

Anneaux

Diviseurs de zéro

Exercice 1 [02233] [Correction]

Montrer qu'un anneau $(A, +, \times)$ n'a pas de diviseurs de zéro si, et seulement si, tous ses éléments non nuls sont réguliers

Exercice 2 [02236] [Correction]

Soient a, b deux éléments d'un anneau $(A, +, \times)$ tels que ab soit inversible et b non diviseur de 0.

Montrer que a et b sont inversibles.

Sous-anneaux

Exercice 3 [02237] [Correction]

Soit $d \in \mathbb{N}$, on note

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a, b) \in \mathbb{Z}^2\}$$

Montrer que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice 4 [02238] [Correction]

On note

$$\mathcal{D} = \left\{ \frac{n}{10^k} \mid n \in \mathbb{Z}, k \in \mathbb{N} \right\}$$

l'ensemble des nombres décimaux.

Montrer que $\mathcal{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.

Exercice 5 [02239] [Correction]

[Anneau des entiers de Gauss 1777-1855] On note

$$\mathbb{Z}[i] = \{a + ib \mid (a, b) \in \mathbb{Z}^2\}$$

- a) Montrer que $\mathbb{Z}[i]$ est un anneau commutatif pour l'addition et la multiplication des nombres complexes.

- b) Pour $z \in \mathbb{Z}[i]$, on pose $N(z) = |z|^2$. Vérifier

$$\forall z, z' \in \mathbb{Z}[i], N(zz') = N(z)N(z') \text{ et } N(z) \in \mathbb{N}$$

- c) Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i]$.

Exercice 6 [02240] [Correction]

Soit

$$A = \left\{ \frac{m}{n} \mid m \in \mathbb{Z} \text{ et } n \in \mathbb{N}^*, \text{ impair} \right\}$$

- a) Montrer que A est un sous anneau de $(\mathbb{Q}, +, \times)$.
b) Quels en sont les éléments inversibles ?

Exercice 7 [02241] [Correction]

Soit

$$A = \left\{ \frac{m}{2^n} \mid m \in \mathbb{Z} \text{ et } n \in \mathbb{N} \right\}$$

- a) Montrer que A est un sous anneau de $(\mathbb{Q}, +, \times)$.
b) Quels en sont les éléments inversibles ?

Exercice 8 [00128] [Correction]

Pour $d \in \mathbb{N}$, on note

$$A_d = \{(x, y) \in \mathbb{Z}^2 \mid d \text{ divise } (y - x)\}$$

- a) Montrer que A_d est un sous anneau $(\mathbb{Z}^2, +, \times)$.
b) Inversement, soit A un sous anneau de $(\mathbb{Z}^2, +, \times)$.
Montrer que $H = \{x \in \mathbb{Z} \mid (x, 0) \in A\}$ est un sous groupe de $(\mathbb{Z}, +)$.
c) En déduire qu'il existe $d \in \mathbb{N}$ tel que $H = d\mathbb{Z}$ et $A = A_d$.

Exercice 9 [03376] [Correction]

Un anneau A est dit régulier si

$$\forall x \in A, \exists y \in A, xyx = x$$

On considère un tel anneau A et l'on introduit

$$Z = \{x \in A \mid \forall a \in A, ax = xa\}$$

- a) Montrer que Z est un sous-anneau de A .
 b) Vérifier que Z est régulier.

Exercice 10 [03856] [\[Correction\]](#)

On note $\mathcal{P}$ l'ensemble des nombres premiers. On se propose d'établir l'existence d'une correspondance bijective entre l'ensemble des sous-anneaux de l'anneau $(\mathbb{Q}, +, \times)$ et l'ensemble des parties de $\mathcal{P}$.

Pour A un sous-anneau de $(\mathbb{Q}, +, \times)$, on note

$$P(A) = \left\{ p \in \mathcal{P} \mid \frac{1}{p} \in A \right\}$$

- a) Soient A et B sont deux sous-anneaux de $(\mathbb{Q}, +, \times)$. Établir

$$P(A) = P(B) \implies A = B$$

- b) Soit P un sous-ensemble de $\mathcal{P}$. Déterminer un sous-anneau A de $(\mathbb{Q}, +, \times)$ vérifiant $P(A) = P$.
 c) Conclure.

Morphismes d'anneaux

Exercice 11 [00126] [\[Correction\]](#)

Soit $f: \mathbb{C} \rightarrow \mathbb{C}$ un morphisme d'anneaux tel que

$$\forall x \in \mathbb{R}, f(x) = x$$

Montrer que f est l'identité ou la conjugaison complexe.

Exercice 12 [00127] [\[Correction\]](#)

Soit a un élément d'un ensemble X .

Montrer l'application $E_a: \mathcal{F}(X, \mathbb{R}) \rightarrow \mathbb{R}$ définie par $E_a(f) = f(a)$ est un morphisme d'anneaux.

Théorème chinois

Exercice 13 [00143] [\[Correction\]](#)

Résoudre les systèmes suivants :

$$\text{a) } \begin{cases} x \equiv 1 \pmod{6} \\ x \equiv 2 \pmod{7} \end{cases}$$

$$\text{b) } \begin{cases} 3x \equiv 2 \pmod{5} \\ 5x \equiv 1 \pmod{6} \end{cases}$$

Exercice 14 [01216] [\[Correction\]](#)

Résoudre le système :

$$\begin{cases} x \equiv 2 \pmod{10} \\ x \equiv 5 \pmod{13} \end{cases}$$

Exercice 15 [01217] [\[Correction\]](#)

Soient $a, b, a', b' \in \mathbb{Z}$ avec b et b' premiers entre eux.

Montrer que le système

$$\begin{cases} x \equiv a \pmod{b} \\ x \equiv a' \pmod{b'} \end{cases}$$

possède des solutions et que celles-ci sont congrues entre elles modulo bb' .

Exercice 16 [01218] [\[Correction\]](#)

Une bande de 17 pirates dispose d'un butin composé de N pièces d'or d'égale valeur. Ils décident de se le partager également et de donner le reste au cuisinier (non pirate). Celui ci reçoit 3 pièces. Mais une rixe éclate et 6 pirates sont tués. Tout le butin est reconstitué et partagé entre les survivants comme précédemment ; le cuisinier reçoit alors 4 pièces. Dans un naufrage ultérieur, seul le butin, 6 pirates et le cuisinier sont sauvés. Le butin est à nouveau partagé de la même manière et le cuisinier reçoit 5 pièces. Quelle est alors la fortune minimale que peut espérer le cuisinier lorsqu'il décide d'empoisonner le reste des pirates ?

Corps

Exercice 17 [02244] [\[Correction\]](#)

Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$, on note

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a, b) \in \mathbb{Q}^2\}$$

Montrer que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un corps.

Exercice 18 [00129] [\[Correction\]](#)

Soit $(A, +, \times)$ un anneau intègre fini.

- a) Soit $a \in A$ avec $a \neq 0_A$. Montrer que l'application $x \mapsto ax$ est une permutation de A .
- b) En déduire que tout élément non nul de $(A, +, \times)$ est inversible.

Exercice 19 [02245] [Correction]

Soit A un anneau commutatif fini non nul.

Montrer que A ne possède pas de diviseurs de zéro si, et seulement si, A est un corps.

Exercice 20 [00130] [Correction]

Soit $\mathbb{K}$ un corps fini commutatif. Calculer

$$\prod_{x \in \mathbb{K}^*} x$$

Exercice 21 [00132] [Correction]

Soient K, L deux corps et f un morphisme d'anneaux entre K et L .

- a) Montrer que $f(x)$ est inversible pour tout $x \in K$ non nul et déterminer $f(x)^{-1}$.
- b) En déduire que tout morphisme de corps est injectif.

Exercice 22 [02662] [Correction]

Soit $K = \mathbb{Q} + \sqrt{2}\mathbb{Q} + \sqrt{3}\mathbb{Q} + \sqrt{6}\mathbb{Q}$.

- a) Montrer que $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est une $\mathbb{Q}$ -base du $\mathbb{Q}$ -espace vectoriel K .
- b) Montrer que K est un sous-corps de $\mathbb{R}$.

Exercice 23 [02677] [Correction]

Soit $\mathbb{K}$ un corps, E un espace vectoriel de dimension finie n sur $\mathbb{K}$ et $\mathbb{L}$ un sous-corps de $\mathbb{K}$ tel que $\mathbb{K}$ est un espace vectoriel de dimension finie p sur $\mathbb{L}$. Montrer que E est un espace vectoriel de dimension finie q sur $\mathbb{L}$. Relier n, p, q .

Indicatrice d'Euler

Exercice 24 [02655] [Correction]

Combien y a-t-il d'éléments inversibles dans $\mathbb{Z}/78\mathbb{Z}$?

Exercice 25 [00151] [Correction]

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z}, \times)$.

- a) Calculer $\varphi(p)$ et $\varphi(p^\alpha)$ pour p premier et $\alpha \in \mathbb{N}^*$.
- b) Soient m et n premiers entre eux.
On considère l'application $f: \mathbb{Z}/mn\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ définie par $f(\bar{x}) = (\hat{x}, \tilde{x})$.
Montrer que f est bien définie et réalise un isomorphisme d'anneaux.
- c) En déduire que $\varphi(mn) = \varphi(m)\varphi(n)$.
- d) Exprimer $\varphi(n)$ selon la décomposition primaire de n .

Exercice 26 [00257] [Correction]

Établir

$$\forall n \geq 3, \varphi(n) \geq \frac{n \ln 2}{\ln n + \ln 2}$$

Exercice 27 [02374] [Correction]

Montrer que pour tout entier $n \geq 3$, $\varphi(n)$ est un nombre pair.

Exercice 28 [00152] [Correction]

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'éléments inversibles dans $(\mathbb{Z}/n\mathbb{Z}, \times)$.

Établir

$$\forall a \in (\mathbb{Z}/n\mathbb{Z})^*, a^{\varphi(n)} = 1$$

Exercice 29 [00153] [Correction]

Pour $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

- a) Montrer que si H est un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$, il existe a divisant n vérifiant $H = \langle \bar{a} \rangle$.
- b) Observer que si $d \mid n$ il existe un unique sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d .
- c) Justifier que si $d \mid n$ le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ possède exactement $\varphi(d)$ éléments d'ordre d .

d) Montrer

$$\forall n \in \mathbb{N}^*, \sum_{d|n} \varphi(d) = n$$

Exercice 30 [03634] [\[Correction\]](#)

On note φ la fonction indicatrice d'Euler.

a) Soit d un diviseur positif de $n \in \mathbb{N}^*$. Combien y a-t-il d'entiers k vérifiant

$$k \in \llbracket 1; n \rrbracket \text{ et } \text{pgcd}(k, n) = d?$$

b) En déduire

$$n = \sum_{d|n} \varphi(d)$$

Exercice 31 [02381] [\[Correction\]](#)

Soient $T = (t_{i,j}) \in \mathcal{M}_n(\mathbb{R})$ déterminée par

$$t_{i,j} = \begin{cases} 1 & \text{si } i \text{ divise } j \\ 0 & \text{sinon} \end{cases}$$

et $D = \text{diag}(\varphi(1), \dots, \varphi(n)) \in \mathcal{M}_n(\mathbb{R})$ matrice diagonale.

On rappelle la propriété

$$\forall n \in \mathbb{N}^*, n = \sum_{d|n} \varphi(d)$$

a) Calculer le coefficient d'indice (i, j) de la matrice ${}^tTDT$ en fonction de $\text{pgcd}(i, j)$.

b) En déduire la valeur du déterminant de la matrice de Smith

$$S = \begin{pmatrix} \text{pgcd}(1, 1) & \text{pgcd}(1, 2) & \cdots & \text{pgcd}(1, n) \\ \text{pgcd}(2, 1) & \text{pgcd}(2, 2) & \cdots & \text{pgcd}(2, n) \\ \vdots & \vdots & & \vdots \\ \text{pgcd}(n, 1) & \text{pgcd}(n, 2) & \cdots & \text{pgcd}(n, n) \end{pmatrix}$$

Exercice 32 [02658] [\[Correction\]](#)

a) Pour $(a, n) \in \mathbb{Z} \times \mathbb{N}^*$ avec $a \wedge n = 1$, montrer que $a^{\varphi(n)} = 1 \pmod{n}$.

b) Pour p premier et $k \in \{1, \dots, p-1\}$, montrer que p divise $\binom{p}{k}$.

c) Soit $(a, n) \in (\mathbb{N}^*)^2$. On suppose que $a^{n-1} = 1 \pmod{n}$. On suppose que pour tout x divisant $n-1$ et différent de $n-1$, on a $a^x \neq 1 \pmod{n}$. Montrer que n est premier.

