

1 Anneaux et idéaux

Exercice 1 ★★ Anneau des entiers de Gauss –

On appelle ensemble des entiers de Gauss noté $\mathbb{Z}[i]$ l'ensemble des nombres complexes qui s'écrivent $a + ib$, avec a et $b \in \mathbb{Z}$.

1. Démontrer que $\mathbb{Z}[i]$ est un anneau.

2. Pour tout nombre complexe z , on note $N(z) = z\bar{z}$.

Démontrer que, pour tous nombres complexes z et z' , $N(z)N(z') = N(zz')$. Démontrer que, pour tout entier de Gauss z , $N(z)$ est un entier naturel. Soit z un entier de Gauss inversible. Dédurre des questions précédentes que $N(z) = 1$. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

3. Démontrer que, pour tous nombres complexes z et z' , $N(z)N(z') = N(zz')$.

4. Démontrer que, pour tout entier de Gauss z , $N(z)$ est un entier naturel.

5. Soit z un entier de Gauss inversible. Dédurre des questions précédentes que $N(z) = 1$.

6. Quels sont les éléments inversibles de $\mathbb{Z}[i]$?

[Indication ▼](#) [Correction ▼](#)

[3220]

Exercice 2 ★★ Centre d'un anneau –

Soit A un anneau. On appelle centre de A et l'on note $C(A)$ l'ensemble des éléments $a \in A$ tels que, pour tout $b \in A$, $ab = ba$. Démontrer que $C(A)$ est un sous-anneau de A .

[Indication ▼](#) [Correction ▼](#)

[3222]

Exercice 3 ★ Idéal dans un anneau de suites –

Soit A l'ensemble des suites réelles et B l'ensemble des suites réelles bornées. On admet que A et B sont deux anneaux pour l'addition et le produit des suites. Soit I l'ensemble des suites réelles qui convergent vers 0. Est-ce que I est un idéal de A ? de B ?

[Indication ▼](#) [Correction ▼](#)

[3333]

Exercice 4 ★ Annulateur –

Soit $(A, +, \times)$ un anneau commutatif et M une partie de A . On appelle annulateur de M l'ensemble des $x \in A$ tels que $xy = 0$ pour tout $y \in M$. Démontrer que l'annulateur de M est un idéal de $(A, +, \times)$.

[Indication ▼](#) [Correction ▼](#)

[1385]

Exercice 5 ★★ Exemple de sous-anneau et d'idéal dans un anneau de fonctions –

Soit $A = \mathcal{C}([0, 1], \mathbb{R})$, $B = \mathcal{C}^1([0, 1], \mathbb{R})$ et $I = \{f \in A : f(0) = 0\}$.

1. Démontrer que A est un anneau pour les opérations somme et produit de fonctions.

2. Démontrer que B est un sous-anneau de A . B est-il un idéal de A ?

3. Démontrer que I est un idéal de A . I est-il un sous-anneau de A ?

4. Démontrer que I est un idéal maximal de A , c'est-à-dire que si J est un idéal de A tel que $I \subset J \subset A$, alors $J = I$ ou $J = A$.

[Indication ▼](#) [Correction ▼](#)

[3334]

Exercice 6 ★★ Peu d'idéaux : c'est un corps! –

Soit A un anneau commutatif.

1. On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A . Démontrer que A est un corps.

2. On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.

[Indication ▼](#) [Correction ▼](#)

[1363]

Exercice 7 ★★ Suites croissantes d'idéaux de $\mathbb{K}[X]$ –

Soit (I_n) une suite croissante d'idéaux de $\mathbb{K}[X]$, où \mathbb{K} est un corps. Démontrer que la suite (I_n) est stationnaire.

[Indication ▼](#) [Correction ▼](#)

[1386]

Exercice 8 ★★★ Produit et Somme –

Soit $(A, +, \times)$ un anneau commutatif. Si I et J sont deux idéaux de A , on note

$$\begin{aligned} I+J &= \{i+j; i \in I, j \in J\} \\ I.J &= \{i_1 j_1 + \dots + i_n j_n; n \geq 1, i_k \in I, j_k \in J\} \end{aligned}$$

On dit que deux idéaux I et J sont étrangers si $I+J=A$.

1. Montrer que $I+J$ et IJ sont encore des idéaux de A .
2. Montrer que $I.J \subset I \cap J$.
3. Montrer que $(I+J).(I \cap J) \subset I.J$.
4. Montrer que si I et J sont étrangers, alors $I.J = I \cap J$.

[Indication ▼](#) [Correction ▼](#)

[1366]

Exercice 9 ★★★ Idéaux de \mathbb{Z}_p . –

Soit p un nombre premier. On note

$$\mathbb{Z}_p = \left\{ x = \frac{m}{n}; (m, n) \in \mathbb{Z} \times \mathbb{N}^*, p \wedge n = 1 \right\}.$$

1. Vérifier que \mathbb{Z}_p est un sous-anneau de $(\mathbb{Q}, +, \times)$.
2. Soit $k \geq 0$. On note

$$J_{p^k} = \left\{ \frac{m}{n}; (m, n) \in \mathbb{Z} \times \mathbb{N}^*, p \wedge n = 1, p^k | m \right\}.$$

Vérifier que J_{p^k} est un idéal de \mathbb{Z}_p .

3. Réciproquement, montrer que si I est un idéal de \mathbb{Z}_p non réduit à $\{0\}$, il existe $k \geq 0$ tel que $I = J_{p^k}$.

[Indication ▼](#) [Correction ▼](#)

[1364]

Exercice 10 ★★★★★ Radical d'un idéal –

Soit A un anneau commutatif (unitaire). Si I est un idéal de A , on appelle radical de I l'ensemble $\sqrt{I} = \{x \in A; \exists n \geq 1, x^n \in I\}$.

1. Montrer que \sqrt{I} est un idéal de A .
2. Soient I, J deux idéaux de A et $p \geq 1$. Montrer que

$$\sqrt{I.J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}, \sqrt{\sqrt{I}} = \sqrt{I} \text{ et } \sqrt{I^p} = \sqrt{I}.$$

3. Si $A = \mathbb{Z}$ et $I = k\mathbb{Z}$, $k \geq 1$, déterminer le radical de I .

[Indication ▼](#) [Correction ▼](#)

[1367]

Exercice 11 ★★★★★ Idéaux d'un anneau produit –

Soit A et B deux anneaux commutatifs et soit $K \subset A \times B$. Démontrer que K est un idéal de $A \times B$ si et seulement si $K = I \times J$, où I est un idéal de A et J est un idéal de B .

[Indication ▼](#) [Correction ▼](#)

[3065]

2 Anneau $\mathbb{Z}/n\mathbb{Z}$

Exercice 12 ★ Inversibles de $\mathbb{Z}/n\mathbb{Z}$. –

1. Est-ce que $\overline{18}$ est inversible dans $\mathbb{Z}/49\mathbb{Z}$? Si oui, quel est son inverse ?
2. Est-ce que $\overline{42}$ est inversible dans $\mathbb{Z}/135\mathbb{Z}$? Si oui, quel est son inverse ?

[Indication ▼](#) [Correction ▼](#)

[2281]

Exercice 13 ★ Équations linéaires –

Résoudre les équations suivantes :

1. $\overline{7}x = \overline{2}$ dans $\mathbb{Z}/37\mathbb{Z}$;
2. $\overline{10}x = \overline{6}$ dans $\mathbb{Z}/34\mathbb{Z}$;
3. $\overline{10}x = \overline{5}$ dans $\mathbb{Z}/34\mathbb{Z}$.

[Indication ▼](#) [Correction ▼](#)

[717]

Exercice 14 ★★ Systèmes d'équations –

Résoudre les systèmes d'équations suivants :

1. $\begin{cases} \overline{2}x + \overline{3}y = \overline{4} \\ \overline{3}x + \overline{2}y = \overline{5} \end{cases}$ dans $\mathbb{Z}/13\mathbb{Z}$.
2. $\begin{cases} \overline{4}x + \overline{7}y = \overline{1} \\ \overline{5}x + \overline{2}y = \overline{2} \end{cases}$ dans $\mathbb{Z}/18\mathbb{Z}$.
3. $\begin{cases} \overline{2}x + \overline{3}y = \overline{1} \\ \overline{3}x + \overline{4}y = \overline{2} \end{cases}$ dans $\mathbb{Z}/18\mathbb{Z}$.

