $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2}$, et remplacer $\sqrt{2}$ par $-\sqrt{2}$ des deux côtés donne $\sigma(xy)=\sigma(x)\sigma(y)$. D'où

$$N(xy) = xy\,\sigma(x)\sigma(y) = x\sigma(x)\times y\sigma(y) = N(x)N(y)$$

**b)** Si $xy=1$, alors $N(x)N(y)=N(1)=1$ avec $N(x), N(y) \in \mathbb{Z}$ : $N(x) = \pm1$. Réciproquement, si $N(x)=\pm1$, alors $x\sigma(x)=\pm1$, donc $x^{-1} = \pm\sigma(x) \in \mathbb{Z}[\sqrt{2}]$.

**c)** $N(u) = 1-2 = -1$ : $u$ est inversible, d'inverse $-\sigma(u) = \sqrt{2}-1$. Comme $u>1$, la suite $(u^n)$ est strictement croissante : les $u^n$ sont des inversibles **deux à deux distincts**, le groupe est infini.

**d)** $u^2 = 1+2\sqrt{2}+2 = 3+2\sqrt{2}$, $u^4 = (3+2\sqrt{2})^2 = 17+12\sqrt{2}$, $u^6 = (3+2\sqrt{2})(17+12\sqrt{2}) = 51+36\sqrt{2}+34\sqrt{2}+48 = 99+70\sqrt{2}$.

— $N(u^{2k}) = (-1)^{2k} = 1$ : les couples $(3,2)$, $(17,12)$, $(99,70)$ vérifient $a^2-2b^2=1$. Contrôle : $99^2 = 9\,801$ et $2\times70^2 = 9\,800$ ✓.

— $a^2-2b^2=1$ donne $\frac{a}{b} \approx \sqrt{2}$ : $\frac{99}{70} \approx 1{,}414\,286$, pour $\sqrt{2} \approx 1{,}414\,214$ (écart inférieur à $10^{-4}$).

**Réponse.** $N$ multiplicative ; inversible $\Leftrightarrow N(x)=\pm1$ ; $u = 1+\sqrt{2}$ d'ordre infini ;

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

$u^2 = 3 + 2\sqrt{2}$, $u^4 = 17 + 12\sqrt{2}$, $u^6 = 99 + 70\sqrt{2}$ ; $\frac{99}{70} \approx \sqrt{2}$.

## Correction de l'exercice 8 – Morphismes d'anneaux

Un morphisme d'anneaux respecte les deux lois **et** l'unité :

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(1) = 1$$

**a)** Un tel $f$ est en particulier un morphisme de groupes additifs, donc déterminé par $f(1) = 1_A$ : $f(k) = k \cdot 1_A$. Réciproquement, $k \mapsto k \cdot 1_A$ respecte la somme, et $(k \cdot 1_A)(l \cdot 1_A) = (kl) \cdot 1_A$ par distributivité. Existence et unicité.

**b)** D'après a), $f(n) = n$ pour $n \in \mathbb{Z}$. Pour $r = \frac{p}{q}$ : $q f(r) = f(q)f(r) = f(qr) = f(p) = p$, donc $f(r) = r$. Seule l'**identité** convient.

**c)** $f(a + \mathrm{i}b) = f(a) + f(b)f(\mathrm{i}) = a + bf(\mathrm{i})$, et $f(\mathrm{i})^2 = f(\mathrm{i}^2) = f(-1) = -1$, donc $f(\mathrm{i}) = \pm\mathrm{i}$.

— $f(\mathrm{i}) = \mathrm{i}$ : $f = \mathrm{id}$ ;

— $f(\mathrm{i}) = -\mathrm{i}$ : $f(z) = \overline{z}$, qui est bien un morphisme ($\overline{z+w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z}\,\overline{w}$).

**d)** $\det(2I_2) = 4 \neq \det I_2 + \det I_2 = 2$ : det n'est **pas** additif. $|1 + (-1)| = 0 \neq |1| + |-1|$ : le module non plus. Tous deux sont seulement des morphismes du **groupe** multiplicatif.

**Remarque** : b) montre que $\mathbb{Q}$ n'a pas d'automorphisme non trivial, c) que $\mathbb{C}$ n'en a que deux qui fixent $\mathbb{R}$.