Exercice 33 [04061] [\[Correction\]](#)

Soient a et n des naturels supérieurs ou égaux à 2. Montrer que n divise $\varphi(a^n - 1)$.

Idéaux

Exercice 34 [00134] [\[Correction\]](#)

Quels sont les idéaux d'un corps $\mathbb{K}$?

Exercice 35 [03854] [\[Correction\]](#)

Un idéal d'un anneau $(A, +, \times)$ est dit principal lorsqu'il est de la forme xA pour un certain $x \in A$.

Montrer que les idéaux d'un sous-anneau de $(\mathbb{Q}, +, \times)$ sont principaux.

Exercice 36 [00135] [\[Correction\]](#)

On note

$$\mathbb{D} = \left\{ \frac{p}{10^n} \mid p \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

l'ensemble des nombres décimaux.

a) Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.

b) Montrer que les idéaux de $\mathbb{D}$ sont principaux (c'est-à-dire de la forme $a\mathbb{D}$ avec $a \in \mathbb{D}$).

Exercice 37 [03635] [\[Correction\]](#)

Soit I un idéal de l'anneau produit $(\mathbb{Z}^2, +, \times)$.

a) On pose $I_1 = \{x \in \mathbb{Z} \mid (x, 0) \in I\}$ et $I_2 = \{y \in \mathbb{Z} \mid (0, y) \in I\}$. Montrer que I_1 et I_2 sont des idéaux de $(\mathbb{Z}, +, \times)$.

b) Établir $I = I_1 \times I_2$.

c) Conclure que les idéaux de l'anneau $(\mathbb{Z}^2, +, \times)$ sont de la forme $x\mathbb{Z}^2$ avec $x \in \mathbb{Z}^2$.

Exercice 38 [00136] [Correction]

[Nilradical d'un anneau] On appelle nilradical d'un anneau commutatif $(A, +, \times)$ l'ensemble N formé des éléments nilpotents de A i.e. des $x \in A$ tels qu'il existe $n \in \mathbb{N}^*$ vérifiant $x^n = 0_A$.

Montrer que N est un idéal de A .

Exercice 39 [00137] [Correction]

[Radical d'un idéal] Soit I un idéal d'un anneau commutatif A . On note $R(I)$ l'ensemble des éléments x de A pour lesquels il existe un entier n non nul tel que $x^n \in I$.

- Montrer que $R(I)$ est un idéal de A contenant I .
- Montrer que si I et J sont deux idéaux alors

$$R(I \cap J) = R(I) \cap R(J) \text{ et } R(I + J) \supset R(I) + R(J)$$

- On suppose que $A = \mathbb{Z}$. Montrer que l'ensemble des entiers n non nuls tels que $R(n\mathbb{Z}) = n\mathbb{Z}$ est exactement l'ensemble des entiers sans facteurs carrés.

Exercice 40 [00138] [Correction]

Soient A un anneau commutatif et e un élément idempotent de A (i.e. $e^2 = e$).

- Montrer que $J = \{x \in A \mid xe = 0\}$ est un idéal de A .
- On note $I = Ae$ l'idéal principal engendré par e . Déterminer $I + J$ et $I \cap J$.
- Établir que pour tout idéal K de A :

$$(K \cap I) + (K \cap J) = K$$

Exercice 41 [00140] [Correction]

[Idéaux premiers] Un idéal I d'un anneau commutatif $(A, +, \times)$ est dit premier si, et seulement si,

$$\forall x, y \in A, xy \in I \implies x \in I \text{ ou } y \in I$$

- Donner un exemple d'idéal premier dans $\mathbb{Z}$.
- Soit $P \in \mathbb{K}[X]$ un polynôme irréductible. Montrer que $P.\mathbb{K}[X]$ est premier.
- Soient J et K deux idéaux de A et I un idéal premier. Montrer

$$J \cap K = I \implies (J = I \text{ ou } K = I)$$

- Soit $(A, +, \times)$ un anneau commutatif dont tout idéal est premier. Établir que A est intègre puis que A est un corps.

Exercice 42 [00141] [Correction]

[$\mathbb{Z}$ est noethérien] Montrer que toute suite croissante (pour l'inclusion) d'idéaux de $\mathbb{Z}$ est stationnaire.

Ce résultat se généralise-t-il aux idéaux de $\mathbb{K}[X]$?

Exercice 43 [02367] [Correction]

Soit A un sous-anneau de $\mathbb{Q}$.

- Soit p un entier et q un entier strictement positif premier avec p . Montrer que si $p/q \in A$ alors $1/q \in A$.
- Soit I un idéal de A autre que $\{0\}$. Montrer qu'il existe $n \in \mathbb{N}^*$ tel que $I \cap \mathbb{Z} = n\mathbb{Z}$ et qu'alors $I = nA$.
- Soit p un nombre premier. On pose

$$Z_p = \{a \mid b; a \in \mathbb{Z}, b \in \mathbb{N}^*, p \wedge b = 1\}$$

Montrer que si $x \in \mathbb{Q}^*$ alors x ou $1/x$ appartient à Z_p .

- On suppose ici que x ou $1/x$ appartient à A pour tout $x \in \mathbb{Q}^*$. On note I l'ensemble des éléments non inversibles de A . Montrer que I inclut tous les idéaux stricts de A . En déduire que $A = \mathbb{Q}$ ou $A = Z_p$ pour un certain nombre premier p .

Exercice 44 [02661] [Correction]

Soit p un nombre premier. On note Z_p l'ensemble des a/b où $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ et p ne divise pas b . On note J_p l'ensemble des a/b où $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, p divise a et p ne divise pas b .

- Montrer que Z_p est un sous-anneau de $\mathbb{Q}$.
- Montrer que J_p est un idéal de Z_p et que tout idéal de Z_p autre que Z_p est inclus dans J_p .
- Déterminer les idéaux de Z_p .

Exercice 45 [02450] [Correction]

Soit A un sous-anneau d'un corps K .

On suppose :

$$\forall x \in K \setminus \{0\}, x \in A \text{ ou } x^{-1} \in A$$

et on forme I l'ensemble des éléments de l'anneau A non inversibles.

- a) Montrer que I est un idéal de A .
 b) Montrer que tout idéal de A autre que A est inclus dans I .

Exercice 46 [03843] [Correction]

Soit A un anneau intègre. On suppose que l'anneau A ne possède qu'un nombre fini d'idéaux.

Montrer que A est un corps.

Classes de congruence

Exercice 47 [00142] [Correction]

Résoudre les équations suivantes :

- a) $3x + 5 = 0$ dans $\mathbb{Z}/10\mathbb{Z}$
 b) $x^2 = 1$ dans $\mathbb{Z}/8\mathbb{Z}$
 c) $x^2 + 2x + 2 = 0$ dans $\mathbb{Z}/5\mathbb{Z}$.

Exercice 48 [03915] [Correction]

Résoudre le système suivant :

$$\begin{cases} x + y \equiv 4 & \text{mod } 11 \\ xy \equiv 10 & \text{mod } 11 \end{cases}$$

Exercice 49 [00147] [Correction]

Déterminer les morphismes de groupes entre $(\mathbb{Z}/n\mathbb{Z}, +)$ et $(\mathbb{Z}/m\mathbb{Z}, +)$.

Exercice 50 [02364] [Correction]

Soit un entier $n \geq 2$. Combien le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ admet-il de sous-groupes ?

Exercice 51 [00145] [Correction]

Soit p un nombre premier et k un entier premier avec $p - 1$.

Montrer que l'application $\varphi: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ définie par $\varphi(x) = x^k$ est bijective.

Exercice 52 [00146] [Correction]

Soit p un entier premier. Montrer que pour tout $k \in \mathbb{N}$, $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$ est égal à 0 ou -1 .

Exercice 53 [03218] [Correction]

Soit p un nombre premier. Calculer dans $\mathbb{Z}/p\mathbb{Z}$

$$\sum_{k=1}^p \bar{k} \text{ et } \sum_{k=1}^p \bar{k}^2$$

Exercice 54 [00148] [Correction]

[Théorème de Wilson] Soit p un nombre premier.

- a) Quels sont les éléments de $\mathbb{Z}/p\mathbb{Z}$ qui sont égaux à leurs inverses ?
 b) En déduire que p divise $(p - 1)! + 1$.
 c) Inversement, montrer que si un entier n supérieur à 2 divise $(n - 1)! + 1$ alors cet entier est premier.

Exercice 55 [03929] [Correction]

- a) Déterminer l'ensemble des inversibles de l'anneau $\mathbb{Z}/8\mathbb{Z}$. De quelle structure peut-on munir cet ensemble ?
 b) Y a-t-il, à isomorphisme près, d'autres groupes de cardinal 4 ?

Exercice 56 [00149] [Correction]

Soit p un nombre premier supérieur à 3.

- a) Quel est le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$?
 b) On suppose $p \equiv 1 \pmod{4}$. En calculant de deux façons $(p - 1)!$, justifier que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
 c) On suppose $p \equiv 3 \pmod{4}$. Montrer que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 57 [02649] [Correction]

Soit $(G, \cdot)$ un groupe fini tel que

$$\forall g \in G, g^2 = e$$

où e est le neutre de G . On suppose G non réduit à $\{e\}$.

Montrer qu'il existe $n \in \mathbb{N}^*$ tel que G est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.

Exercice 58 [02660] [\[Correction\]](#)

Si p est un nombre premier, quel est le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$?

Exercice 59 [03780] [\[Correction\]](#)

Donner l'ensemble G des inversibles de l'anneau $\mathbb{Z}/20\mathbb{Z}$.

Montrer que $(G, \times)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, +)$

Exercice 60 [00144] [\[Correction\]](#)

[Petit théorème de Fermat] Soit p un nombre premier. Montrer

$$\forall a \in (\mathbb{Z}/p\mathbb{Z})^*, a^{p-1} = 1$$

Algèbres

Exercice 61 [01265] [\[Correction\]](#)

Soit

$$E = \left\{ M(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} / (a, b, c) \in \mathbb{R}^3 \right\}$$

Montrer que E est une sous-algèbre commutative de $\mathcal{M}_3(\mathbb{R})$ dont on déterminera la dimension.

Exercice 62 [03408] [\[Correction\]](#)

Soit $\mathbb{K}$ une algèbre intègre sur $\mathbb{R}$ de dimension finie $n \geq 2$. On assimile $\mathbb{R}$ à $\mathbb{R}.1$ où 1 est l'élément de $\mathbb{K}$ neutre pour le produit.

- Montrer que tout élément non nul de $\mathbb{K}$ est inversible.
- Soit a un élément de $\mathbb{K}$ non situé dans $\mathbb{R}$. Montrer que la famille $(1, a)$ est libre tandis que la famille $(1, a, a^2)$ est liée.
- Montrer l'existence de $i \in \mathbb{K}$ tel que $i^2 = -1$.
- Montrer que si $\mathbb{K}$ est commutative alors $\mathbb{K}$ est isomorphe à $\mathbb{C}$.

Exercice 63 [02390] [\[Correction\]](#)

Soit n un entier ≥ 2 et $\mathcal{A}$ un hyperplan de $\mathcal{M}_n(\mathbb{C})$ stable pour le produit matriciel.

- On suppose que $I_n \notin \mathcal{A}$. Montrer, si $M^2 \in \mathcal{A}$, que $M \in \mathcal{A}$. En déduire que pour tout $i \in \{1, \dots, n\}$ que la matrice $E_{i,i}$ est dans $\mathcal{A}$. En déduire une absurdité.
- On prend $n = 2$. Montrer que $\mathcal{A}$ est isomorphe à l'algèbre des matrices triangulaires supérieures.