[Indication ▼](#) [Correction ▼](#)

[3332]

Exercice 15 ★★★ Équations du second degré –

1. Déterminer un élément \overline{k} de $\mathbb{Z}/13\mathbb{Z}$ tel que, pour tout $x \in \mathbb{Z}/13\mathbb{Z}$, $x^2 + x + \overline{7} = (x + \overline{7})^2 - \overline{k}^2$. En déduire les solutions de $x^2 + x + \overline{7} = \overline{0}$ dans $\mathbb{Z}/13\mathbb{Z}$.
2. Déterminer un élément \overline{k} de $\mathbb{Z}/13\mathbb{Z}$ tel que, pour tout $x \in \mathbb{Z}/13\mathbb{Z}$, $x^2 + x + \overline{7} = (x + \overline{7})^2 - \overline{k}^2$.
3. En déduire les solutions de $x^2 + x + \overline{7} = \overline{0}$ dans $\mathbb{Z}/13\mathbb{Z}$.
4. Quels sont les éléments de $\mathbb{Z}/12\mathbb{Z}$ dont le carré vaut $\overline{1}$? En déduire que l'équation $x^2 - \overline{4}x + \overline{3} = \overline{0}$ admet exactement quatre solutions dans $\mathbb{Z}/12\mathbb{Z}$, que l'on déterminera.
5. Quels sont les éléments de $\mathbb{Z}/12\mathbb{Z}$ dont le carré vaut $\overline{1}$?
6. En déduire que l'équation $x^2 - \overline{4}x + \overline{3} = \overline{0}$ admet exactement quatre solutions dans $\mathbb{Z}/12\mathbb{Z}$, que l'on déterminera.

[Indication ▼](#) [Correction ▼](#)

[720]

Exercice 16 ★ Inversibles de $\mathbb{Z}/8\mathbb{Z}$ –

Déterminer les inversibles de $\mathbb{Z}/8\mathbb{Z}$. Le groupe des inversibles $(\mathbb{Z}/8\mathbb{Z})^*$ est-il cyclique ?

[Indication ▼](#) [Correction ▼](#)

[3336]

Exercice 17 ★★★ Contre-exemple au théorème chinois –

Les groupes $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ et $(\mathbb{Z}/2\mathbb{Z})^3$ sont-ils isomorphes ?

[Indication ▼](#) [Correction ▼](#)

[719]

Exercice 18 ★★★★★ Carrés de $\mathbb{Z}/n\mathbb{Z}$ –

Dans cet exercice, on s'intéresse au nombre de solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$, où $n \geq 2$.

1. Quel est le nombre de solutions pour $n = p^\alpha$, où $\alpha \geq 1$ et p est un nombre premier impair ?
2. Quel est le nombre de solutions pour $n = 2, 4$?

3. Quel est le nombre de solutions pour $n = 2^\alpha$, $\alpha \geq 3$?
4. Quel est le nombre de solutions pour une valeur quelconque de n ?

[Indication ▼](#) [Correction ▼](#)

[725]

Exercice 19 ★★★★★ Un groupe d'inversibles non cyclique –

Soit $n \geq 3$ un entier.

1. Soit a un entier impair. Montrer que $a^{2^{n-2}} \equiv 1 \pmod{2^n}$.
2. Le groupe $(\mathbb{Z}/(2^n\mathbb{Z}))^*$ est-il cyclique ?

[Indication ▼](#) [Correction ▼](#)

[727]

Exercice 20 ★★★★★ Sous-groupes de $(\mathbb{Z}/20\mathbb{Z})^*$ –

Soit $G = (\mathbb{Z}/20\mathbb{Z})^*$ le groupe des éléments inversibles de $\mathbb{Z}/20\mathbb{Z}$.

1. Donner la liste de tous les éléments de G .
2. Pour tout $a \in G$, déterminer le sous groupe $\langle a \rangle$ engendré par a .
3. Déterminer un ensemble minimal de générateurs de (G, \cdot) .
4. (G, \cdot) est-il un groupe cyclique ?
5. Déterminer tous les sous-groupes de G et, pour chaque sous-groupe, préciser un ensemble de générateurs.
6. Parmi les sous-groupes de (G, \cdot) , lesquels sont isomorphes à un groupe additif $(\mathbb{Z}/m\mathbb{Z}, +)$?

[Indication ▼](#) [Correction ▼](#)

[2193]

Exercice 21 ★★★★★ Ordre d'éléments dans le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$ et divisibilité –

Le but de cet exercice est de montrer qu'il n'existe pas d'entier $n \geq 2$ tel que n divise $2^n - 1$. On raisonne par l'absurde et on suppose qu'un tel entier n existe. On note p le plus petit diviseur premier de n .

1. Montrer que $p > 2$.
2. On note m l'ordre de la classe de 2 dans $(\mathbb{Z}/p\mathbb{Z})^*$.
Montrer que $m|p-1$. Montrer que $m|n$. Conclure.
3. Montrer que $m|p-1$.
4. Montrer que $m|n$.
5. Conclure.

[Indication ▼](#) [Correction ▼](#)

[724]

3 Anneaux de polynômes

Exercice 22 ★ Déterminer toutes les racines sachant que... –

Soit $P(X) = X^4 - 4X^3 + 4X^2 + X - 2$.

1. Déterminer deux racines évidentes a et b de P .
2. Effectuer la division euclidienne de P par $(X-a)(X-b)$.
3. En déduire toutes les racines de P .

[Indication ▼](#) [Correction ▼](#)

[2978]

Exercice 23 ★ Décomposer ! –

Décomposer le polynôme suivant en produit d'irréductibles de $\mathbb{R}[X]$:

$$P(X) = 2X^4 + X^2 - 3.$$

[Indication ▼](#) [Correction ▼](#)

[2509]

Exercice 24 ★★★★★ Polynôme irréductible sur $\mathbb{Q}[X]$ –

Montrer que les polynômes suivants sont irréductibles dans $\mathbb{Q}[X]$:

$$P = X^3 + 3X^2 + 2 \text{ et } Q = X^4 + 1.$$

[Indication ▼](#) [Correction ▼](#)

[3341]

4 Algèbre

Exercice 25 ★ Algèbre des matrices qui commutent avec une autre –

Soit $A \in \mathcal{M}_n(\mathbb{R})$. On note $C = \{M \in \mathcal{M}_n(\mathbb{R}); AM = MA\}$. Montrer que C est une algèbre.

[Indication ▼](#) [Correction ▼](#)

[1375]

Exercice 26 ★ Une algèbre de matrices –

Pour $a, b, c \in \mathbb{R}$, on note

$$M(a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix}$$

et $E = \{M(a, b, c); a, b, c \in \mathbb{R}\}$. Démontrer que E est une algèbre, et en donner une base en tant qu'espace vectoriel.

[Indication ▼](#) [Correction ▼](#)

[1376]

Exercice 27 ★★★★★ Algèbres commutatives intègres de dimension finie sur \mathbb{R} . –

Soit A une algèbre commutative intègre de dimension finie $n \geq 2$ sur \mathbb{R} . On identifie \mathbb{R} avec $\mathbb{R}.1$, où 1 est l'élément neutre de A pour la multiplication.

1. Démontrer que tout $a \in A$ non-nul est inversible.
2. Soit $a \in A$ et non dans $\mathbb{R} = \text{vect}(1)$. Prouver que la famille $(1, a)$ est libre, tandis que la famille $(1, a, a^2)$ est liée.

3. En déduire l'existence de $i \in \text{vect}(1, a)$ tel que $i^2 = -1$.

4. En déduire que $\dim(A) = 2$.

5. En déduire que A est isomorphe à \mathbb{C} .

[Indication ▼](#) [Correction ▼](#)

[1377]

Indication pour l'exercice 1 ▲

1. C'est un sous-anneau d'un anneau bien connu.
2. Utiliser une propriété bien connue du module.

Quand est-ce que le produit de deux entiers naturels peut-il être égal à 1 ? Quand est-ce que la somme de deux entiers naturels peut-elle être égale à 1 ?

3. Utiliser une propriété bien connue du module.
 - 4.
 5. Quand est-ce que le produit de deux entiers naturels peut-il être égal à 1 ?
 6. Quand est-ce que la somme de deux entiers naturels peut-elle être égale à 1 ?
-

Indication pour l'exercice 2 ▲

Il suffit de vérifier les hypothèses du théorème de caractérisation des sous-anneaux.