**Réponse.** a) $k \mapsto k \cdot 1_A$, unique · b) l'identité · c) id et la conjugaison · d) non (ni det ni $|\cdot|$ ne sont additifs).

## Correction de l'exercice 9 – Un anneau intègre fini est un corps

**a)** Si $ax = ay$, alors $a(x-y) = 0$ avec $a \neq 0$ ; l'anneau étant intègre, $x = y$. Une injection d'un ensemble **fini** dans lui-même est une bijection : $\overline{1}$ a un antécédent $b$, $ab = 1$ (et $ba = 1$ par commutativité).

$$A \text{ intègre et fini} \Rightarrow A \text{ corps}$$

**b)** $\mathbb{Z}$ est intègre, mais 2 n'y est pas inversible. $\varphi_2 : x \mapsto 2x$ est injective sans être surjective : c'est la **finitude** qui manque.

**c)** Si $n = ab$ avec $1 < a, b < n$, alors $\overline{a}\overline{b} = \overline{0}$ avec $\overline{a}, \overline{b} \neq \overline{0}$ : non intègre. Si $n$ est premier et $\overline{a}\overline{b} = \overline{0}$, alors $n \mid ab$, donc $n \mid a$ ou $n \mid b$ (lemme d'Euclide) : intègre, donc corps par a). Un corps est intègre, ce qui boucle les équivalences.

**d)** Divisions successives :

— $19 = 2 \times 7 + 5$, $7 = 1 \times 5 + 2$, $5 = 2 \times 2 + 1$.

— On remonte :
$1 = 5 - 2 \times 2 = 5 - 2(7-5) = 3 \times 5 - 2 \times 7 = 3(19 - 2 \times 7) - 2 \times 7 = 3 \times 19 - 8 \times 7$.

Donc $-8 \times 7 \equiv 1 \pmod{19}$ et $\overline{7}^{-1} = -\overline{8} = \overline{11}$. Contrôle : $7 \times 11 = 77 = 4 \times 19 + 1$ ✓.

**Réponse.** $\varphi_a$ bijective donc $a$ inversible ; $\mathbb{Z}$ est intègre non corps ; $\mathbb{Z}/n\mathbb{Z}$ corps ⇔ intègre ⇔ $n$ premier ; $\overline{7}^{-1} = \overline{11}$ dans $\mathbb{Z}/19\mathbb{Z}$.

## Correction de l'exercice 10 – L'anneau des fonctions continues

**a)** Si $fg = 1$, $f$ ne s'annule pas. Réciproquement, si $f$ ne s'annule pas, $\frac{1}{f}$ est continue et $f \times \frac{1}{f} = 1$. Donc

$$A^\times = \{f \in A,\ \forall x \in [0,1],\ f(x) \neq 0\}$$

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— par le théorème des valeurs intermédiaires, ce sont les fonctions continues de **signe strict constant**.

**b)** $f$ et $g$ sont continues, non nulles ($f(0) = \frac{1}{2}$, $g(1) = \frac{1}{2}$). Pour $x \leq \frac{1}{2}$, $g(x) = 0$ ; pour $x \geq \frac{1}{2}$, $f(x) = 0$. Donc $fg = 0$ : $A$ n'est pas intègre.

**c)** $f^2 = f$ impose $f(x)(f(x) - 1) = 0$, donc $f(x) \in \{0, 1\}$ en tout point. Une fonction continue sur l'intervalle $[0, 1]$ à valeurs dans $\{0, 1\}$ est constante (sinon, par le TVI, elle prendrait la valeur $\frac{1}{2}$). Les idempotents de $A$ sont 0 et 1.

— Dans $F([0, 1], \mathbb{R})$, ce sont toutes les indicatrices $1_E$, $E \subset [0, 1]$ : une infinité.

**d)** $h(0) = 0$, donc $h$ n'est pas inversible. Si $hg = 0$ avec $g \in A$, alors $g(x) = 0$ pour tout $x \in ]0, 1]$, puis $g(0) = \lim_{x \to 0} g(x) = 0$ par continuité : $g = 0$. Ainsi $h$ n'est pas diviseur de zéro.