Corrections

Exercice 1 : [énoncé]

Supposons que A n'ait pas de diviseurs de zéro.

Soit $x \in A$ avec $x \neq 0$.

$$\forall a, b \in A, xa = xb \implies x(a - b) = 0 \implies a - b = 0$$

car $x \neq 0$.

Ainsi x est régulier à gauche. Il en est de même à droite.

Supposons que tout élément non nul de A soit régulier.

$$\forall x, y \in A, xy = 0 \implies xy = x \cdot 0 \implies x = 0 \text{ ou } y = 0$$

(par régularité de x dans le cas où $x \neq 0$).

Par suite l'anneau A ne possède pas de diviseurs de zéro.

Exercice 2 : [énoncé]

Soit $x = b(ab)^{-1}$. Montrons que x est l'inverse de a .

On a $ax = ab(ab)^{-1} = 1$ et $xab = b(ab)^{-1}ab = b$ donc $(xa - 1)b = 0$ puis $xa = 1$ car b n'est pas diviseur de 0. Ainsi a est inversible et x est son inverse.

De plus $b = a^{-1}(ab)$ l'est aussi par produit d'éléments inversibles.

Exercice 3 : [énoncé]

$$\mathbb{Z}[\sqrt{d}] \subset \mathbb{R}, 1 \in \mathbb{Z}[\sqrt{d}].$$

Soient $x, y \in \mathbb{Z}[\sqrt{d}]$, on peut écrire $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$ avec $a, b, a', b' \in \mathbb{Z}$.

$$x - y = (a - a') + (b - b')\sqrt{d} \text{ avec } a - a', b - b' \in \mathbb{Z} \text{ donc } x - y \in \mathbb{Z}[\sqrt{d}].$$

$$xy = (aa' + bb'd) + (ab' + a'b)\sqrt{d} \text{ avec } aa' + bb'd, ab' + a'b \in \mathbb{Z} \text{ donc } xy \in \mathbb{Z}[\sqrt{d}].$$

Ainsi $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $(\mathbb{R}, +, \times)$.

Exercice 4 : [énoncé]

$\mathcal{D} \subset \mathbb{Q}$ et $1 \in \mathcal{D}$ car $1 = \frac{1}{10^0}$.

Soient $x, y \in \mathcal{D}$, on peut écrire $x = \frac{n}{10^k}$ et $y = \frac{m}{10^\ell}$ avec $n, m \in \mathbb{Z}$ et $k, \ell \in \mathbb{N}$.

$$x - y = \frac{n10^\ell - m10^k}{10^{k+\ell}} \text{ avec } n10^\ell - m10^k \in \mathbb{Z} \text{ et } k + \ell \in \mathbb{N} \text{ donc } x - y \in \mathcal{D}.$$

$$xy = \frac{nm}{10^{k+\ell}} \text{ avec } nm \in \mathbb{Z} \text{ et } k + \ell \in \mathbb{N} \text{ donc } xy \in \mathcal{D}.$$

Ainsi $\mathcal{D}$ est un sous-anneau de $(\mathbb{Q}, +, \times)$.

Exercice 5 : [énoncé]

a) Montrer que $\mathbb{Z}[i]$ est un sous anneau de $(\mathbb{C}, +, \times)$. $\mathbb{Z}[i] \subset \mathbb{C}$, $1 \in \mathbb{Z}[i]$.
 $\forall x, y \in \mathbb{Z}[i]$, on peut écrire $x = a + ib$ et $y = a' + ib'$ avec $a, b, a', b' \in \mathbb{Z}$.
 $x - y = (a - a') + i(b - b')$ avec $a - a', b - b' \in \mathbb{Z}$ donc $x - y \in \mathbb{Z}[i]$.
 $xy = (aa' - bb') + i(ab' + a'b)$ avec $aa' - bb', ab' + a'b \in \mathbb{Z}$ donc $xy \in \mathbb{Z}[i]$.
Ainsi $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.

b) $N(zz') = |zz'|^2 = |z|^2 |z'|^2 = N(z)N(z')$ et $N(z) = a^2 + b^2 \in \mathbb{N}$ avec $z = a + ib$ et $a, b \in \mathbb{Z}$.

c) Si z est inversible d'inverse z' alors $N(zz') = N(z)N(z') = 1$. Or $N(z), N(z') \in \mathbb{N}$ donc $N(z) = N(z') = 1$.
On en déduit $z = 1, -1, i$ ou $-i$. La réciproque est immédiate.

Exercice 6 : [énoncé]

a) $A \subset \mathbb{Q}$, $1 \in A$, $\forall x, y \in A, x - y \in A$ et $xy \in A$: clair.

Par suite A est un sous anneau de $(\mathbb{Q}, +, \times)$.

b) $x \in A$ est inversible si, et seulement si, il existe $y \in A$ tel que $xy = 1$.

$x = \frac{m}{n}, y = \frac{m'}{n'}$ avec n, n' impairs. $xy = 1 \implies mm' = nn'$ donc m est impair et la réciproque est immédiate.

Ainsi

$$U(A) = \left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}^* \text{ impairs} \right\}$$

Exercice 7 : [énoncé]

a) $A \subset \mathbb{Q}$, $1 \in A$, $\forall x, y \in A, x - y \in A$ et $xy \in A$: facile.

Ainsi A est un sous anneau de $(\mathbb{Q}, +, \times)$.

b) $x \in A$ est inversible si, et seulement si, il existe $y \in A$ tel que $xy = 1$.

Puisqu'on peut écrire $x = \frac{m}{2^n}, y = \frac{m'}{2^{n'}}$ avec $m, m' \in \mathbb{Z}$ et $n, n' \in \mathbb{N}$,

$$xy = 1 \implies mm' = 2^{n+n'}$$

Par suite m est, au signe près, une puissance de 2.

La réciproque est immédiate.

Finalement

$$U(A) = \{\pm 2^k \mid k \in \mathbb{Z}\}$$

Exercice 8 : [énoncé]

- a) $A_d \subset \mathbb{Z}^2$ et $1_{\mathbb{Z}^2} = (1, 1) \in A_d$.
 Pour $(x, y), (x', y') \in A_d$, $(x, y) - (x', y') = (x - x', y - y')$ avec
 $d \mid (y - y') - (x - x')$ donc $(x, y) - (x', y') \in A_d$.
 Aussi $(x, y)(x', y') = (xx', yy')$ avec $d \mid (yy' - xx') = (y - x)y' + x(y' - x')$
 donc $(x, y)(x', y') \in A_d$.
- b) $H \neq \emptyset$ car $0 \in H$ et $\forall x, y \in H$, $x - y \in H$ car $(x - y, 0) = (x, 0) - (y, 0) \in A$.
- c) H sous groupe de $(\mathbb{Z}, +)$ donc il existe $d \in \mathbb{N}$ tel que

$$H = d\mathbb{Z}$$

Pour tout $(x, y) \in A$, on a $(x, y) - (y, y) = (x - y, 0) \in A$ car
 $(y, y) \in \langle (1, 1) \rangle \subset A$. Par suite $x - y \in d\mathbb{Z}$.
 Inversement, si $x - y \in d\mathbb{Z}$ alors $(x - y, 0) \in A$ puis
 $(x, y) = (x - y, 0) + y.(1, 1) \in A$.
 Ainsi

$$(x, y) \in A \iff x - y \in d\mathbb{Z}$$

et donc alors

$$A = \{(x, y) \in \mathbb{Z}^2 \mid d \text{ divise } (y - x)\} = A_d$$

Exercice 9 : [énoncé]

- a) Immédiatement $Z \subset A$ et $1_A \in Z$.
 Soient $x, y \in Z$. Pour tout $a \in A$

$$a(x - y) = ax - ay = xa - ya = (x - y)a$$

et

$$a(xy) = xay = xya$$

donc $x - y \in A$ et $xy \in A$.
 Ainsi Z est un sous-anneau de A .

- b) Soit $x \in Z$. Il existe $y \in A$ tel que $xyx = x$. La difficulté est de voir que l'on peut se ramener au cas où $y \in Z$... Pour cela considérons l'élément $z = xy^2$. On observe

$$xzx = x^3y^2 = xyxyx = xyx = x$$

Il reste à montrer $z \in Z$. Posons $a \in A$. L'élément x^3 commute avec y^2ay^2 et donc

$$x^3y^2ay^2 = y^2ay^2x^3$$

ce qui donne

$$xay^2 = y^2ax$$

puis $az = za$. On peut alors conclure que l'anneau Z est régulier au sens défini.

Exercice 10 : [énoncé]

- a) Supposons $P(A) = P(B)$.
 Soit $x \in A$ de représentant irréductible a/b . Puisque a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$ et alors

$$\frac{1}{b} = \frac{au + bv}{b} = u \cdot \frac{a}{b} + v$$

Sachant que a/b est élément de A et que 1 l'est aussi, par addition dans le sous-groupe $(A, +)$, on obtient

$$\frac{1}{b} \in A$$

Si p est diviseur premier de b , on peut écrire $b = pk$ avec $k \in \mathbb{Z}$ et alors

$$\frac{1}{p} = k \cdot \frac{1}{b} \in A$$

Par suite les diviseurs premiers de b sont éléments de $P(A)$. Or $P(A) = P(B)$ et les diviseurs premiers de b sont aussi éléments de B . Puisque B est stable par produit, l'élément $1/b$ appartient à B et, finalement,

$$x = a \cdot \frac{1}{b} \in B$$

Ainsi $A \subset B$ et, par argument de symétrie, $A = B$.

- b) Formons

$$A = \left\{ \frac{a}{b} \mid \text{les diviseurs premiers de } b \text{ sont éléments de } P \right\}$$

On vérifie aisément que A est une partie de $\mathbb{Q}$, contenant 1, stable par différence et produit. C'est donc un sous-anneau pour lequel on vérifie aisément $P = P(A)$.

- c) L'application $A \mapsto P(A)$ définit la correspondance bijective voulue.

Exercice 11 : [énoncé]

Posons $j = f(i)$. On a $j^2 = f(i)^2 = f(i^2) = f(-1) = -f(1) = -1$ donc $j = \pm i$.
 Si $j = i$ alors $\forall a, b \in \mathbb{R}$, $f(a + ib) = f(a) + f(i)f(b) = a + ib$ donc $f = \text{Id}_{\mathbb{C}}$.
 Si $j = -i$ alors $\forall a, b \in \mathbb{R}$, $f(a + ib) = f(a) + f(i)f(b) = a - ib$ donc $f: z \mapsto \bar{z}$.

Exercice 12 : [énoncé]

$E_a(x \mapsto 1) = 1$.
 $\forall f, g \in \mathcal{F}(X, \mathbb{R})$, $E_a(f + g) = (f + g)(a) = f(a) + g(a) = E_a(f) + E_a(g)$ et
 $E_a(fg) = (fg)(a) = f(a)g(a) = E_a(f)E_a(g)$ donc E_a est un morphisme d'anneaux.

Exercice 13 : [énoncé]

- a) 6 et 7 sont premiers entre eux avec la relation de Bézout $(-1) \times 6 + 7 = 1$.
 $x_1 = 7$ et $x_2 = -6$ sont solutions des systèmes

$$\begin{cases} x \equiv 1 & \text{mod } 6 \\ x \equiv 0 & \text{mod } 7 \end{cases} \text{ et } \begin{cases} x \equiv 0 & \text{mod } 6 \\ x \equiv 1 & \text{mod } 7 \end{cases}$$

donc $x = 1 \times 7 + 2 \times (-6) = -5$ est solution du système étudié dont la solution générale est alors

$$x = 37 + 42k \text{ avec } k \in \mathbb{Z}$$

b)

$$\begin{cases} 3x \equiv 2 & \text{mod } 5 \\ 5x \equiv 1 & \text{mod } 6 \end{cases} \iff \begin{cases} x \equiv 4 & \text{mod } 5 \\ x \equiv 5 & \text{mod } 6 \end{cases}$$

on poursuit comme ci-dessus. Les solutions sont $29 + 30k$ avec $k \in \mathbb{Z}$.