Indication pour l'exercice 3 ▲

Pour démontrer que I n'est pas un idéal de A , on pourra considérer dans A une suite (x_n) qui tend vers $+\infty$, puis la suite $(1/x_n)$ qui est dans I .

Indication pour l'exercice 4 ▲

Indication pour l'exercice 5 ▲

- 1.
- 2.
- 3.
4. Considérer un idéal J tel que $I \subset J \subset A$ et $I \neq J$. Fixer $g \in J \setminus I$, puis considérer, pour tout $f \in A$, la fonction

$$h = f - \frac{f(0)}{g(0)}g.$$

Indication pour l'exercice 6 ▲

1. Prendre $x \in A$ et considérer l'idéal engendré par x .
 2. Prendre $x \in A$ et considérer les idéaux $I_n = x^n A$.
-

Indication pour l'exercice 7 ▲

Raisonner sur le degré du générateur de (I_n) .

Indication pour l'exercice 8 ▲

1. Il suffit d'écrire la définition ?
 2. $i \in I, j \in J$ implique $ij \in I$ par exemple.
 - 3.
 4. Ecrire $x = 1.x$.
-

Indication pour l'exercice 9 ▲

- 1.
 - 2.
 3. Poser $k = \max\{l \geq 0; \forall x \in I, \exists (m, n) \in \mathbb{Z} \times \mathbb{N}^*, x = \frac{m}{n}, p^l | m, p \wedge n = 1\}$ et prouver que $p^k \in I$.
-

Indication pour l'exercice 10 ▲

1. Pour montrer la stabilité par la loi $+$, on pourra utiliser la formule du binôme à une bonne puissance de $(x+y)$.
 2. Pour les trois premières égalités, raisonner par inclusions successives $(1 \subset 2 \subset 3 \subset 1)$ fonctionne. On pourra remarquer que si $x^n \in I$ et $x^m \in J$, alors $x^{n+m} \in I.J$.
 3. Décomposer k en produits de facteurs premiers $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ et prouver que $\exists n \geq 1, k|x^n$ est équivalent à $x \in (p_1 \dots p_r)\mathbb{Z}$.
-

Indication pour l'exercice 11 ▲

Partant de K , on pourra poser $I = p_A(K)$ et $J = p_B(K)$ où p_A et p_B sont les projections canoniques. Pour montrer que $I \times J \subset K$, on pourra utiliser que si $(x, b) \in K$, alors $(x, 0) \in K$ par la structure d'idéal de K .

Indication pour l'exercice 12 ▲

Indication pour l'exercice 13 ▲

1. Chercher l'inverse de $\bar{7}$ dans $\mathbb{Z}/37\mathbb{Z}$, en résolvant une équation de Bezout.
 2. Traduire cette équation en terme de congruences.
 - 3.
-

Indication pour l'exercice 14 ▲

Procéder comme pour un système ordinaire (par exemple, par combinaison).

Indication pour l'exercice 15 ▲

1. Développer $(x + \bar{7})^2$. Factoriser en utilisant une identité remarquable.
 2. Développer $(x + \bar{7})^2$.
 3. Factoriser en utilisant une identité remarquable.
 4. Faire un tableau calculant tous les carrés dans $\mathbb{Z}/12\mathbb{Z}$. Commencer par mettre le trinôme sous forme canonique, puis utiliser le résultat de la question précédente.
 5. Faire un tableau calculant tous les carrés dans $\mathbb{Z}/12\mathbb{Z}$.
 6. Commencer par mettre le trinôme sous forme canonique, puis utiliser le résultat de la question précédente.
-

Indication pour l'exercice 16 ▲

Indication pour l'exercice 17 ▲

Penser en terme d'ordre des éléments.

Indication pour l'exercice 18 ▲

1. Montrer, en utilisant un argument de divisibilité, que 1 et -1 sont les seules solutions.
 2. On peut faire une étude exhaustive.
 3. Procéder comme à la première question.
 4. Utiliser le théorème chinois.
-

Indication pour l'exercice 19 ▲

1. Procéder par récurrence sur n .
 2. Combien y-a-t-il d'éléments dans $(\mathbb{Z}/(2^n\mathbb{Z}))^*$?
-

Indication pour l'exercice 20 ▲

-
1. Il y a un critère...
 2. Prendre un élément et toutes ses puissances, jusqu'à tomber sur 1.
 - 3.
 4. La question 2. donne la réponse !
 5. Quels sont les sous-groupes engendrés par deux éléments d'ordre 2 ?
 - 6.
-

Indication pour l'exercice 21 ▲

1. $2^n - 1$ est impair.
 2. Appliquer le théorème de Lagrange. On a $2^n = 1$ dans $\mathbb{Z}/n\mathbb{Z}$. $(p-1) \wedge n = 1$.
 3. Appliquer le théorème de Lagrange.
 4. On a $2^n = 1$ dans $\mathbb{Z}/n\mathbb{Z}$.
 5. $(p-1) \wedge n = 1$.
-

Indication pour l'exercice 22 ▲

1. Calculer $P(1)$ et $P(2)$.
 - 2.
 3. Résoudre également $x^2 + x + 1 = 0$.
-

Indication pour l'exercice 23 ▲

Commencer par décomposer $Q(X) = 2X^2 + X - 3$.

Indication pour l'exercice 24 ▲

Pour P il suffit de vérifier qu'il ne possède pas de racines rationnelles. Ceci peut se faire par l'absurde. Pour Q on peut vérifier qu'il ne possède pas de racines rationnelles, et aussi qu'il est impossible qu'il se factorise en produit de deux polynômes de degré 2 de $\mathbb{Q}[X]$.

Indication pour l'exercice 25 ▲

Démontrer que c'est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$.

Indication pour l'exercice 26 ▲

Démontrer que E est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$.

Indication pour l'exercice 27 ▲

1. Démontrer que l'application (linéaire) $x \mapsto ax$ est bijective, pour tout $a \in A$, $a \neq 0$.
 2. Puisque A est de dimension finie, il existe un polynôme P tel que $P(a) = 0$. Factoriser alors P .
 3. Partir du polynôme précédent. . . et essayer de trouver -1 comme un carré.
 4. Reasonner par l'absurde. Trouver $j \neq i$ tel que $j^2 = -1$ et conclure...
 - 5.
-

Correction de l'exercice 1 ▲

1. On va prouver que $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} . En effet, $1 = 1 + 0i \in \mathbb{Z}[i]$; Soit $z = a + ib$ et $z' = a' + ib' \in \mathbb{Z}[i]$. Alors

$$z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i]$$

(puisque $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$) et

$$zz' = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i]$$

(puisque $aa' - bb' \in \mathbb{Z}$ et $ab' + a'b \in \mathbb{Z}$).

2. $1 = 1 + 0i \in \mathbb{Z}[i]$;

3. Soit $z = a + ib$ et $z' = a' + ib' \in \mathbb{Z}[i]$. Alors

$$z - z' = (a - a') + i(b - b') \in \mathbb{Z}[i]$$

(puisque $a - a' \in \mathbb{Z}$ et $b - b' \in \mathbb{Z}$) et

$$zz' = (aa' - bb') + i(ab' + a'b) \in \mathbb{Z}[i]$$

(puisque $aa' - bb' \in \mathbb{Z}$ et $ab' + a'b \in \mathbb{Z}$).

4. On remarque que $N(z) = |z|^2$. Puisque $|zz'| = |z| \cdot |z'|$, en mettant au carré cette égalité, on a le résultat demandé. Si $z = a + ib$, alors $N(z) = a^2 + b^2$ et a^2, b^2 sont des entiers naturels, donc $N(z)$ aussi. Soit z un entier de Gauss inversible et soit z' son inverse. Alors on sait que $zz' = 1$ et donc $N(z) \times N(z') = 1$. Or le produit de deux entiers naturels est égal à 1 si et seulement si ces deux entiers sont égaux à 1. Donc $N(z) = 1$. Soit $z = a + ib \in \mathbb{Z}[i]$ inversible. Alors $N(z) = 1$, et donc $a^2 + b^2 = 1$. Or, puisque a^2 et b^2 sont des entiers naturels, ceci n'est possible que dans quatre cas : $(a, b) = (1, 0)$, $(a, b) = (-1, 0)$, $(a, b) = (0, 1)$, et $(a, b) = (0, -1)$. Réciproquement, il est facile de vérifier que $1, -1, i$ et $-i$ sont inversibles dans $\mathbb{Z}[i]$, d'inverse respectif $1, -1, -i$ et i . Les éléments inversibles de $\mathbb{Z}[i]$ sont donc $1, -1, i$ et $-i$.