**Contraste** : dans $M_2(\mathbb{R})$ ou $\mathbb{Z}/n\mathbb{Z}$, tout élément non nul est inversible ou diviseur de zéro ; ici non.

**Réponse.** $A^\times$ : fonctions qui ne s'annulent pas ; $fg = 0$ ; idempotents 0 et 1 (contre toutes les indicatrices dans $F$) ; $x \mapsto x$ ni inversible ni diviseur de zéro.

## Correction de l'exercice 11 – L'anneau des nombres décimaux

**a)** Si $\frac{1}{3} = \frac{k}{10^n}$, alors $3k = 10^n = 2^n 5^n$ : 3 diviserait $2^n 5^n$, ce qui contredit l'unicité de la décomposition en facteurs premiers.

**b)** Soit $x = \frac{k}{10^n} \in \mathrm{D}^\times$, d'inverse $\frac{k'}{10^m}$. Alors

$$kk' = 10^{n+m} = 2^{n+m} 5^{n+m}$$

— donc $k$ divise une puissance de 10 : $k = \pm 2^\alpha 5^\beta$ avec $\alpha, \beta \geq 0$, et $x = \pm 2^{\alpha - n} 5^{\beta - n}$.

— Réciproquement, pour $a, b \in \mathbb{Z}$ et $N \geq \max(|a|, |b|)$, on écrit $2^a 5^b = \frac{2^{a+N} 5^{b+N}}{10^N} \in \mathrm{D}$ ; son inverse $2^{-a} 5^{-b}$ est de la même forme. Donc $\mathrm{D}^\times = \{\pm 2^a 5^b,\ a, b \in \mathbb{Z}\}$.

**c)** $0{,}125 = \frac{1}{8} = 2^{-3}$ : **inversible**, d'inverse 8. $0{,}3 = \frac{3}{10}$ : son inverse $\frac{10}{3}$ n'est pas décimal (comme en a)), **non inversible**.

**d)** D est un sous-anneau du corps $\mathbb{Q}$, donc commutatif et sans diviseur de zéro : **intègre**. Mais $3 \neq 0$ n'y est pas inversible d'après a) : ce n'est **pas un corps**.

**Lecture** : un rationnel est décimal si et seulement si, sous forme irréductible, son dénominateur n'a pour facteurs premiers que 2 et 5.

**Réponse.** $\frac{1}{3} \notin \mathrm{D}$ ; $\mathrm{D}^\times = \{\pm 2^a 5^b\}$ ; 0,125 inversible (inverse 8), 0,3 non ; intègre, pas un corps.

## Correction de l'exercice 12 – Matrices triangulaires supérieures

**a)** $I_2 \in T$, la différence de deux matrices de $T$ est dans $T$, et

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$$

— $T$ est un sous-anneau. Non commutatif : $E_{11}E_{12} = E_{12}$ et $E_{12}E_{11} = 0$.

**b)** La formule du produit montre que les coefficients diagonaux se multiplient : $\pi(MM') = (aa', cc') = \pi(M)\pi(M')$ ; $\pi$ respecte la somme et $\pi(I_2) = (1, 1)$. Surjectif : $(a, c) = \pi(\mathrm{diag}(a, c))$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— $\ker\pi = \left\{\begin{pmatrix}0 & b\\ 0 & 0\end{pmatrix}\right\}$ ; chacune de ces matrices vérifie $M^2 = \begin{pmatrix}0 & 0\cdot b + b\cdot 0\\ 0 & 0\end{pmatrix} = 0$.

**c)** $M \in T$ est inversible dans $M_2(\mathbb{R})$ si et seulement si $\det M = ac \neq 0$. Alors

— $\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\begin{pmatrix}\frac{1}{a} & -\frac{b}{ac}\\ 0 & \frac{1}{c}\end{pmatrix} = \begin{pmatrix}1 & -\frac{b}{c}+\frac{b}{c}\\ 0 & 1\end{pmatrix} = I_2$ : l'inverse est dans $T$, et $T^\times = \{M,\, ac \neq 0\}$.

**d)** Si $M^n = 0$, alors $\pi(M)^n = (a^n, c^n) = (0,0)$, donc $a = c = 0$. Réciproquement, $a = c = 0$ donne $M \in \ker\pi$, et $M^2 = 0$ d'après b).