Exercice 14 : [énoncé]

$10 \wedge 13 = 1$ avec la relation de Bézout

$$-9 \times 10 + 7 \times 13 = 1$$

Les nombres $x_1 = 7 \times 13 = 91$ et $x_2 = -9 \times 10 = -90$ sont solutions des systèmes

$$\begin{cases} x \equiv 1 & \text{mod } 10 \\ x \equiv 0 & \text{mod } 13 \end{cases} \text{ et } \begin{cases} x \equiv 0 & \text{mod } 10 \\ x \equiv 1 & \text{mod } 13 \end{cases}$$

On en déduit que

$$x = 2 \times 91 - 5 \times 90 = -268$$

est solution du système dont la solution générale est alors

$$x = -268 + 130k = 122 + 130\ell \text{ avec } \ell \in \mathbb{Z}$$

Exercice 15 : [énoncé]

Il existe $u, v \in \mathbb{Z}$ tels que $bu + b'v = 1$.

Soit $x = a'bu + ab'v$.

On a

$$x = a'bu + a - abu = a \pmod{b}$$

et

$$x = a' - a'b'v + ab'v = a' \pmod{b'}$$

donc x est solution.

Soit x' une autre solution. On a

$$x = x' \pmod{b}$$

et

$$x = x' \pmod{b'}$$

donc $b \mid (x' - x)$ et $b' \mid (x' - x)$.

Or $b \wedge b' = 1$ donc $bb' \mid (x' - x)$.

Inversement, soit x' tel que $bb' \mid x' - x$, on a bien

$$x' = x = a \pmod{b}$$

et

$$x' = x = a' \pmod{b'}$$

Exercice 16 : [énoncé]

Notons $x \in \mathbb{N}$ le montant du trésor. De part les hypothèses

$$\begin{cases} x \equiv 3 & \text{mod } 17 \\ x \equiv 4 & \text{mod } 11 \\ x \equiv 5 & \text{mod } 6 \end{cases}$$

On commence par résoudre le système

$$\begin{cases} x \equiv 3 & \text{mod } 17 \\ x \equiv 4 & \text{mod } 11 \end{cases}$$

$17 \wedge 11 = 1$ avec la relation de Bézout $2 \times 17 - 3 \times 11 = 1$. On a alors la solution particulière

$$x = 3 \times (-33) + 4 \times 34 = 37$$

et donc

$$\begin{cases} x \equiv 3 & \text{mod } 17 \\ x \equiv 4 & \text{mod } 11 \\ x \equiv 5 & \text{mod } 6 \end{cases} \iff \begin{cases} x \equiv 37 & \text{mod } 187 \\ x \equiv 5 & \text{mod } 6 \end{cases}$$

$187 \wedge 6 = 1$ avec la relation de Bézout $187 - 31 \times 6 = 1$. On a alors la solution particulière

$$x = 37 \times (-186) + 5 \times (187) = -5947$$

La solution générale du système est alors

$$x = -5947 + 1122k = 785 + 1122\ell \text{ avec } \ell \in \mathbb{Z}$$

Le cuisinier peut espérer empocher au moins 785 pièces d'or.

Exercice 17 : [énoncé]

Montrons que $\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $(\mathbb{R}, +, \times)$.

$$\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}, 1 \in \mathbb{Q}[\sqrt{d}].$$

Soient $x, y \in \mathbb{Q}[\sqrt{d}]$, on peut écrire $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$ avec $a, b, a', b' \in \mathbb{Q}$.

$$x - y = (a - a') + (b - b')\sqrt{d} \text{ avec } a - a', b - b' \in \mathbb{Q} \text{ donc } x - y \in \mathbb{Q}[\sqrt{d}].$$

$$xy = (aa' + bb'd) + (ab' + a'b)\sqrt{d} \text{ avec } aa' + bb'd, ab' + a'b \in \mathbb{Q} \text{ donc } xy \in \mathbb{Q}[\sqrt{d}].$$

Si $x \neq 0$ alors

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

avec

$$\frac{a}{a^2 - db^2}, \frac{b}{a^2 - db^2} \in \mathbb{Q}$$

Notons que, ici $a - b\sqrt{d} \neq 0$ car $\sqrt{d} \notin \mathbb{Q}$.

Finalement $\mathbb{Q}[\sqrt{d}]$ est un sous-corps de $(\mathbb{R}, +, \times)$ et c'est donc un corps.

Exercice 18 : [énoncé]

a) L'anneau $(A, +, \times)$ est intègre et $a \neq 0_A$ donc

$$\forall x, y \in A, ax = ay \implies x = y$$

L'application $\varphi: x \mapsto ax$ est une injection de A vers A , et l'ensemble A étant fini, cette injection est nécessairement bijective.

b) Soit $a \in A$ différent de 0_A . Par la surjectivité de l'application φ , il existe $b \in A$ tel que $ab = 1_A$. Aussi, on a

$$\varphi(ba) = a(ba) = (ab)a = a = \varphi(1_A)$$

Par l'injectivité de φ , on peut affirmer $ba = 1_A$. On peut alors conclure que a est inversible (et b est son inverse).

Exercice 19 : [énoncé]

($\Leftarrow$) tout élément non nul d'un corps est symétrisable donc régulier et n'est donc pas diviseur de zéro.

($\Rightarrow$) Supposons que A n'ait pas de diviseurs de zéros. Soit $a \in A$ tel que $a \neq 0$. Montrons que a est inversible. Considérons l'application $\varphi: A \rightarrow A$ définie par $\varphi(x) = ax$.

a n'étant pas diviseur de zéro, on démontre aisément que φ est injective, or A est fini donc φ est bijective. Par conséquent il existe $b \in A$ tel que $\varphi(b) = 1$ i.e. $ab = 1$. Ainsi a est inversible. Finalement A est un corps.

Exercice 20 : [énoncé]

En regroupant chaque x avec son inverse, lorsqu'ils sont distincts, on simplifie

$$\prod_{x \in \mathbb{K}^*} x = \prod_{x \in \mathbb{K}^*, x=x^{-1}} x$$

Or $x = x^{-1}$ équivaut à $x^2 = 1_{\mathbb{K}}$ et a pour solutions $1_{\mathbb{K}}$ et $-1_{\mathbb{K}}$.

Que celles-ci soient ou non distinctes, on obtient

$$\prod_{x \in \mathbb{K}^*} x = -1_{\mathbb{K}}$$

Notons que si le corps $\mathbb{K}$ est $\mathbb{Z}/2\mathbb{Z}$ (ou plus généralement un corps de caractéristique 2) alors $-1_{\mathbb{K}} = 1_{\mathbb{K}}$.

Exercice 21 : [énoncé]

a) Pour $x \in K \setminus \{0\}$, $f(x).f(x^{-1}) = f(x.x^{-1}) = f(1_K) = 1_L$ donc $f(x)$ est inversible et $f(x)^{-1} = f(x^{-1})$.

b) Si $f(x) = f(y)$ alors $f(x) - f(y) = f(x - y) = 0_L$. Or 0_L n'est pas inversible donc $x - y = 0_K$ i.e. $x = y$.

Ainsi f est morphisme injectif.

Exercice 22 : [\[énoncé\]](#)

- a) Il est clair que K est un sous-espace vectoriel de $\mathbb{R}$ et que la famille $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est $\mathbb{Q}$ -génératrice.
 Montrons qu'elle est libre en raisonnant par l'absurde.
 Supposons $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ avec $a, b, c, d \in \mathbb{Q}$ non tous nuls.
 Quitte à réduire au même dénominateur, on peut supposer $a, b, c, d \in \mathbb{Z}$ non tous nuls.
 Quitte à factoriser, on peut aussi supposer $\text{pgcd}(a, b, c, d) = 1$.
 On a $(a + b\sqrt{2})^2 = (c\sqrt{3} + d\sqrt{6})^2$ donc

$$a^2 + 2ab\sqrt{2} + 2b^2 = 3c^2 + 6cd\sqrt{2} + 6d^2.$$

Par l'irrationalité de $\sqrt{2}$ on parvient au système

$$\begin{cases} a^2 + 2b^2 = 3c^2 + 6d^2 \\ ab = 3cd \end{cases}$$

Par suite $3 \mid ab$ et $3 \mid a^2 + 2b^2$ donc $3 \mid a$ et $3 \mid b$.
 Ceci entraîne $3 \mid cd$ et $3 \mid c^2 + 2d^2$ donc $3 \mid c$ et $3 \mid d$.
 Ceci contredit $\text{pgcd}(a, b, c, d) = 1$.
 Ainsi la famille $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est $\mathbb{Q}$ -libre et c'est donc une $\mathbb{Q}$ -base de K .

- b) Sans peine, on vérifie que $\mathbb{K}$ est un sous-anneau de $\mathbb{R}$.
 Soit $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathbb{K}$ avec $a, b, c, d \in \mathbb{Q}$ non tous nuls.

$$\begin{aligned} \frac{1}{x} &= \frac{1}{(a + b\sqrt{2}) + (c\sqrt{3} + d\sqrt{6})} \\ &= \frac{a + b\sqrt{2} - (c\sqrt{3} + d\sqrt{6})}{(a^2 + 2b^2 - 3c^2 - 6d^2) + 2(ab - 3cd)\sqrt{2}} \\ &= \frac{a + b\sqrt{2} - (c\sqrt{3} + d\sqrt{6})}{\alpha + \beta\sqrt{2}} \end{aligned}$$

puis

$$\frac{1}{x} = \frac{(a + b\sqrt{2} - (c\sqrt{3} + d\sqrt{6}))(\alpha - \beta\sqrt{2})}{\alpha^2 - 2\beta^2} \in K$$

et donc K est un sous-corps de $\mathbb{R}$.

Notons que les quantités conjuguées par lesquelles on a ci-dessus multiplié ne sont pas nuls car x est non nul et la famille $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ est $\mathbb{Q}$ -libre.

Exercice 23 : [\[énoncé\]](#)

Il est facile de justifier que E est un $\mathbb{L}$ -espace vectoriel sous réserve de bien connaître la définition des espaces vectoriels et de souligner que qui peut le plus, peut le moins...

Soit $(\vec{e}_1, \dots, \vec{e}_n)$ une base de $\mathbb{K}$ -espace vectoriel E et $(\lambda_1, \dots, \lambda_p)$ une base du $\mathbb{L}$ -espace vectoriel $\mathbb{K}$.

Considérons la famille des $(\lambda_j \vec{e}_i)_{1 \leq i \leq n, 1 \leq j \leq p}$. Il est facile de justifier que celle-ci est une famille libre et génératrice du $\mathbb{L}$ -espace vectoriel E . Par suite E est de dimension finie $q = np$.

Exercice 24 : [\[énoncé\]](#)

Les inversibles dans $\mathbb{Z}/78\mathbb{Z}$ sont les classes associés aux entiers de $\{1, \dots, 78\}$ qui sont premiers avec $78 = 2 \times 3 \times 13$. Il suffit ensuite de dénombrer les multiples de 2, 3, 13 compris entre 1 et 78. On conclut qu'il y a 24 éléments inversible dans $\mathbb{Z}/78\mathbb{Z}$. On peut aussi calculer $\varphi(78) = 1 \times 2 \times 12 = 24$.

Exercice 25 : [\[énoncé\]](#)

Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, \times)$ sont les éléments représentés par un nombre premier avec n .