5. On remarque que $N(z) = |z|^2$. Puisque $|zz'| = |z| \cdot |z'|$, en mettant au carré cette égalité, on a le résultat demandé.

6. Si $z = a + ib$, alors $N(z) = a^2 + b^2$ et a^2, b^2 sont des entiers naturels, donc $N(z)$ aussi.

7. Soit z un entier de Gauss inversible et soit z' son inverse. Alors on sait que $zz' = 1$ et donc $N(z) \times N(z') = 1$. Or le produit de deux entiers naturels est égal à 1 si et seulement si ces deux entiers sont égaux à 1. Donc $N(z) = 1$.

8. Soit $z = a + ib \in \mathbb{Z}[i]$ inversible. Alors $N(z) = 1$, et donc $a^2 + b^2 = 1$. Or, puisque a^2 et b^2 sont des entiers naturels, ceci n'est possible que dans quatre cas : $(a, b) = (1, 0)$, $(a, b) = (-1, 0)$, $(a, b) = (0, 1)$, et $(a, b) = (0, -1)$. Réciproquement, il est facile de vérifier que $1, -1, i$ et $-i$ sont inversibles dans $\mathbb{Z}[i]$, d'inverse respectif $1, -1, -i$ et i . Les éléments inversibles de $\mathbb{Z}[i]$ sont donc $1, -1, i$ et $-i$.

Correction de l'exercice 2 ▲

Il suffit de vérifier le théorème de caractérisation des sous-anneaux.

$1 \in C(A)$, puisque $1a = a1 = a$ pour tout $a \in A$. Soit $a, a' \in C(A)$ et soit $b \in A$. Alors

$$(a - a')b = ab - a'b = ba - ba' = b(a - a')$$

(on a utilisé deux fois la distributivité) et donc $a - a' \in C(A)$. Soit $a, a' \in C(A)$ et soit $b \in A$. Alors

$$(aa')b = a(a'b) = a(ba') = (ab)a' = (ba)a' = b(aa')$$

(on a utilisé plusieurs fois l'associativité) et donc $aa' \in C(A)$.

Correction de l'exercice 3 ▲

On commence par remarquer que $(I, +)$ est un sous-groupe de $(A, +)$. En effet, la suite nulle est dans I , et si (u_n) et (v_n) sont dans I , alors $(u_n + v_n)$ est dans I puisque la somme de deux suites qui convergent vers 0 converge elle-même vers 0. On va ensuite prouver que I n'est pas un idéal de A . Considérons en effet la suite (x_n) telle que $x_n = 2^n$ et la suite (u_n) telle que $u_n = 2^{-n}$. Alors $(x_n) \in A$, $(u_n) \in I$ et le produit $(x_n u_n)$ n'est pas dans I puisque c'est la suite identiquement égale à 1. En revanche, I est un idéal de B . En effet, le produit d'une

suite bornée avec une suite qui tend vers 0 est une suite qui tend vers 0. Donc si $(x_n) \in B$ et $(u_n) \in I$, alors $(x_n u_n) \in I$.

Correction de l'exercice 4 ▲

Notons I cet ensemble. Il suffit d'appliquer la définition. En effet, on remarque que $0 \in I$. De plus, prenons $u, v \in I$ et $a \in A$. Alors, pour tout $y \in M$, on a

$$(u - v)y = uy - vy = 0$$

et

$$(au)y = a(uy) = 0.$$

Ainsi, $u - v$ et au sont dans I qui est un idéal.

Correction de l'exercice 5 ▲

1. La fonction $\mathbf{1}_{[0,1]}$ est une fonction continue, la différence et le produit de deux fonctions continues est une fonction continue : A est donc un sous-anneau de l'anneau $\mathcal{F}([0, 1], \mathbb{R})$ des fonctions de $[0, 1]$ dans \mathbb{R} .

2. La même démonstration en remplaçant "continue" par "de classe \mathcal{C}^1 " prouve que B est un sous-anneau de A . En revanche, B n'est pas un idéal de A . En effet, si on considère $f(x) = 1$ et $g(x) = |x - 1/2|$, alors $f \in B$, $g \in A$ et le produit gf n'est pas élément de B .

3. Puisque la fonction $\mathbf{1}_{[0,1]}$ n'est pas dans I , I n'est pas un sous-anneau de A . De plus, soit $f, g \in I$ et $h \in A$. Alors il est facile de vérifier que $f - g$, $f \times g$ et $f \times h$ sont dans I puisque

$$f(0) - g(0) = f(0)g(0) = f(0)h(0) = 0.$$

Ainsi, I est un idéal de A .

4. Soit J un idéal de A tel que $I \subset J \subset A$. Supposons que $I \neq J$, donc qu'il existe $g \in J \setminus I$. En particulier, $g(0) \neq 0$. Soit $f \in A$ et considérons

$$h = f - \frac{f(0)}{g(0)}g.$$

Il est facile de voir que $h(0) = 0$ et donc $h \in I$. Mais comme

$$f = h + \frac{f(0)}{g(0)}g$$

et que $h \in I$, $\frac{f(0)}{g(0)}g \in J$ (car J est un idéal et qu'on a multiplié une fonction de J par une fonction de A), on en déduit (toujours parce que J est un idéal) que $f \in J$. Ainsi, on a $J = A$.

Correction de l'exercice 6 ▲

1. Soit $x \in A \setminus \{0\}$. Alors l'idéal engendré par x ne peut pas être l'idéal $\{0\}$, donc c'est A tout entier. En particulier, il existe $y \in A$ tel que $yx = xy = 1_A$. C'est bien que A est un corps.

2. Prenons toujours $x \in A \setminus \{0\}$ et considérons les idéaux $I_n = x^n A$. Alors puisque A admet un nombre fini d'idéaux, il existe $n < p$ tel que $x^n A = x^p A$. En particulier, il existe $a \in A$ tel que $x^n = x^p a$. Ceci entraîne $x^n(1 - x^{p-n}a) = 0$. L'anneau étant intègre (et x étant non nul), ceci entraîne que $x^{p-n}a = 1$. x est alors inversible, d'inverse $x^{p-n-1}a$.

Correction de l'exercice 7 ▲

Méthode 1 : Il existe un unique polynôme unitaire P_n tel que $I_n = (P_n)$. De plus, la condition $I_n \subset I_{n+1}$ entraîne que $P_{n+1} | P_n$. La suite $(\deg(P_n))$ est donc une suite d'entiers naturels décroissante : elle est stationnaire. Soit $p \in \mathbb{N}$ tel que, pour tout $n \geq p$, on a $\deg(P_n) = \deg(P_p)$. On a alors $P_n | P_p$, P_n et P_p sont unitaires et de même degré, donc ils sont égaux et $I_n = I_p$. La suite (I_n) est bien stationnaire. Méthode 2 : Posons $I = \bigcup_n I_n$. Puisque la suite (I_n) est croissante, il est facile de vérifier que I est un idéal. Il existe $P \in \mathbb{K}[X]$ tel que $I = (P)$. Mais alors, il existe $N \in \mathbb{N}$ tel que $P \in I_N$. On prouve alors que pour tout $n \geq N$, on a $I_n = (P)$. En effet, on a $I_n \subset I = (P)$, et $P \in I_N \subset I_n \implies (P) \subset I_n$.

Correction de l'exercice 8 ▲

1. Commençons par $I + J$. Il faut d'abord démontrer que c'est un sous-groupe de $(A, +)$. Mais $0 = 0 + 0 \in I + J$. D'autre part, si x et y sont éléments de $I + J$, on les écrit $x = i + j$, $y = i' + j'$, et on a

$$x - y = (i - i') + (j - j') \in I + J$$

puisque $i - i' \in I$ et $j - j' \in J$. D'autre part, pour $a \in A$, on a, par distributivité de \times par rapport à $+$:

$$ax = ai + aj \in I + J$$

puisque, I et J étant deux idéaux, $ai \in I$ et $aj \in J$. Ceci prouve que $I + J$ est un idéal. Passons maintenant à $I.J$: $0 \times 0 = 0$ est élément de $I.J$. De plus, si $x = \sum_{k=1}^n i_k j_k$ et $y = \sum_{k=1}^m i'_k j'_k$, en posant $i_k = -i'_{k-n}$ et $j'_k = j'_{k-n}$ pour k allant de $n+1$ à $n+m$, on a

$$x - y = \sum_{k=1}^{n+m} i_k j_k$$

ce qui prouve que $I.J$ est un sous-groupe de $(A, +)$. Enfin, pour tout a dans A , on a

$$ax = \sum_{k=1}^n (ai_k) j_k \in I.J$$

puisque chaque ai_k (resp. j_k) est élément de I (resp. de J).