**Méthode** : un morphisme d'anneaux vers un anneau plus simple ($\mathbb{R}^2$) transporte les propriétés (inversibilité, nilpotence) et permet de les lire sur la diagonale.

**Réponse.** $T$ sous-anneau non commutatif ; $\pi$ morphisme surjectif de noyau les matrices strictement triangulaires (de carré nul) ; $T^\times = \{ac \neq 0\}$ ; nilpotents : $a = c = 0$.

## Correction de l'exercice 13 – Binôme et morphisme de Frobenius

**a)** $k\binom{p}{k} = p\binom{p-1}{k-1}$ montre que $p$ divise $k\binom{p}{k}$. Or $1 \le k \le p-1$ et $p$ premier donnent $p \wedge k = 1$ : par le lemme de Gauss, $p \mid \binom{p}{k}$.

**b)** $A$ est commutatif, donc le binôme s'applique :

$$(a+b)^p = a^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k b^{p-k} + b^p$$

— chaque $\binom{p}{k}$ du milieu est un multiple de $p$, et $p \cdot 1_A = 0$ annule ces termes : $(a+b)^p = a^p + b^p$.

— $F(xy) = (xy)^p = x^p y^p$ (commutativité) et $F(1) = 1$ : $F$ est un morphisme d'anneaux, le **morphisme de Frobenius**.

**c)** Dans $\mathbb{Z}/p\mathbb{Z}$, $p\cdot\overline{1} = \overline{0}$. $\overline{0}^{\,p} = \overline{0}$ ; si $\overline{k}^{\,p} = \overline{k}$, alors par b)

— $\overline{k+1}^{\,p} = \left(\overline{k}+\overline{1}\right)^p = \overline{k}^{\,p} + \overline{1}^{\,p} = \overline{k}+\overline{1}$.

Donc $k^p \equiv k \pmod p$ pour tout $k \in \mathbb{N}$ : c'est le petit théorème de Fermat, obtenu sans théorie des groupes.

**d)** Dans $\mathbb{Z}/4\mathbb{Z}$, $4\cdot\overline{1} = \overline{0}$ mais 4 n'est pas premier : $\left(\overline{1}+\overline{1}\right)^4 = \overline{2}^4 = \overline{16} = \overline{0}$, alors que $\overline{1}^4 + \overline{1}^4 = \overline{2}$. Ici $\binom{4}{2} = 6$ n'est pas multiple de 4 : le terme $6a^2b^2$ ne disparaît pas.

**Réponse.** $p \mid \binom{p}{k}$ ; $(a+b)^p = a^p + b^p$, $F$ morphisme d'anneaux ; $k^p \equiv k$ $(p)$ ; dans $\mathbb{Z}/4\mathbb{Z}$, $(\overline{1}+\overline{1})^4 = \overline{0} \neq \overline{2}$.

## Correction de l'exercice 14 – Les quaternions

**a)** Le produit se calcule directement :

$$M(a,b)M(c,d) = \begin{pmatrix}ac - \overline{b}d & -a\overline{d} - \overline{b}\overline{c}\\ bc + \overline{a}d & -b\overline{d} + \overline{a}\overline{c}\end{pmatrix}$$

— avec $X = ac - \overline{b}d$ et $Y = bc + \overline{a}d$, le coefficient en bas à droite est $\overline{X}$ et celui en haut à droite $-\overline{Y}$ : le produit vaut $M(X,Y) \in \mathrm{H}$. De plus $I_2 = M(1,0)$ et $M(a,b) - M(c,d) = M(a-c, b-d)$ : sous-anneau.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

**b)** $\det M(a,b) = a\overline{a} + b\overline{b} = |a|^2 + |b|^2$, strictement positif dès que $(a,b) \neq (0,0)$. L'inverse est $\frac{1}{|a|^2+|b|^2}\begin{pmatrix} \overline{a} & \overline{b} \\ -b & a \end{pmatrix} = \frac{1}{|a|^2+|b|^2} M(\overline{a}, -b) \in \mathrm{H}$.

**c)** $I = \mathrm{diag}(\mathrm{i}, -\mathrm{i})$ et $J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ :

— $I^2 = J^2 = -I_2$ ; $K = IJ = \begin{pmatrix} 0 & -\mathrm{i} \\ -\mathrm{i} & 0 \end{pmatrix}$ ; $JI = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} = -K$ ; $K^2 = -I_2$.