- a) $\varphi(p) = p - 1$. Etre premier avec p^α équivaut à être premier avec p i.e. à ne pas être divisible par p puisque $p \in \mathcal{P}$. Il y a $p^{\alpha-1}$ multiples de p compris entre 1 et p^α donc $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- b) Si $x = y \pmod{mn}$ alors $x = y \pmod{n}$ et $x = y \pmod{m}$ donc f est bien définie.
 $\varphi(\tilde{1}) = (\tilde{1}, \tilde{1})$ et si $a = x + y/xy \pmod{mn}$ alors $a = x + y/xy \pmod{n}$ donc φ est un morphisme d'anneaux.
 Si $f(\bar{x}) = f(\bar{y})$ alors $x = y \pmod{m}$ et $x = y \pmod{n}$ alors $m, n \mid y - x$ et puisque $m \wedge n = 1$ alors $mn \mid y - x$ donc $\bar{x} = \bar{y} \pmod{mn}$.
 f est injective puis bijective par l'égalité des cardinaux.
- c) Les inversibles de $\mathbb{Z}/mn\mathbb{Z}$ correspondent aux couples formés par un inversible de $\mathbb{Z}/n\mathbb{Z}$ et un inversible de $\mathbb{Z}/m\mathbb{Z}$. Par suite $\varphi(mn) = \varphi(m)\varphi(n)$.
- d) Si $n = \prod_{i=1}^N p_i^{\alpha_i}$ alors $\varphi(n) = \prod_{i=1}^N p_i^{\alpha_i-1}(p_i - 1)$.

Exercice 26 : [\[énoncé\]](#)

Notons $p_1, \dots, p_r$ les facteurs premiers de n . On sait

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

En ordonnant les $p_1, p_2, \dots, p_r$, on peut affirmer

$$\forall 1 \leq i \leq r, p_i \geq 1 + i$$

et donc

$$\left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \geq \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \dots \left(1 - \frac{1}{1+r}\right)$$

Par produit télescopique

$$\left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) > \frac{1}{2} \frac{2}{3} \dots \frac{r}{r+1} = \frac{1}{r+1}$$

Or on a aussi

$$n \geq p_1 \dots p_r \geq 2^r$$

et donc

$$r \leq \frac{n}{\ln 2}$$

On en déduit

$$\varphi(n) \geq \frac{n}{\frac{n}{\ln 2} + 1} = \frac{n \ln 2}{n + \ln 2}$$

Exercice 27 : [énoncé]

Si n possède un facteur premier impair p alors on peut écrire $n = p^\alpha m$ avec m premier avec p . On a alors

$$\varphi(n) = \varphi(p^\alpha) \varphi(m) = (p^\alpha - p^{\alpha-1}) \varphi(m)$$

Puisque $p^\alpha - p^{\alpha-1}$ est un nombre pair (par différence de deux impairs), on obtient que $\varphi(n)$ est pair.

Si n ne possède pas de facteurs premiers impairs, on peut écrire $n = 2^\alpha$ avec $\alpha \geq 2$ et alors $\varphi(n) = 2^{\alpha-1}$ est un nombre pair.

Exercice 28 : [énoncé]

Soit $f: x \mapsto ax$ de $(\mathbb{Z}/n\mathbb{Z})^*$ vers lui-même.

Cette application est bien définie, injective et finalement bijective par cardinalité.

Ainsi

$$\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x = \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} ax = a^{\varphi(n)} \prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$$

puis $a^{\varphi(n)} = 1$ car l'élément $\prod_{x \in (\mathbb{Z}/n\mathbb{Z})^*} x$ est inversible.

Exercice 29 : [énoncé]

a) Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.

Si $H = \{0\}$ alors $H = \langle n \rangle$.

Sinon, on peut introduire $a = \min \{k \in \mathbb{N}^* \mid \bar{k} \in H\}$.

La division euclidienne de n par a donne $n = qa + r$ d'où $\bar{r} \in H$ puis $r = 0$.

Ainsi $a \mid n$.

On a $\langle \bar{a} \rangle \subset H$ et par division euclidienne on montre $H \subset \langle \bar{a} \rangle$ d'où $\langle \bar{a} \rangle = H$.

b) Si a divise n , on observe que $\langle \bar{a} \rangle$ est de cardinal l'ordre n/a . Ainsi $\langle n/d \rangle$ est l'unique sous-groupe d'ordre d de $(\mathbb{Z}/n\mathbb{Z}, +)$.

c) Un élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$ est générateur d'un sous-groupe à d éléments donc générateur de $\langle n/d \rangle$. Inversement, tout générateur de $\langle n/d \rangle$ est élément d'ordre d de $\mathbb{Z}/n\mathbb{Z}$. Or $\langle n/d \rangle$ est cyclique d'ordre d donc isomorphe à $\mathbb{Z}/d\mathbb{Z}$ et possède ainsi $\varphi(d)$ générateurs. On peut donc affirmer que $\mathbb{Z}/n\mathbb{Z}$ possède exactement $\varphi(d)$ élément d'ordre d .

d) L'ordre d'un élément de $\mathbb{Z}/n\mathbb{Z}$ est cardinal d'un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ et donc diviseur de n . En dénombrant $\mathbb{Z}/n\mathbb{Z}$ selon l'ordre de ses éléments, on obtient

$$\sum_{d \mid n} \varphi(d) = n$$

Exercice 30 : [énoncé]

a) On peut écrire $n = dm$.

Si $k \in \llbracket 1; n \rrbracket$ vérifie $\text{pgcd}(k, n) = d$ alors d divise k et donc on peut écrire $k = d\ell$ avec $\ell \in \llbracket 1; m \rrbracket$.

De plus $\text{pgcd}(k, n) = \text{pgcd}(d\ell, dm) = d$ donne $\ell \wedge m = 1$.

Inversement, si $k = d\ell$ avec $\ell \in \llbracket 1; m \rrbracket$ et $\ell \wedge m = 1$ alors $k \in \llbracket 1; n \rrbracket$ et

$\text{pgcd}(k, n) = \text{pgcd}(d\ell, dm) = d$.

Ainsi, il y a autant de k cherché que de ℓ éléments de $\llbracket 1; m \rrbracket$ premiers avec m , à savoir $\varphi(m)$.

b) En partitionnant $\llbracket 1; n \rrbracket$ selon les valeurs possibles d du pgcd de ses éléments avec n (ce qui détermine un diviseur de n), on peut écrire

$$\llbracket 1; n \rrbracket = \bigcup_{d \mid n} \{k \in \llbracket 1; n \rrbracket \mid \text{pgcd}(k, n) = d\}$$

Puisque c'est une union d'ensembles deux à deux disjoints, on obtient

$$\text{Card} \llbracket 1; n \rrbracket = \sum_{d \mid n} \text{Card} \{k \in \llbracket 1; n \rrbracket \mid \text{pgcd}(k, n) = d\}$$

ce qui donne

$$n = \sum_{d|n} \varphi(n/d) = \sum_{\delta|n} \varphi(\delta)$$

en procédant pour l'étape finale à une réindexation de la somme.

Exercice 31 : [énoncé]

- a) Le coefficient d'indice (i, j) de la matrice DT est $\varphi(i)t_{i,j}$.
Le coefficient d'indice (i, j) de la matrice ${}^tTDT$ est

$$\sum_{k=1}^n t_{k,i} \varphi(k) t_{k,j} = \sum_{k|i \text{ et } k|j} \varphi(k)$$

Or les diviseurs communs à i et j sont les diviseurs de $\text{pgcd}(i, j)$ et donc

$$\sum_{k=1}^n t_{k,i} \varphi(k) t_{k,j} = \sum_{k|\text{pgcd}(i,j)} \varphi(k) = \text{pgcd}(i, j)$$

- b) La matrice T est triangulaire supérieure à coefficients diagonaux égaux à 1 donc $\det T = 1$ puis

$$\det S = \det D = \prod_{k=1}^n \varphi(k)$$

Ce résultat a été publié par H. J. S. Smith en 1875.

Exercice 32 : [énoncé]

- a) L'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de cardinal $\varphi(n)$.
b) $k \binom{p}{k} = p \binom{p-1}{k-1}$ donc $p \mid k \binom{p}{k}$ or $p \wedge k = 1$ donc $p \mid \binom{p}{k}$.
c) Posons $d = (n-1) \wedge \varphi(n)$. $d = (n-1)u + \varphi(n)v$ donc $a^d = 1 \quad [n]$. Or $d \mid n-1$ donc nécessairement $d = n-1$. Par suite $n-1 \mid \varphi(n)$ puis $\varphi(n) = n-1$ ce qui entraîne que n est premier.

Exercice 33 : [énoncé]

Notons $N = a^n - 1$. On a

$$a^n \equiv 1 \pmod{N} \text{ et } \forall 1 \leq k < n, a^k \not\equiv 1 \pmod{N}$$

On en déduit que a est inversible dans l'anneau $\mathbb{Z}/N\mathbb{Z}$ et que a est un élément d'ordre exactement n dans le groupe $(U(\mathbb{Z}/N\mathbb{Z}), \times)$. Or ce groupe est de cardinal $\varphi(N)$ et puisque l'ordre des éléments divise le cardinal du groupe, on obtient que n divise $\varphi(N)$.

Exercice 34 : [énoncé]

Soit I un idéal d'un corps $\mathbb{K}$. Si $I \neq \{0\}$ alors I contient un élément x non nul. Puisque $x \in I$ et $x^{-1} \in \mathbb{K}$ on a $1 = xx^{-1} \in I$ puis pour tout $y \in \mathbb{K}$, $y = 1 \times y \in I$ et finalement $I = \mathbb{K}$. Les idéaux de $\mathbb{K}$ sont donc $\{0\}$ et $\mathbb{K}$.

Exercice 35 : [énoncé]

Soit I un idéal d'un sous-anneau A de $(\mathbb{Q}, +, \times)$.

$I \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc de la forme $d\mathbb{Z}$ pour un certain $d \in \mathbb{N}$.

Vérifions qu'alors I est l'idéal engendré par d .

Puisque $d \in I$, on a déjà par absorption $(d) = dA \subset I$.

Inversement, soit $x \in I$. On peut écrire $x = p/q$ avec $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$ premiers entre eux.

On a alors $qx = p \in \mathbb{Z}$ et, par addition, $qx = x + \dots + x \in I$. Ainsi

$qx \in I \cap \mathbb{Z} = d\mathbb{Z}$ ce qui permet d'écrire $x = dk/q$.

Il reste à montrer que k/q est élément du sous-anneau A pour pouvoir conclure $x \in (d) = dA$.

Puisque A est un sous-anneau de $(\mathbb{Q}, +, \times)$, c'est un sous-groupe additif ce qui entraîne

$$\forall a \in A, \forall k \in \mathbb{Z}, k.a \in A$$

Sachant les entiers p et q premiers entre eux, on peut écrire

$$pu + qv = 1 \text{ avec } u, v \in \mathbb{Z}$$

et alors

$$\frac{1}{q} = \frac{p}{q}u + v = u.x + v.1$$

Sachant que 1 et x sont éléments de A , $1/q$ l'est aussi et enfin $k/q = k.(1/q) \in A$.

Exercice 36 : [énoncé]

- a) Il suffit de vérifier les axiomes définissant un sous-anneau...

- b) Soit I un idéal de $\mathbb{D}$. L'intersection $I \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il existe $a \in \mathbb{Z}$ vérifiant

$$I \cap \mathbb{Z} = a\mathbb{Z}$$

Puisque $a \in I$, on a $a\mathbb{D} \subset I$.

Inversement, soit $x \in I$. On peut écrire

$$x = \frac{p}{10^n} \text{ avec } p \in \mathbb{Z} \text{ et } n \in \mathbb{N}$$

On a alors $10^n x \in I$ par absorption donc $p \in I \cap \mathbb{Z}$. On en déduit $a \mid p$ puis $x \in a\mathbb{D}$.