2. Soit $x = \sum_{k=1}^n i_k j_k$ un élément de $I.J$. Pour chaque k , $i_k j_k$ est un élément de I puisque I est un idéal. Comme I est de plus stable par la somme, $I.J$ est bien contenu dans I . Par symétrie du rôle joué par I et J , $I.J$ est aussi contenu dans J et donc $I.J$ est contenu dans $I \cap J$.

3. Soit $x \in (I + J).(I \cap J)$. On écrit $x = \sum_{k=1}^n a_k b_k$ avec $a_k \in I + J$ et $b_k \in I \cap J$. Puisque $I.J$ est un idéal, il suffit de prouver que $a_k b_k \in I.J$. On écrit $a_k = i_k + j_k$, de sorte que

$$a_k b_k = i_k b_k + b_k j_k.$$

C'est un élément de $I.J$, car $i_k \in I$, $b_k \in J$ et $b_k \in I$, $j_k \in J$.

4. Il suffit de prouver que $I \cap J \subset I.J$. D'après la question précédente, on a $A.(I \cap J) \subset I.J$. Prenons $x \in I \cap J$. Alors $x = 1_A x \in A.(I \cap J) \subset I.J$. Ceci prouve l'inclusion restante.

Correction de l'exercice 9 ▲

1. La preuve est facile et laissée au lecteur : le point clé est que si p est premier avec n et avec n' , alors p est premier avec le produit nn' .

2. D'abord, on peut remarquer que $0 \in J_{p^k}$. Prenons ensuite $x = \frac{m}{n}$ et $y = \frac{m'}{n'}$ deux éléments de J_{p^k} . Alors

$$x - y = \frac{mn' - m'n}{nn'}$$

avec $p \wedge (nn') = 1$ (voir plus haut) et $p^k | m$, $p^k | m'$ et donc $p^k | mn' - m'n$. Ensuite, si $z = \frac{a}{b} \in \mathbb{Z}_p$, alors $xz = \frac{am}{bn}$ est tel que $p^k | am$ et $p \wedge (bn) = 1$, et donc $xz \in J_{p^k}$. J_{p^k} est bien un idéal de \mathbb{Z}_p .

3. Considérons $A = \{l \geq 0; \forall x \in I, \exists (m, n) \in \mathbb{Z} \times \mathbb{N}^*, x = \frac{m}{n}, p^l | m, p \wedge n = 1\}$. Alors A est un ensemble non vide d'entiers (car il contient 0) et il est majoré : si $x \in J$ s'écrit $x = m/n$ avec $p \wedge n = 1$, soit ℓ_0 le plus grand possible tel que p^{ℓ_0} divise m . Alors tout $l \in A$ vérifie $l \leq \ell_0$. Posons alors $k = \max(A)$ et prouvons que $I = J_{p^k}$. D'abord, il est clair que $I \subset J_{p^k}$. En effet, si $x \in I$, par définition de k , $x = \frac{m}{n}$ avec $(m, n) \in \mathbb{Z} \times \mathbb{N}^*$, $p^k | m$ et $p \wedge n = 1$. Réciproquement, soit $x \in J_{p^k}$, il faut prouver que $x \in I$. Par définition de k , on sait que l'on peut trouver $y = \frac{a}{b} \in I$ tel que $a = p^k a'$ avec $a' \wedge p = b \wedge p = 1$. Mais alors, $\frac{a'}{b}$ est inversible dans \mathbb{Z}_p , d'inverse $\frac{b}{a'}$. Puisque I est un idéal, ceci entraîne que $p^k = y \times \frac{b}{a'} \in I$. Mais alors, puisque x s'écrit $x = p^k \frac{m'}{n}$ avec $p \wedge n = 1$, on en déduit que $x \in I$. On a bien démontré que tous les idéaux de \mathbb{Z}_p sont de la forme J_{p^k} .

Correction de l'exercice 10 ▲

1. On commence par remarquer que si $x^n \in I$, alors pour tout $k \geq n$, $x^k = x^{k-n}x^n \in I$ (qui est un idéal). Montrons d'abord que $(\sqrt{I}, +)$ est un sous-groupe de $(A, +)$. En effet, $0 \in \sqrt{I}$ puisque $I \subset \sqrt{I}$ (prendre $n = 1$). De plus, si x est dans \sqrt{I} alors $(-x)^n = (-1)^n x^n \in I$ puisque $x^n \in I$ et que I est un idéal. Prenons maintenant $x, y \in \sqrt{I}$ et $n, m \in \mathbb{N}$ tels que $x^n \in I$, $y^m \in I$. Alors, par la formule du binôme que l'on peut appliquer dans l'anneau commutatif A , on a

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

Or, si $k \leq n$, alors $n+m-k \geq m$ et donc $y^{n+m-k} \in I$, ce qui entraîne $x^k y^{n+m-k} \in I$. Si $k \geq n$, cette fois $x^k \in I$ et donc $x^k y^{n+m-k} \in I$. $(I, +)$ étant un sous-groupe de $(A, +)$, on en déduit que $(x+y)^{n+m} \in I$, c'est-à-dire $x+y \in \sqrt{I}$. Finalement, prouvons que pour $a \in A$ et $x \in \sqrt{I}$, alors $ax \in \sqrt{I}$. Soit $n \geq 0$ tel que $x^n \in I$. Alors $(ax)^n = a^n x^n \in I$, ce qui prouve le résultat.

2. Soit $x \in \sqrt{I \cap J}$. Il existe $n \geq 1$ tel que $x^n \in I \cap J$, c'est-à-dire $x^n = \sum_k a_k b_k$ avec $a_k \in I$ et $b_k \in J$. Alors $x^n \in I$ puisque I est un idéal et $x^n = ab$, $a \in I$, et de même $x^n \in J$ (on utilise en fait que $I \cap J \subset I \cap J$). Ainsi, $x \in \sqrt{I \cap J}$. Soit maintenant $x \in \sqrt{I \cap J}$. Alors il existe $n \geq 1$ tel que $x^n \in I$ et $x^n \in J$. Donc $x \in \sqrt{I}$ et $x \in \sqrt{J}$, soit $x \in \sqrt{I} \cap \sqrt{J}$. Finalement, soit $x \in \sqrt{I} \cap \sqrt{J}$. Alors il existe $n, m \geq 1$ tels que $x^n \in I$ et $x^m \in J$. Alors $x^{n+m} = x^n x^m \in I \cap J$, et donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cap J}$. On a $I \subset \sqrt{I}$ et donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Réciproquement, prenons $x \in \sqrt{\sqrt{I}}$. Il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$. Posons $y = x^n \in \sqrt{I}$. Il existe $m \geq 1$ tel que $y^m \in I$. Alors, $x^{nm} = y^m \in I$ et donc $x \in \sqrt{I}$. La dernière égalité se prouve de façon tout à fait identique !

3. Soit $x \in \sqrt{I \cap J}$. Il existe $n \geq 1$ tel que $x^n \in I \cap J$, c'est-à-dire $x^n = \sum_k a_k b_k$ avec $a_k \in I$ et $b_k \in J$. Alors $x^n \in I$ puisque I est un idéal et $x^n = ab$, $a \in I$, et de même $x^n \in J$ (on utilise en fait que $I \cap J \subset I \cap J$). Ainsi, $x \in \sqrt{I \cap J}$. Soit maintenant $x \in \sqrt{I \cap J}$. Alors il existe $n \geq 1$ tel que $x^n \in I$ et $x^n \in J$. Donc $x \in \sqrt{I}$ et $x \in \sqrt{J}$, soit $x \in \sqrt{I} \cap \sqrt{J}$. Finalement, soit $x \in \sqrt{I} \cap \sqrt{J}$. Alors il existe $n, m \geq 1$ tels que $x^n \in I$ et $x^m \in J$. Alors $x^{n+m} = x^n x^m \in I \cap J$, et donc $\sqrt{I} \cap \sqrt{J} \subset \sqrt{I \cap J}$.