Tout élément non nul est inversible, mais $IJ \neq JI$ : H n'est **pas commutatif**, donc pas un corps au sens du programme ; c'est un **corps gauche**.

**d)** $I, J, K$ anticommutent deux à deux ($IJ = -JI = K$, et de même $JK = -KJ$, $KI = -IK$), donc les doubles produits s'annulent :

$$(bI + cJ + dK)^2 = b^2I^2 + c^2J^2 + d^2K^2 = -\left(b^2 + c^2 + d^2\right) I_2$$

— toute la sphère $b^2 + c^2 + d^2 = 1$ fournit des solutions : une **infinité** de racines pour une équation de degré 2, ce qui est impossible dans un corps commutatif.

**Réponse.** H sous-anneau, $\det M(a,b) = |a|^2 + |b|^2$ ; non nul ⇒ inversible ; $IJ = K = -JI$, $I^2 = J^2 = K^2 = -I_2$ ; corps gauche ; $X^2 = -I_2$ a une infinité de solutions.

## Correction de l'exercice 15 – Synthèse : entiers de Gauss et sommes de deux carrés

**a)** $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$ (exercice 1), donc commutatif et sans diviseur de zéro : **intègre**. $N(a + \mathrm{i}b) = a^2 + b^2 \in \mathbb{N}$, et $|zw|^2 = |z|^2|w|^2$.

**b)** Si $zw = 1$, alors $N(z)N(w) = 1$ dans $\mathbb{N}$, donc $N(z) = a^2 + b^2 = 1$ :
$(a,b) \in \{(\pm 1, 0), (0, \pm 1)\}$. Réciproquement ces quatre éléments sont inversibles :

$$\mathbb{Z}[\mathrm{i}]^\times = \{1, -1, \mathrm{i}, -\mathrm{i}\}$$

**c)** Avec $z = a + \mathrm{i}b$ et $w = c + \mathrm{i}d$, $zw = (ac - bd) + \mathrm{i}(ad + bc)$ et $N(zw) = N(z)N(w)$ s'écrit

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ac - bd)^2 + (ad + bc)^2$$

**d)** $5 = 2^2 + 1^2 = N(2 + \mathrm{i})$ et $13 = 3^2 + 2^2 = N(3 + 2\mathrm{i})$.

— $(2 + \mathrm{i})(3 + 2\mathrm{i}) = 6 + 4\mathrm{i} + 3\mathrm{i} - 2 = 4 + 7\mathrm{i}$, d'où $65 = 4^2 + 7^2 = 16 + 49$ ✓.

— $(2 + \mathrm{i})(3 - 2\mathrm{i}) = 6 - 4\mathrm{i} + 3\mathrm{i} + 2 = 8 - \mathrm{i}$, d'où $65 = 8^2 + 1^2 = 64 + 1$ ✓.

**e)** Un carré est congru à 0 ou 1 modulo 4 ($(2k)^2 = 4k^2$, $(2k+1)^2 = 4(k^2 + k) + 1$), donc une somme de deux carrés est congrue à 0, 1 ou 2, jamais à 3.

— Si $3 = zw$, alors $N(z)N(w) = 9$. Si ni $z$ ni $w$ n'est inversible, $N(z) \neq 1$ et $N(w) \neq 1$, donc $N(z) = 3$ : 3 serait somme de deux carrés. Impossible : 3 est **irréductible** dans $\mathbb{Z}[\mathrm{i}]$.

— En revanche $5 = (2 + \mathrm{i})(2 - \mathrm{i})$, avec $N(2 \pm \mathrm{i}) = 5 \neq 1$ : 5, premier dans $\mathbb{Z}$, ne l'est plus dans $\mathbb{Z}[\mathrm{i}]$.

**Réponse.** Intègre, $N$ multiplicative ; $\mathbb{Z}[\mathrm{i}]^\times = \{\pm 1, \pm \mathrm{i}\}$ ;
$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$ ; $65 = 4^2 + 7^2 = 8^2 + 1^2$ ; 3 irréductible, $5 = (2 + \mathrm{i})(2 - \mathrm{i})$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).