Finalement, $I = a\mathbb{D}$

Exercice 37 : [énoncé]

- a) $I_1 \subset \mathbb{Z}$ et $0 \in I_1$ car $(0, 0) = 0_{\mathbb{Z}^2} \in I$.
Soient $x, x' \in I_1$. On a $(x + x', 0) = (x, 0) + (x', 0) \in I$ donc $x + x' \in I_1$.
Soit de plus $a \in \mathbb{Z}$. On a $(ax, 0) = (a, 1234) \times (x, 0) \in I$ donc $ax \in I_1$.
Ainsi I_1 est un idéal de $(\mathbb{Z}, +, \times)$ et de façon analogue I_2 aussi.
- b) Soit $(x, y) \in I_1 \times I_2$. On a $(x, 0) \in I$ et $(0, y) \in I$ donc
 $(x, y) = (x, 0) + (0, y) \in I$.
Ainsi $I_1 \times I_2 \subset I$.
Inversement soit $(x, y) \in I$.
On a $(x, 0) = (x, y) \times (1, 0) \in I$ donc $x \in I_1$. De même $y \in I_2$ et donc
 $(x, y) \in I_1 \times I_2$.
Finalement $I \subset I_1 \times I_2$ puis $I = I_1 \times I_2$.
- c) Les idéaux de $(\mathbb{Z}, +, \times)$ sont de la forme $n\mathbb{Z}$ donc il existe $a, b \in \mathbb{Z}$ tels que
 $I_1 = a\mathbb{Z}$ et $I_2 = b\mathbb{Z}$.
L'idéal I apparaît alors comme étant celui engendré par $x = (a, b)$

$$I = x\mathbb{Z}^2 = \{(ak, b\ell) \mid k, \ell \in \mathbb{Z}\}$$

Exercice 38 : [énoncé]

$N \subset A$, $0_A \in N$ donc $N \neq \emptyset$. Pour $x, y \in N$, il existe $n, m \in \mathbb{N}^*$ tel que
 $x^n = y^m = 0_A$.

Par la formule du binôme,

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

Pour $k \geq n$, $x^k = 0_A$ et pour $k \leq n-1$, $y^{n+m-1-k} = 0_A$. Dans les deux cas
 $x^k y^{n+m-1-k} = 0_A$ et donc $(x + y)^{n+m-1} = 0_A$. Par suite $x + y \in N$.
Enfin pour $a \in A$ et $x \in N$, $ax \in N$ car $(ax)^n = a^n x^n$.

Exercice 39 : [énoncé]

- a) Par définition $R(I) \subset A$
 $0^1 = 0 \in I$ donc $0 \in R(I)$.
Soient $x, y \in R(I)$, il existe $n, m \in \mathbb{N}^*$ tels que $x^n, y^m \in I$.
On a alors

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

car les premiers termes de la somme sont dans I puisque $y^{n+m-1-k} \in I$ et les suivants le sont aussi car $x^k \in I$

donc $x + y \in R(I)$.

Soit de plus $a \in A$. On a $(ax)^n = a^n x^n \in I$ donc $ax \in R(I)$.

Ainsi $R(I)$ est un idéal de A .

Soit $x \in I$, on a $x^1 \in I$ donc $x \in R(I)$.

- b) Si $x \in R(I \cap J)$ alors il existe $n \in \mathbb{N}^*$ tel que $x^n \in I \cap J$.
On a alors $x^n \in I$ donc $x \in R(I)$ et de même $x \in R(J)$. Ainsi

$$R(I \cap J) \subset R(I) \cap R(J)$$

Soit $x \in R(I) \cap R(J)$. Il existe $n, m \in \mathbb{N}^*$ tel que $x^n \in I$ et $x^m \in J$.

Pour $N = \max(m, n)$, on a par absorption $x^N \in I$ et $x^N \in J$ donc
 $x^N \in I \cap J$. Ainsi $x \in R(I \cap J)$ et on peut affirmer

$$R(I \cap J) \supset R(I) \cap R(J)$$

puis l'égalité.

Puisque $I \subset I + J$, on a clairement $R(I) \subset R(I + J)$. De même

$R(J) \subset R(I + J)$.

Enfin $R(I + J)$ étant stable par somme $R(I) + R(J) \subset R(I + J)$.

- c) Si n a un facteur carré d^2 avec $d \geq 2$.

Posons $k \in \mathbb{Z}$ tel que $n = d^2 k$.

On a $dk \notin n\mathbb{Z}$ et $(dk)^2 = nk \in n\mathbb{Z}$ donc $dk \in R(n\mathbb{Z})$. Ainsi $R(n\mathbb{Z}) \neq n\mathbb{Z}$.

Si n n'a pas de facteurs carrés alors n s'écrit $n = p_1 p_2 \dots p_m$ avec $p_1, \dots, p_m$ nombres premiers deux à deux distincts.

Pour tout $x \in R(n\mathbb{Z})$, il existe $k \in \mathbb{N}^*$ tel que $x^k \in n\mathbb{Z}$.

Tous les $p_1, \dots, p_m$ sont alors facteurs premiers de x^k donc de x et par conséquent n divise x .

Finalement $R(n\mathbb{Z}) \subset n\mathbb{Z}$ puis $R(n\mathbb{Z}) = n\mathbb{Z}$ car l'autre inclusion est toujours vraie.

Exercice 40 : [énoncé]

- a) sans difficultés.
- b) Pour tout $x \in A$, $x = xe + x(1 - e)$ avec $xe \in I$ et $x - xe \in J$. Par suite $I + J = A$.
Si $xe \in J$ alors $xe = xe^2 = 0$ donc $I \cap J = \{0\}$.
- c) L'inclusion $(K \cap I) + (K \cap J) \subset K$ est immédiate. L'inclusion réciproque provient de l'écriture $x = xe + x(1 - e)$.

Exercice 41 : [énoncé]

- a) Pour $p \in \mathcal{P}$, $p\mathbb{Z}$ est un idéal premier. En effet on sait que $p\mathbb{Z}$ est un idéal et en vertu du lemme d'Euclide : $xy \in p\mathbb{Z} \implies x \in p\mathbb{Z}$ ou $y \in p\mathbb{Z}$.
- b) Même principe
- c) Supposons $J \cap K = I$.
Si $J = I$ ok.
Sinon il existe $a \in J$ tel que $a \notin I$. Pour tout $b \in K$, $ab \in J \cap K$ d'où $ab \in I$ puis $b \in I$ car $a \notin I$. Ainsi $K \subset I$. D'autre part $I = J \cap K \subset K$ donc $I = K$.
- d) $I = \{0\}$ est un idéal premier donc

$$xy = 0 \implies x = 0 \text{ ou } y = 0$$

Soit $x \in A$ tel que $x \neq 0$. x^2A est premier et $x^2 \in x^2A$ donc $x \in x^2A$.

Ainsi il existe $y \in A$ tel que $x = x^2y$ et puisque $x \neq 0$, $xy = 1$.

Ainsi A est un corps.

Exercice 42 : [énoncé]

Une suite croissante (I_n) d'idéaux de $\mathbb{Z}$ se détermine par une suite d'entiers naturels (a_n) vérifiant $I_n = a_n\mathbb{Z}$ et $a_{n+1} \mid a_n$. Si pour tout $n \in \mathbb{N}$, $I_n = \{0\}$ alors la suite (I_n) est stationnaire.

Sinon à partir d'un certain rang $I_n \neq \{0\}$ et la relation $a_{n+1} \mid a_n$ entraîne $a_{n+1} \leq a_n$. La suite d'entiers naturels (a_n) est décroissante et donc stationnaire. Il en est de même pour (I_n) .

Ce résultat se généralise à $\mathbb{K}[X]$ en travaillant avec une suite de polynômes unitaires (P_n) vérifiant $P_{n+1} \mid P_n$ ce qui permet d'affirmer en cas de non nullité $\deg P_{n+1} \leq \deg P_n$ puis $(\deg P_n)$ stationnaire, puis encore (P_n) stationnaire et enfin (I_n) stationnaire.

Exercice 43 : [énoncé]

Notons qu'un sous-anneau de $\mathbb{Q}$ possédant 1 contient nécessairement $\mathbb{Z}$.

- a) Par égalité de Bézout, on peut écrire $pu + qv = 1$ avec $u, v \in \mathbb{Z}$. Si $\frac{p}{q} \in A$ alors

$$\frac{1}{q} = u \frac{p}{q} + v.1 \in A$$

- b) $I \cap \mathbb{Z}$ est un sous-groupe de $(\mathbb{Z}, +)$ donc il est de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.
Puisque $I \neq \{0\}$, il existe $p/q \in I$ non nul et par absorption, $p = q.p/q \in I \cap \mathbb{Z}$ avec $p \neq 0$. Par suite $I \cap \mathbb{Z} \neq \{0\}$ et donc $n \in \mathbb{N}^*$.
Puisque $n \in I$, on peut affirmer par absorption que $nA \subset I$.
Inversement, pour $p/q \in I$ avec $p \wedge q = 1$ on a $1/q \in A$ et $p \in n\mathbb{Z}$ donc $p/q \in nA$. Ainsi $I = nA$.
- c) On peut vérifier que Z_p est un sous-anneau de $\mathbb{Q}$.
Pour $x = a/b \in \mathbb{Q}^*$ avec $a \wedge b = 1$. Si $p \nmid b$ alors $p \wedge b = 1$ et $x \in Z_p$. Sinon $p \mid b$ et donc $p \nmid a$ d'où l'on tire $1/x \in Z_p$.
- d) Soit J un idéal strict de A . J ne contient pas d'éléments inversibles de A car sinon il devrait contenir 1 et donc être égal à A .
Ainsi J est inclus dans I . De plus, on peut montrer que I est un idéal de A .
En effet $I \subset A$ et $0 \in I$.
Soient $a \in A$ et $x \in I$.
Cas $a = 0$: $ax = 0 \in I$.
Cas $a \neq 0$: Supposons $(ax)^{-1} \in A$ alors $a^{-1}x^{-1} \in A$ et donc $x^{-1} = a(a^{-1}x^{-1}) \in A$ ce qui est exclu. Ainsi, $(ax)^{-1} \notin A$ et donc $ax \in I$.
Soient $x, y \in I$. Montrons que $x + y \in I$.
Cas $x = 0$, $y = 0$ ou $x + y = 0$: c'est immédiat.
Cas $x \neq 0$, $y \neq 0$ et $x + y \neq 0$: On a $(x + y)^{-1}(x + y) = 1$ donc

$$(x + y)^{-1}(1 + x^{-1}y) = x^{-1} \text{ et } (x + y)^{-1}(1 + xy^{-1}) = y^{-1} (*)$$

Par l'hypothèse de départ, l'un au moins des deux éléments $x^{-1}y$ ou $xy^{-1} = (x^{-1}y)^{-1}$ appartient à A .

Par opérations dans A à l'aide des relations (*), si $(x + y)^{-1} \in A$ alors x^{-1} ou y^{-1} appartient à A ce qui est exclu. Ainsi $(x + y)^{-1} \notin A$ et donc $x + y \in I$.

Finalement I est un idéal de A .

Par suite, il existe $n \in \mathbb{N}$, vérifiant $I = nA$.

Si $n = 0$ alors $I = \{0\}$ et alors $A = \mathbb{Q}$ car pour tout $x \in \mathbb{Q}^*$, x ou $1/x \in A$ et dans les deux cas $x \in A$ car $I = \{0\}$.

Si $n = 1$ alors $I = A$ ce qui est absurde car $1 \in A$ est inversible.

Nécessairement $n \geq 2$. Si $n = qr$ avec $2 \leq q, r \leq n-1$ alors puisque $1/n \notin A$, au moins l'un des éléments $1/q$ et $1/r \notin A$. Quitte à échanger, on peut supposer $1/q \notin A$. qA est alors un idéal strict de A donc $qA \subset I$. Inversement $I \subset qA$ puisque n est multiple de q . Ainsi, si n n'est pas premier alors il existe un facteur non trivial q de n tel que $I = nA = qA$. Quitte à recommencer, on peut se ramener à un nombre premier p .

Finalement, il existe un nombre premier p vérifiant $I = pA$.

Montrons qu'alors $A = Z_p$.

Soit $x \in A$. On peut écrire $x = a/b$ avec $a \wedge b = 1$. On sait qu'alors $1/b \in A$ donc si $p \mid b$ alors $1/p \in A$ ce qui est absurde car $p \in I$. Ainsi $p \nmid b$ et puisque p est premier, $p \wedge b = 1$. Ainsi $A \subset Z_p$.

Soit $x \in Z_p$, $x = a/b$ avec $b \wedge p = 1$. Si $x \notin A$ alors $x \neq 0$ et $1/x = b/a \in A$ puis $b/a \in I \subset pA$ ce qui entraîne, après étude arithmétique, $p \mid b$ et est absurde.

Ainsi $Z_p \subset A$ puis finalement $Z_p = A$.