4. On a $I \subset \sqrt{I}$ et donc $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Réciproquement, prenons $x \in \sqrt{\sqrt{I}}$. Il existe $n \geq 1$ tel que $x^n \in \sqrt{I}$. Posons $y = x^n \in \sqrt{I}$. Il existe $m \geq 1$ tel que $y^m \in I$. Alors, $x^{nm} = y^m \in I$ et donc $x \in \sqrt{I}$.

5. La dernière égalité se prouve de façon tout à fait identique !

6. Soit $x \in \mathbb{Z}$. x est dans $\sqrt{k\mathbb{Z}}$ si et seulement si il existe $n \geq 1$ tel que $x^n \in k\mathbb{Z}$. Autrement dit, $k|x^n$. Décomposons k en produits de facteurs premiers : $k = p_1^{\alpha_1} \dots p_r^{\alpha_r}$. On obtient que $p_i | x^n \implies p_i | x$ pour tout $i = 1, \dots, r$ et donc $p_1 \dots p_r | x$, ce qui peut encore s'écrire $x \in (p_1 \dots p_r)\mathbb{Z}$. Réciproquement, si $x \in (p_1 \dots p_r)\mathbb{Z}$, alors, x s'écrit $x = p_1 \dots p_r m$. Notant $n = \max_{i \in \{1, \dots, r\}} (\alpha_i)$, on a $k | x^n$. Ainsi, on a prouvé que $\sqrt{I} = (p_1 \dots p_r)\mathbb{Z}$.

Correction de l'exercice 11 ▲

D'une part, il est facile (et laissé au lecteur) de vérifier que si I et J sont deux idéaux respectifs de A et B , alors $I \times J$ est un idéal de $A \times B$. Réciproquement, fixons K un idéal de $A \times B$ et construisons des idéaux I de A et J de B tels que $K = I \times J$. On désigne par $p_A : A \times B \rightarrow A$ et $p_B : A \times B \rightarrow B$ les projections respectives sur A et B , et on pose $I = p_A(K)$, $J = p_B(K)$. Comme p_A et p_B sont des morphismes surjectifs, I et J sont des idéaux respectivement de A et de B . Prenons ensuite $z \in K$. Alors $z = (p_A(z), p_B(z))$ est bien un élément de $I \times J$. Pour l'autre inclusion, fixons $(x, y) \in I \times J$ et prouvons que $(x, y) \in K$. Puisque $x \in I$, il existe $b \in B$ tel que $(x, b) \in K$. Puisque $y \in J$, il existe $a \in A$ tel que $(a, y) \in K$. Maintenant, $(1, 0) \cdot (x, b) = (x, 0) \in K$ (puisque K est un idéal) et de même $(0, 1) \cdot (a, y) = (0, y) \in K$. Par somme, $(x, 0) + (0, y) = (x, y) \in K$.

Correction de l'exercice 12 ▲

1. 18 et 49 sont premiers entre eux, et donc $\overline{18}$ est inversible dans $\mathbb{Z}/49\mathbb{Z}$. Pour trouver son inverse, il faut résoudre l'équation de Bezout $18u + 49v = 1$. Avec l'algorithme d'Euclide ou un logiciel, on trouve que $7 \times 49 - 19 \times 18 = 1$. Ainsi, l'inverse de $\overline{18}$ dans $\mathbb{Z}/49\mathbb{Z}$ est $-\overline{19} = \overline{30}$.

2. 3 divise à la fois 42 et 135. Ainsi, $\overline{42}$ n'est pas inversible dans $\mathbb{Z}/135\mathbb{Z}$.

Correction de l'exercice 13 ▲

1. On cherche d'abord l'inverse de $\bar{7}$ dans $\mathbb{Z}/37\mathbb{Z}$. Cela revient à résoudre l'équation de Bézout $7u + 37v = 1$. En appliquant l'algorithme d'Euclide, on trouve qu'une solution particulière est donnée par $16 \times 7 - 3 \times 37 = 1$. Ainsi, $\bar{16}$ est inverse de $\bar{7}$ dans $\mathbb{Z}/37\mathbb{Z}$. Il vient

$$\bar{7}x = \bar{2} \iff \bar{16} \times \bar{7}x = \bar{16} \times \bar{2} \iff x = \bar{32}.$$

2. La situation est un peu plus difficile car 10 et 34 ne sont pas premiers entre eux, mais on va tout de même pouvoir simplifier. Soit $k \in \mathbb{Z}$ tel que $x = \bar{k}$. Alors on a

$$\begin{aligned} \bar{10}x = \bar{6} &\iff 10k \equiv 6 \pmod{34} \\ &\iff \exists m \in \mathbb{Z}, 10k = 6 + 34m \\ &\iff \exists m \in \mathbb{Z}, 5k = 3 + 17m \\ &\iff 5k \equiv 3 \pmod{17} \end{aligned}$$

On cherche ensuite un entier a tel que $5a \equiv 1 \pmod{17}$. On peut appliquer l'algorithme de Bézout, ou remarquer que 7 convient. On en déduit

$$\begin{aligned} \bar{10}x = \bar{6} &\iff 35k \equiv 21 \pmod{17} \\ &\iff k \equiv 4 \pmod{17} \\ &\iff k = 4 + 17\ell, \ell \in \mathbb{Z}. \end{aligned}$$

Finalement, les solutions de l'équation initiale sont $\{\bar{4}, \bar{21}\}$.

3. Cette fois, l'équation n'a pas de solutions. En effet, si $x = \bar{k}$, on obtient $10k = 5 + 34m$, avec $m \in \mathbb{Z}$, et le membre de gauche est divisible par 2 alors que le membre de droite ne l'est pas.

Correction de l'exercice 14 ▲

1. Comme $\bar{2}$ et $\bar{3}$ sont inversibles dans $\mathbb{Z}/13\mathbb{Z}$ (puisque 2 et 3 sont premiers avec 13), on peut réaliser l'opération $-\bar{3}L_1 + \bar{2}L_2 \rightarrow L_2$ sans changer les solutions du système. Le système est donc équivalent à

$$\begin{cases} \bar{2}x + \bar{3}y = \bar{4} \\ -\bar{5}y = -\bar{2} \end{cases} \iff \begin{cases} \bar{2}x + \bar{3}y = \bar{4} \\ \bar{5}y = \bar{2} \end{cases}$$

On résout ensuite l'équation $\bar{5}y = \bar{2}$. En remarquant que $5 \wedge 13 = 1$ et donc que $\bar{5}$ est inversible dans $\mathbb{Z}/13\mathbb{Z}$, on obtient

$$\bar{5}y = \bar{2} \iff \bar{25}y = \bar{10} \iff -\bar{y} = -\bar{3} \iff \bar{y} = \bar{3}.$$

On reporte dans la première équation et on trouve

$$\bar{2}x + \bar{9} = \bar{4} \iff \bar{2}x = \bar{-5}.$$

En multipliant cette fois par $\bar{7}$ (remarquons que $7 \wedge 13 = 1$), on trouve

$$\bar{2}x = \bar{-5} \iff \bar{14}x = \bar{-35} \iff x = \bar{4}.$$

Le système admet donc une unique solution, le couple $(\bar{4}, \bar{3})$.

2. On procède comme à la question précédente, mais il faut toutefois prendre garde que $\bar{4}$ n'est pas premier avec 18. Toutefois, en effectuant l'opération $-\bar{5}L_1 + \bar{4}L_2 \rightarrow L_2$, on voit que toute solution du système vérifie

$$\begin{cases} \bar{4}x + \bar{7}y = \bar{1} \\ -\bar{27}y = \bar{3} \end{cases}$$

On essaie donc de résoudre $-\bar{27}y = \bar{3} \iff \bar{9}y = \bar{3}$. Mais si cette équation admet une solution y , en prenant $k \in \mathbb{Z}$ tel que $y = \bar{k}$, il existe $m \in \mathbb{Z}$ tel que l'on ait

$$9k = 3 + 18m.$$

Mais ceci est impossible car $9|9k$, $9|18$ mais 9 ne divise pas 3. Ainsi, le système n'admet pas de solutions.

3. Il faut faire un peu plus attention car les coefficients du système ne sont plus inversibles dans $\mathbb{Z}/18\mathbb{Z}$ et on ne peut plus raisonner par équivalence, mais seulement par implication. On remarque toutefois en effectuant $3L_1 - 2\bar{L}_2$ qu'on a nécessairement $y = -1$. On a alors un système du système si et seulement si

$$\begin{cases} \bar{2}x = \bar{4} \\ \bar{3}x = \bar{6} \end{cases}$$

On résout individuellement chacune de ces équations. Pour la première, en écrivant $x = \bar{k}$ avec $k \in \mathbb{Z}$, on trouve

$$\begin{aligned} \bar{2}x = \bar{4} &\iff 2k \equiv 4 \pmod{18} \\ &\iff \exists m \in \mathbb{Z}, 2k = 4 + 18m \\ &\iff \exists m \in \mathbb{Z}, k = 2 + 9m \\ &\iff x \in \{\bar{2}, \bar{11}\}. \end{aligned}$$

De même, on résout la deuxième équation et on trouve

$$\bar{3}x = \bar{6} \iff x \in \{\bar{2}, \bar{8}, \bar{14}\}.$$

La seule solution commune est $\bar{2}$ et finalement le système admet une unique équation, qui est le couple $(\bar{2}, \bar{-1})$.

Correction de l'exercice 15 ▲

1. On peut remarquer pour cette question que $\bar{14} = \bar{1}$ et que $\bar{49} = \bar{10}$. Ainsi,

$$(x + \bar{7})^2 = x^2 + x + \bar{10}$$

et k doit vérifier que $\bar{k}^2 = \bar{3}$. On remarque alors que $\bar{4}$ convient puisque $\bar{4}^2 = \bar{3}$. Remarquons qu'on ne demande pas toutes les solutions de l'équation.

2. Par la question précédente, l'équation est équivalente à

$$(x + \bar{7})^2 - \bar{4}^2 = 0 \iff (x + \bar{7} + \bar{4})(x + \bar{7} - \bar{4}) = 0.$$

Puisque $\mathbb{Z}/13\mathbb{Z}$ est un corps, et donc en particulier est intègre, ceci est encore équivalent à $x + \bar{11} = \bar{0}$ ou $x + \bar{3} = \bar{0}$. L'ensemble des solutions est donc $\{\bar{2}, \bar{10}\}$.

On dresse le tableau :

t	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
t^2	$\bar{0}$	$\bar{1}$	$\bar{4}$	$\bar{-3}$	$\bar{4}$	$\bar{1}$	$\bar{0}$

Ainsi, l'ensemble des solutions de l'équation $t^2 = 1$ dans $\mathbb{Z}/12\mathbb{Z}$ est $\{\bar{-5}, \bar{-1}, \bar{1}, \bar{5}\}$. On procède comme pour la question précédente. En mettant sous forme canonique, on trouve

$$x^2 - \bar{4}x + \bar{3} = (x - \bar{2})^2 - \bar{4} + \bar{3} = (x - \bar{2})^2 - \bar{1}.$$

L'équation est donc équivalente à

$$(x - \bar{2})^2 - \bar{1} = 0.$$

On peut bien sûr encore factoriser et obtenir que l'équation est équivalente à

$$(x - \bar{2} - \bar{1})(x - \bar{2} + \bar{1}) = 0.$$

Mais cette fois, on ne peut pas aller plus loin car $\mathbb{Z}/12\mathbb{Z}$ n'est pas un corps. Il faut plutôt écrire $(x - \bar{2})^2 = \bar{1}$. D'après la question précédente, cette équation est équivalente $x - \bar{2} \in \{\bar{-5}, \bar{-1}, \bar{1}, \bar{5}\}$. L'ensemble des solutions est donc $\{\bar{-3}, \bar{1}, \bar{3}, \bar{7}\}$. Il y a en particulier plus de deux solutions à cette équation polynomiale de degré 2 !

Correction de l'exercice 16 ▲

D'après le cours, les éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont les classes d'entiers k tels que $k \wedge 8 = 1$. On a donc

$$(\mathbb{Z}/8\mathbb{Z})^* = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}.$$

On remarque que tous ces éléments sont d'ordre 1 ou 2 (par exemple, $\bar{3}^2 = \bar{9} = 1$, $\bar{7}^2 = \bar{49} = \bar{1}$). Ainsi, aucun n'engendre $(\mathbb{Z}/8\mathbb{Z})^*$ et ce groupe n'est pas cyclique.

Correction de l'exercice 17 ▲

Non, ces groupes ne sont pas isomorphes. En effet, si f est un isomorphisme de G sur H , et si g est un élément de G d'ordre n , alors $f(g)$ est aussi d'ordre n . Or, ici, $\mathbb{Z}/8\mathbb{Z}$ est le seul des 3 groupes à avoir un élément d'ordre 8, tandis que $(\mathbb{Z}/2\mathbb{Z})^3$ est le seul à ne pas avoir d'éléments d'ordre 4. Ces 3 groupes ne sont pas deux à deux isomorphes.

Correction de l'exercice 18 ▲

1. 1 et -1 sont deux solutions distinctes. D'autre part, si m est un entier naturel dont la classe dans $\mathbb{Z}/n\mathbb{Z}$, notée x , est une solution, alors $p^\alpha | (m-1)(m+1)$, et donc m s'écrit $m = 1 + kp^u$, $m = -1 + lp^v$ avec $u + v \geq \alpha$ et k, l premiers avec p . Mais alors, on a

$$2 = lp^v - kp^u.$$

Si $u \neq 0$ et $v \neq 0$, alors $p | lp^v - kp^u$ et donc $p | 2$, ce qui n'est pas vrai. Donc $u = 0$ ou $v = 0$, ce qui entraîne $u \geq \alpha$ ou $v \geq \alpha$. Ainsi, dans $\mathbb{Z}/n\mathbb{Z}$, $x = 1$ ou $x = -1$, et donc on a exactement deux solutions dans ce cas.

2. Une étude exhaustive des cas donne, pour $n = 2$, une seule solution ($x = 1$) et pour $n = 4$ deux solutions ($x = 1$ ou $x = 3 = -1$).

3. On procède comme pour la première question. Soit m un entier compris entre 0 et $2^\alpha - 1$ tel que, si on note x sa classe dans $\mathbb{Z}/n\mathbb{Z}$, alors $x^2 = 1$. m s'écrit

$$m = 1 + k2^u \text{ et } m = -1 + l2^v$$

avec $u + v \geq \alpha$ et k, l premiers avec 2. Mais alors on a

$$2 = l2^v - k2^u,$$

et ceci entraîne que $u \leq 2$ ou $v \leq 2$, ou alors qu'un des deux entiers k, l est nul.

Si $u = 0$, alors $v \geq \alpha$ et donc (puisque $m \leq 2^\alpha - 1$), $v = \alpha$ et $m = -1 + 2^\alpha$, ce qui donne une première solution à l'équation. Le cas $v = 0$ est symétrique et donne $m = 1$, et donc une deuxième solution à l'équation. Si $u = 1$, alors $v \geq \alpha - 1$. Puisqu'on veut également que $0 \leq m < 2^\alpha - 1$ (cette dernière solution a déjà été considérée plus haut), il est nécessaire que $v = \alpha - 1$ et on trouve $m = -1 + 2^{\alpha-1}$. Son carré, dans $\mathbb{Z}/n\mathbb{Z}$, vaut bien 1, et cet entier est différent des précédents car $\alpha \geq 3$. Le cas $v = 1$ est symétrique et donne $m = 1 + 2^{\alpha-1}$. Si l'un des deux entiers k, l est nul, on retrouve une des solutions précédentes (à savoir 1 ou $-1 + 2^\alpha$).

Finalement, on a prouvé que dans ce cas on a 4 solutions à l'équation.

4. Si $u = 0$, alors $v \geq \alpha$ et donc (puisque $m \leq 2^\alpha - 1$), $v = \alpha$ et $m = -1 + 2^\alpha$, ce qui donne une première solution à l'équation.

5. Le cas $v = 0$ est symétrique et donne $m = 1$, et donc une deuxième solution à l'équation.

6. Si $u = 1$, alors $v \geq \alpha - 1$. Puisqu'on veut également que $0 \leq m < 2^\alpha - 1$ (cette dernière solution a déjà été considérée plus haut), il est nécessaire que $v = \alpha - 1$ et on trouve $m = -1 + 2^{\alpha-1}$. Son carré, dans $\mathbb{Z}/n\mathbb{Z}$, vaut bien 1, et cet entier est différent des précédents car $\alpha \geq 3$.