Exercice 44 : [énoncé]

a) Facile.

b) J_p idéal de Z_p : facile.

Soit I un idéal de Z_p . On suppose $I \not\subset J_p$, il existe donc un élément $a/b \in I$ vérifiant $a/b \notin J_p$. Par suite p ne divise ni a , ni b et donc $b/a \in Z_p$ de sorte que a/b est inversible dans Z_p . Ainsi l'idéal contient un élément inversible, donc par absorption il possède 1 et enfin il est égal à Z_p .

c) Pour $k \in \mathbb{N}$, posons J_{p^k} l'ensemble des a/b où $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$, $p^k \mid a$ et p ne divise pas b . On vérifie aisément que J_{p^k} est un idéal de Z_p .

Soit I un idéal de Z_p . Posons

$k = \max \{ \ell / \forall x \in I, \exists (a, b) \in \mathbb{Z} \times \mathbb{N}^*, x = a/b, p^\ell \mid a, p \nmid b \}$.

On a évidemment $I \subset J_{p^k}$.

Inversement, il existe $x = a/b \in I$ avec $p^k \mid a$, p^{k+1} ne divise pas a et p ne divise pas b .

On peut écrire $a = p^k a'$ avec p qui ne divise pas a' , et donc on peut écrire $x = p^k x'$ avec $x' = a'/b$ inversible dans Z_p . Par suite tout élément de J_{p^k} peut s'écrire xy avec $y \in Z_p$ et donc appartient à I . Ainsi $J_{p^k} \subset I$ puis $=$. Finalement les idéaux de Z_p sont les J_{p^k} avec $k \in \mathbb{N}$.

Exercice 45 : [énoncé]

a) $I \subset A$ et $0 \in I$.

Soient $a \in A$ et $x \in I$

Si $a = 0$ alors $ax = 0 \in I$.

Pour $a \neq 0$, supposons $(ax)^{-1} \in A$.

On a alors $a^{-1}x^{-1} \in A$ et donc $x^{-1} = a(a^{-1}x^{-1}) \in A$ ce qui est exclu.

Nécessairement $(ax)^{-1} \notin A$ et donc $ax \in I$.

Soient $x, y \in I$. Montrons que $x + y \in I$.

Si $x = 0$, $y = 0$ ou $x + y = 0$, c'est immédiat. Sinon :

On a $(x + y)^{-1}(x + y) = 1$ donc

$$(x + y)^{-1}(1 + x^{-1}y) = x^{-1} \text{ et } (x + y)^{-1}(1 + xy^{-1}) = y^{-1} (*)$$

Par l'hypothèse de départ, l'un au moins des deux éléments $x^{-1}y$ ou $xy^{-1} = (x^{-1}y)^{-1}$ appartient à A .

Par opérations dans A à l'aide des relations (*), si $(x + y)^{-1} \in A$ alors x^{-1} ou y^{-1} appartient à A ce qui est exclu. Ainsi $(x + y)^{-1} \notin A$ et donc $x + y \in I$.

Finalement I est un idéal de A .

b) Soit J un idéal de A distinct de A .

Pour tout $x \in J$, si $x^{-1} \in A$ alors par absorption $1 = xx^{-1} \in J$ et donc $J = A$ ce qui est exclu.

On en déduit que $x^{-1} \notin A$ et donc $x \in I$. Ainsi $J \subset I$.

Exercice 46 : [énoncé]

Soit $x \in A$ avec $x \neq 0_A$. Il suffit d'établir que x est inversible pour conclure. Pour chaque $n \in \mathbb{N}$, $x^n A$ est un idéal. Puisque l'anneau A ne possède qu'un nombre fini d'idéaux, il existe $p < q \in \mathbb{N}$ tels que $x^p A = x^q A$. En particulier, puisque $x^p \in x^p A$, il existe $a \in A$ tel que

$$x^p = x^q a$$

On a alors

$$x^p(1_A - x^{q-p}a) = 0_A$$

L'anneau A étant intègre et sachant $x \neq 0_A$, on a nécessairement

$$x^{q-p}a = 1_A$$

On en déduit que x est inversible avec

$$x^{-1} = x^{q-p-1}a$$

Exercice 47 : [énoncé]

- a) $3x + 5 = 0 \iff x + 5 = 0 \iff x = 5$ car l'inverse de 3 dans $\mathbb{Z}/10\mathbb{Z}$ est 7.
 b) Il suffit de tester les entiers 0, 1, 2, 3, 4. 1 et 3 conviennent. Les solutions sont 1, 3, 5, 7.
 c) $x^2 + 2x + 2 = 0 \iff x^2 + 2x - 3 = 0 \iff (x - 1)(x + 3) = 0$ donc les solutions sont 1 et -3 .

Exercice 48 : [énoncé]

Les solutions du système sont solutions de l'équation

$$z^2 - 4z + 10 = 0 \pmod{11}$$

Or

$$z^2 - 4z + 10 = z^2 + 7z + 10 = (z + 2)(z + 5)$$

donc les solutions sont $-2 = 9$ et $-5 = 6$. On obtient comme solutions, les couples (9, 6) et (6, 9).

Exercice 49 : [énoncé]

Notons $\bar{x}$ les éléments de $\mathbb{Z}/n\mathbb{Z}$ et $\hat{x}$ ceux de $\mathbb{Z}/m\mathbb{Z}$.

Posons $d = \text{pgcd}(n, m)$. On peut écrire

$$n = dn' \text{ et } m = dm' \text{ avec } n' \wedge m' = 1$$

Soit φ un morphisme de $(\mathbb{Z}/n\mathbb{Z}, +)$ vers $(\mathbb{Z}/m\mathbb{Z}, +)$.

On a

$$n.\varphi(\bar{1}) = \varphi(n.\bar{1}) = \varphi(\bar{n}) = \varphi(\bar{0}) = \hat{0}$$

Si l'on note $\varphi(\bar{1}) = \hat{k}$, on a donc $m \mid nk$ d'où $m' \mid n'k$ puis $m' \mid k$ car m' et n' sont premiers entre eux.

Ainsi $\varphi(\bar{1}) = \widehat{m'a}$ pour un certain $a \in \mathbb{Z}$ puis alors

$$\forall x \in \mathbb{Z}, \varphi(\bar{x}) = \widehat{m'ax}$$

Inversement, si l'on considère pour $a \in \mathbb{Z}$, l'application $\varphi: \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ donnée par

$$\forall x \in \mathbb{Z}, \varphi(\bar{x}) = \widehat{m'ax}$$

on vérifie que φ est définie sans ambiguïté car

$$\bar{x} = \bar{y} \implies m = m'd \mid m'(x - y) \implies \widehat{m'ax} = \widehat{m'ay}$$

On observe aussi que φ est bien un morphisme de groupe.

Exercice 50 : [énoncé]

On note $\bar{x}$ la classe d'un entier x dans $\mathbb{Z}/n\mathbb{Z}$.

Soit H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$.

On peut introduire

$$a = \min \{k > 0, \bar{k} \in H\}$$

car toute partie non vide de $\mathbb{N}$ possède un plus petit élément.

Considérons alors $\langle \bar{a} \rangle$ le groupe engendré par la classe de a . On peut décrire ce groupe

$$\langle \bar{a} \rangle = \{q.\bar{a} \mid q \in \mathbb{Z}\}$$

C'est le plus petit sous-groupe contenant l'élément $\bar{a}$ car il est inclus dans tout sous-groupe contenant cet élément. Par conséquent $\langle \bar{a} \rangle$ est inclus dans H .

Montrons qu'il y a en fait égalité.

Soit $\bar{k} \in H$. Par division euclidienne de k par a , on écrit

$$k = aq + r \text{ avec } r \in \{0, \dots, a - 1\}$$

On a alors $\bar{k} = q.\bar{a} + \bar{r}$ et donc, par opérations dans le groupe H , on obtient $\bar{r} = \bar{k} - q.\bar{a} \in H$. On ne peut alors avoir $r > 0$ car cela contredirait la définition de a . Il reste donc $r = 0$ et par conséquent $\bar{k} = q.\bar{a} \in \langle \bar{a} \rangle$

Finalement

$$H = \langle \bar{a} \rangle$$

De plus, en appliquant le raisonnement précédent avec $k = n$ (ce qui est possible car $\bar{n} = \bar{0} \in H$), on obtient que a est un diviseur de n .

Inversement, considérons un diviseur a de n . On peut écrire

$$n = aq \text{ avec } q \in \mathbb{N}^*$$

et on peut alors décrire les éléments du groupe engendré par $\bar{a}$, ce sont

$$\bar{0}, \bar{a}, 2.\bar{a}, \dots, (q - 1).\bar{a}$$

On constate alors que les diviseurs de n déterminent des sous-groupes deux à deux distincts de $(\mathbb{Z}/n\mathbb{Z}, +)$.

On peut conclure qu'il y a autant de sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ que de diviseurs positifs de n .

Exercice 51 : [énoncé]

Par l'égalité de Bézout,

$$uk - (p - 1)v = 1$$

Considérons alors l'application $\psi: \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$ définie par $\psi(x) = x^u$.

On observe

$$\psi(\varphi(x)) = x^{ku} = x \times x^{(p-1)v}$$

Si $x = 0$ alors $\psi(\varphi(x)) = 0 = x$.

Si $x \neq 0$ alors par le petit théorème de Fermat, $x^{p-1} = 1$ puis

$$\psi(\varphi(x)) = x \times 1^v = x$$

Ainsi $\psi \circ \varphi = \text{Id}$ et de même $\varphi \circ \psi = \text{Id}$. On peut conclure que φ est bijective.

Exercice 52 : [énoncé]

Considérons $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Il est clair que l'application $x \mapsto ax$ est une permutation de $\mathbb{Z}/p\mathbb{Z}$ donc

$$a^k \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (ax)^k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$$

puis

$$(a^k - 1) \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = 0$$

S'il existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ tel que $a^k \neq 1$ alors

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = 0$$

Sinon,

$$\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k = 0 + \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^*} 1 = p - 1 = -1$$

Exercice 53 : [énoncé]

On a

$$\sum_{k=1}^p \bar{k} = \sum_{k=1}^p k = \frac{p(p+1)}{2}$$

Si $p = 2$ alors

$$\sum_{k=1}^p \bar{k} = \bar{1}$$

Si $p \geq 3$ alors $(p+1)/2$ est un entier et donc

$$\sum_{k=1}^p \bar{k} = \bar{p} \times \frac{(p+1)}{2} = \bar{0}$$

On a

$$\sum_{k=1}^p \bar{k}^2 = \sum_{k=1}^p k^2 = \frac{p(p+1)(2p+1)}{6}$$

Si $p = 2$ alors

$$\sum_{k=1}^p \bar{k}^2 = \bar{1}$$

Si $p = 3$ alors

$$\sum_{k=1}^p \bar{k}^2 = \bar{1}^2 + \bar{2}^2 = \bar{2}$$

Si $p \geq 5$ alors $(p+1)(2p+1)$ est divisible par 6.

En effet, $p+1$ est pair donc $(p+1)(2p+1)$ aussi.

De plus, sur les trois nombres consécutifs

$$2p, (2p+1), (2p+2)$$

l'un est divisible par 3. Ce ne peut être $2p$ et si $2p+2$ est divisible par 3 alors $p+1$ l'est aussi. Par suite $(p+1)(2p+1)$ est divisible par 3.

Ainsi

$$\sum_{k=1}^p \bar{k}^2 = \bar{p} \times \frac{(p+1)(2p+1)}{6} = \bar{0}$$

Exercice 54 : [énoncé]

- Dans le corps $\mathbb{Z}/p\mathbb{Z}$ l'équation $x^2 = 1$ n'a que pour seules solutions 1 et $-1 = p-1 \pmod{p}$ (éventuellement confondues quand $p = 2$)
- Dans le produit $(p-1)! = 1 \times 2 \times \dots \times p-1$ où l'on retrouve tous les éléments inversibles de $\mathbb{Z}/p\mathbb{Z}$ chaque élément, sauf 1 et $p-1$, peut être apparié à son inverse (qui lui est distincts). Par suite $(p-1)! = p-1 = -1 \pmod{p}$.
- Dans $(\mathbb{Z}/n\mathbb{Z}, +, \times)$, $1 \times 2 \times \dots \times (n-1) = -1$ donc les éléments $1, 2, \dots, n-1$ sont tous inversibles. Il en découle que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps et donc n est premier.

Exercice 55 : [énoncé]

- Les inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont les $\bar{k}$ avec $k \wedge 8 = 1$. Ce sont donc les éléments $\bar{1}, \bar{3}, \bar{5}$ et $\bar{7}$.
L'ensemble des inversibles d'un anneau est un groupe multiplicatif.

- b) Le groupe $(\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \times)$ vérifie la propriété $x^2 = 1$ pour tout x élément de celui-ci. Ce groupe n'est donc pas isomorphe au groupe cyclique $(\mathbb{Z}/4\mathbb{Z}, +)$ qui constitue donc un autre exemple de groupe de cardinal 4. En fait le groupe $(\{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}, \times)$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

Exercice 56 : [énoncé]

- a) Considérons l'application $\varphi: x \mapsto x^2$ dans $\mathbb{Z}/p\mathbb{Z}$.
 Dans le corps $\mathbb{Z}/p\mathbb{Z}$: $\varphi(x) = \varphi(y) \iff x = \pm y$.
 Dans $\text{Im } \varphi$, seul 0 possède un seul antécédent, les autres éléments possèdent deux antécédents distincts. Par suite $\text{Card } \mathbb{Z}/p\mathbb{Z} = 1 + 2(\text{Card Im } \varphi - 1)$ donc il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.
- b) D'une part, dans le produit $(p-1)!$ calculé dans $\mathbb{Z}/p\mathbb{Z}$, tous les termes qui ne sont pas égaux à leur inverse se simplifient. Il ne reste que les termes égaux à leur inverse qui sont les solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/p\mathbb{Z}$ à savoir 1 et -1 . Ainsi $(p-1)! = -1$ dans $\mathbb{Z}/p\mathbb{Z}$.
 D'autre part, en posant $n = \frac{p-1}{2}$,
 $(p-1)! = 1 \times \dots \times n \times (n+1) \times \dots \times (p-1) =$
 $1 \times \dots \times n \times (-n) \times \dots \times (-1) = (-1)^n (n!)^2$.
 Or $p \equiv 1 \pmod{4}$ donc n est pair et $-1 = (p-1)! = (n!)^2$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$.
- c) Si -1 est un carré de $\mathbb{Z}/p\mathbb{Z}$, alors l'application $x \mapsto -x$ définit une involution sur l'ensemble des carrés de $\mathbb{Z}/p\mathbb{Z}$. Puisque seul 0 est point fixe de cette application, on peut affirmer qu'il y a un nombre impair de carrés dans $\mathbb{Z}/p\mathbb{Z}$.
 Or si $p \equiv 3 \pmod{4}$, $(p+1)/2$ est un entier pair, -1 ne peut donc être un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 57 : [énoncé]

Le groupe $(G, \cdot)$ est abélien. En effet, pour tout $x \in G$, on a $x^{-1} = x$ donc, pour $x, y \in G$, $(xy)^{-1} = xy$. Or $(xy)^{-1} = y^{-1}x^{-1} = yx$ donc $xy = yx$.
 Pour $\bar{0}, \bar{1} \in \mathbb{Z}/2\mathbb{Z}$ et $x \in G$, posons

$$\bar{0}.x = e \text{ et } \bar{1}.x = x$$

On vérifie qu'on définit alors un produit extérieur sur G munissant le groupe abélien $(G, \cdot)$ d'une structure de $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel. En effet, pour $(x, y) \in G^2$ et $(\lambda, \mu) \in (\mathbb{Z}/2\mathbb{Z})^2$ on a

$$(\lambda + \mu).x = \lambda.x + \mu.x, \lambda.(x + y) = \lambda.x + \lambda.y, \lambda.(\mu.x) = (\lambda\mu).x \text{ et } \bar{1}.x = x$$

De plus, cet espace est de dimension finie car $\text{Card } G < +\infty$, il est donc isomorphe à l'espace $((\mathbb{Z}/2\mathbb{Z})^n, +, \cdot)$ pour un certain $n \in \mathbb{N}^*$.
 En particulier, le groupe $(G, \cdot)$ est isomorphe à $((\mathbb{Z}/2\mathbb{Z})^n, +)$.

Exercice 58 : [énoncé]

Si $p = 2$: il y a deux carrés dans $\mathbb{Z}/2\mathbb{Z}$.

Si $p \geq 3$, considérons l'application $\varphi: x \mapsto x^2$ dans $\mathbb{Z}/p\mathbb{Z}$.

Dans le corps $\mathbb{Z}/p\mathbb{Z}$: $\varphi(x) = \varphi(y) \iff x = \pm y$.

Dans $\text{Im } \varphi$, seul 0 possède un seul antécédent, les autres éléments possèdent deux antécédents distincts. Par suite $\text{Card } \mathbb{Z}/p\mathbb{Z} = 1 + 2(\text{Card Im } \varphi - 1)$ donc il y a $\frac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 59 : [énoncé]

Les inversibles sont obtenus à partir des nombres premiers avec 20

$$G = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

3 est un élément d'ordre 4 dans $(G, \times)$ avec

$$\langle 3 \rangle = \{1, 3, 9, 7\}$$

et 11 est un élément d'ordre 2 n'appartenant pas à $\langle 3 \rangle$.

Le morphisme $\varphi: \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \rightarrow G$ donné par

$$\varphi(k, \ell) = 11^k \times 3^\ell$$

est bien défini et injectif par les arguments qui précèdent.
 Par cardinalité, c'est un isomorphisme.

Exercice 60 : [énoncé]

Pour $a \in (\mathbb{Z}/p\mathbb{Z})^*$, l'application $x \mapsto ax$ est une permutation de $(\mathbb{Z}/p\mathbb{Z})^*$.

Le calcul

$$\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x = \prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} ax = a^{p-1} \prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x$$

donne alors $a^{p-1} = 1$ car $\prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x \neq 0$.

Exercice 61 : [énoncé]

On peut écrire

$$M(a, b, c) = aI + bJ + cK$$

avec

$$I = M(1, 0, 0), J = M(0, 1, 0) \text{ et } K = M(0, 0, 1) = J^2$$

Ainsi, $E = \text{Vect}(I, J, K)$ est un sous-espace vectoriel de dimension 3 de $\mathcal{M}_3(\mathbb{R})$ (car (I, J, K) est clairement une famille libre).

Aussi

$$M(a, b, c)M(a', b', c') = (aa' + bc' + cb')I + (ab' + a'b + cc')J + (ac' + a'c + bb')K$$

Donc E est une sous algèbre (visiblement commutative) de $\mathcal{M}_3(\mathbb{R})$.

Exercice 62 : [énoncé]

- a) Soit a un élément non nul de $\mathbb{K}$. L'application $\varphi: x \mapsto ax$ est $\mathbb{R}$ -linéaire de $\mathbb{K}$ vers $\mathbb{K}$ et son noyau est réduit à $\{0\}$ car l'algèbre $\mathbb{K}$ est intègre. Puisque $\mathbb{K}$ est un $\mathbb{R}$ -espace vectoriel de dimension finie, l'endomorphisme φ est bijectif et il existe donc $b \in \mathbb{K}$ vérifiant $ab = 1$. Puisque

$$\varphi(ba) = a(ba) = (ab)a = a = \varphi(1)$$

on a aussi $ba = 1$ et donc a est inversible d'inverse b .

- b) Puisque $1 \neq 0$, si la famille $(1, a)$ était liée alors $a \in \mathbb{R} \cdot 1 = \mathbb{R}$ ce qui est exclu ; on peut donc affirmer que la famille $(1, a)$ est libre. Puisque la $\mathbb{R}$ -algèbre $\mathcal{A}$ est de dimension n , on peut affirmer que la famille $(1, a, a^2, \dots, a^n)$ est liée car formée de $n + 1$ vecteurs. Il existe donc un polynôme non nul $P \in \mathbb{R}_n[X]$ tel que $P(a) = 0$. Or ce polynôme se décompose en un produit de facteurs de degrés 1 ou 2. Puisque les facteurs de degré 1 n'annulent pas a et puisque l'algèbre est intègre, il existe un polynôme de degré 2 annulant a . On en déduit que la famille $(1, a, a^2)$ est liée.
- c) Plus exactement avec ce qui précède, on peut affirmer qu'il existe $\alpha, \beta \in \mathbb{R}$ tel que

$$a^2 + \alpha a + \beta = 0 \text{ avec } \Delta = \alpha^2 - 4\beta < 0$$

On a alors

$$\left(a + \frac{\alpha}{2}\right)^2 = \frac{\alpha^2 - 4\beta}{4}$$

et on obtient donc $i^2 = -1$ en prenant

$$i = \frac{2a + \alpha}{\sqrt{4\beta - \alpha^2}}$$

- d) Par l'absurde, supposons $n = \dim \mathbb{K} > 2$.

Il existe $a, b \in \mathbb{K}$ tels que $(1, a, b)$ soit libre.

Comme ci-dessus, on peut alors introduire $i \in \text{Vect}(1, a)$ et $j \in \text{Vect}(1, b)$ tels que

$$i^2 = -1 = j^2$$

On a alors par commutativité

$$(i - j)(i + j) = 0$$

et l'intégrité de $\mathbb{K}$ entraîne $i = j$ ou $i = -j$. Dans un cas comme dans l'autre, on obtient

$$1, a, b \in \text{Vect}(1, i)$$

ce qui contredit la liberté de la famille $(1, a, b)$.

On en déduit $n = 2$. Il est alors facile d'observer que $\mathbb{K}$ est isomorphe à $\mathbb{C}$.

Exercice 63 : [énoncé]

- a) Supposons $M^2 \in \mathcal{A}$. $\mathcal{A}$ et $\text{Vect}(I_n)$ étant supplémentaires dans $\mathcal{M}_n(\mathbb{C})$, on peut écrire $M = A + \lambda I_n$ avec $A \in \mathcal{A}$. On a alors $M^2 = A^2 + 2\lambda AI_n + \lambda^2 I_n$ d'où l'on tire $\lambda^2 I_n \in \mathcal{A}$ puis $\lambda = 0$ ce qui donne $M \in \mathcal{A}$. Pour $i \neq j$, $E_{i,j}^2 = 0 \in \mathcal{A}$ donc $E_{i,j} \in \mathcal{A}$ puis $E_{i,i} = E_{i,j} \times E_{j,i} \in \mathcal{A}$. Par suite $I_n = E_{1,1} + \dots + E_{n,n} \in \mathcal{A}$. Absurde.
- b) Formons une équation de l'hyperplan $\mathcal{A}$ de la forme $ax + by + cz + dt = 0$ en la matrice inconnue $M = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ avec $(a, b, c, d) \neq (0, 0, 0, 0)$. Cette équation peut se réécrire $\text{tr}(AM) = 0$ avec $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$. Puisque $I_2 \in \mathcal{A}$, on a $\text{tr} A = 0$. Soit λ une valeur propre de A . Si $\lambda \neq 0$ alors $-\lambda$ est aussi valeur propre de A et donc A est diagonalisable via une matrice P . On observe alors que les matrices M de $\mathcal{A}$ sont celles telles que $P^{-1}MP$ a ses coefficients diagonaux égaux. Mais alors pour $M = P \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} P^{-1}$ et $N = P \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} P^{-1}$ on a $M, N \in \mathcal{A}$ alors que $MN \notin \mathcal{A}$.

Si $\lambda = 0$ alors A est trigonalisable en $\begin{pmatrix} 0 & \alpha \\ 0 & 0 \end{pmatrix}$ avec $\alpha \neq 0$ via une matrice P .

On observe alors que les matrices M de $\mathcal{A}$ sont celles telles que $P^{-1}MP$ est triangulaire supérieure. L'application $M \mapsto P^{-1}MP$ est un isomorphisme comme voulu.