7. Le cas $v = 1$ est symétrique et donne $m = 1 + 2^{\alpha-1}$.

8. Si l'un des deux entiers k, l est nul, on retrouve une des solutions précédentes (à savoir 1 ou $-1 + 2^\alpha$).

9. Notons $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, avec $p_1 = 2$. Les anneaux $\mathbb{Z}/n\mathbb{Z}$ et $(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \dots \times (\mathbb{Z}/p_r^{\alpha_r}\mathbb{Z})$ sont isomorphes d'après le théorème chinois, l'isomorphisme étant donné par $x \mapsto (x_1, \dots, x_r)$, où x_i désigne la classe de x modulo $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. Il est clair que $x^2 = 1$ si et seulement si $x_i^2 = 1$ pour tout $i = 1, \dots, r$ (car l'application prendre le carré "commute" avec l'isomorphisme précédent). Le nombre de solutions de l'équation $x^2 = 1$ dans $\mathbb{Z}/n\mathbb{Z}$ est donc le produit du nombre de solutions de l'équation $x_i^2 = 1$ dans chaque $\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$. Ce nombre de solutions vaut donc :

$$2^{r-1} \text{ si } \alpha_1 = 0, 1; 2^r \text{ si } \alpha_1 = 2; 2^{r+1} \text{ si } \alpha_1 \geq 3.$$

10. 2^{r-1} si $\alpha_1 = 0, 1$;
 11. 2^r si $\alpha_1 = 2$;
 12. 2^{r+1} si $\alpha_1 \geq 3$.
-

Correction de l'exercice 19 ▲

1. On procède par récurrence sur n et on écrit $a = 2k + 1$. Pour $n = 3$, on a $(2k + 1)^2 = 4k^2 + 4k + 1 = 1 + 4k(k + 1)$. Or, $k(k + 1)$ est un nombre pair car ou bien k , ou bien $k + 1$ est pair. Ainsi, $4k(k + 1)$ est divisible par 8 et $a^2 \equiv 1 \pmod{8}$. Supposons maintenant le résultat établi au rang n , c'est-à-dire que $a^{2^{n-2}} = 1 + u2^n$. On met tout au carré et on trouve :

$$\begin{aligned} a^{2^{(n+1)-2}} &= (1 + u2^n)^2 \\ &= 1 + 2u2^n + u^2 2^{2n} \\ &= 1 + 2^{n+1}(u + u^2 2^{n-1}) \end{aligned}$$

ce qui prouve bien le résultat au rang $n + 1$.

2. Soit $G = \left(\mathbb{Z}/(2^n\mathbb{Z})\right)^*$. Un élément \bar{x} de $\mathbb{Z}/(2^n\mathbb{Z})$ est élément de G si et seulement si $x \wedge 2^n = 1$, si et seulement si $x \wedge 2 = 1$. Ainsi, on peut décrire G comme

$$G = \{\bar{x}; 1 \leq x \leq 2^n, x \wedge 2 = 1\}.$$

Mais dans $\{1, \dots, 2^n\}$, il y a exactement 2^{n-1} éléments impairs. Le cardinal de G est donc égal à 2^{n-1} . Or, pour $g = \bar{a} \in G$, la question précédente nous dit que

$$\{g^k; k \geq 0\} = \{g^k; 0 \leq k < 2^{n-2}\}.$$

Ce dernier ensemble comporte au plus 2^{n-2} éléments, et g n'est pas un élément cyclique de G . G n'est donc pas cyclique.

Correction de l'exercice 20 ▲

1. Rappelons que par le théorème de Bézout, n est inversible dans $(\mathbb{Z}/20\mathbb{Z}, \cdot)$ si et seulement si n est premier avec 20. On a donc $G = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

2. On prend un élément et toutes ses puissances, jusqu'à obtenir l'élément neutre 1. On obtient

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle 3 \rangle &= \{1, 3, 7, 9\} \\ \langle 7 \rangle &= \{1, 3, 7, 9\} \\ \langle 9 \rangle &= \{1, 9\} \\ \langle 11 \rangle &= \{1, 11\} \\ \langle 13 \rangle &= \{1, 9, 13, 17\} \\ \langle 17 \rangle &= \{1, 9, 13, 17\} \\ \langle 19 \rangle &= \{1, 19\} \end{aligned}$$

3. On vient de voir qu'on ne peut pas engendrer le groupe avec un seul élément. Essayons avec deux éléments. C'est facile à voir. Si on prend par exemple 3 et 11, le groupe engendré comprend au moins $\langle 3 \rangle$ et $\langle 11 \rangle$, c'est-à-dire au moins 5 éléments. Comme son ordre doit diviser l'ordre du groupe, il contient au moins 8 éléments, c'est-à-dire que c'est G tout entier. Autrement dit, on a prouvé que $\langle 3, 11 \rangle = G$ et donc $\{3, 11\}$ est un ensemble minimal de générateurs de G .

4. Aucun élément de G n'engendre seul le groupe. G n'est pas cyclique.

5. Les sous-groupes de G sont d'ordre 1, 2, 4 ou 8. Dans G , il y a un élément d'ordre 1, 4 éléments d'ordre 4 et 3 éléments d'ordre 2. Si on combine deux éléments d'ordre 4 qui n'engendrent pas le même sous-groupe, ou un élément d'ordre 4 avec un élément d'ordre 2 qui n'est pas dans le sous-groupe engendré (comme à la

question 3), on obtiendra G tout entier. Reste à voir les sous-groupes engendrés par les éléments d'ordre 2 : on a

$$\langle 11, 19 \rangle = \{1, 11, 19, 9\}$$

$$\langle 3, 11 \rangle = \langle 3, 13 \rangle = \langle 3, 19 \rangle = \langle 11, 13 \rangle = \langle 13, 19 \rangle = G.$$

6. Parmi les sous-groupes de G , ceux de la deuxième question sont cycliques, donc isomorphes à $\mathbb{Z}/m\mathbb{Z}$ où $m = 1, 2, 4$ suivant le cas. Le sous-groupe $\langle 11, 19 \rangle$ n'est pas cyclique, car il n'est pas engendré par un seul élément. De même, G n'est pas cyclique.

Correction de l'exercice 21 ▲

1. Si $2|n$, alors $2|2^n - 1$ et donc $2^n - 1$ est pair, ce qui n'est pas le cas.

2. Puisque p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe de cardinal $p - 1$. D'après le théorème de Lagrange, l'ordre de tout élément divise $p - 1$. Donc $m|p - 1$. Par hypothèse, $2^n \equiv 1 [n]$ ce qui entraîne $2^n \equiv 1 [p]$, ou encore $2^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. n est donc un multiple de l'ordre de 2, ou encore $m|n$. Puisque p est le plus petit facteur premier de n , on a $n \wedge (p - 1) = 1$. Ainsi, $m|\text{pgcd}(p - 1, n) = 1$, et donc $m = 1$. C'est absurde puisque $2 \neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$, $p \geq 3$. Il est donc impossible que n divise $2^n - 1$.

3. Puisque p est premier, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe de cardinal $p - 1$. D'après le théorème de Lagrange, l'ordre de tout élément divise $p - 1$. Donc $m|p - 1$.

4. Par hypothèse, $2^n \equiv 1 [n]$ ce qui entraîne $2^n \equiv 1 [p]$, ou encore $2^n = 1$ dans $\mathbb{Z}/p\mathbb{Z}$. n est donc un multiple de l'ordre de 2, ou encore $m|n$.

5. Puisque p est le plus petit facteur premier de n , on a $n \wedge (p - 1) = 1$. Ainsi, $m|\text{pgcd}(p - 1, n) = 1$, et donc $m = 1$. C'est absurde puisque $2 \neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$, $p \geq 3$. Il est donc impossible que n divise $2^n - 1$.

Correction de l'exercice 22 ▲

1. On vérifie facilement que $P(1) = P(2) = 0$.

2. La division euclidienne de $P(X)$ par $(X - 1)(X - 2) = X^2 - 3X + 2$ donne

$$X^4 - 4X^3 + 4X^2 + X - 2 = (X^2 - X - 1)(X^2 - 3X + 2).$$

3. On a

$$x^4 - x^3 + x - 2 = 0 \iff (x^2 - x - 1) = 0 \text{ ou } x^2 - 3x + 2 = 0.$$

Les solutions de $x^2 - 3x + 2 = 0$ sont $x = 1$ et $x = 2$. Quant aux solutions de $x^2 - x - 1 = 0$, après un calcul du discriminant, on trouve $x_1 = \frac{1+\sqrt{5}}{2}$ et $x_2 = \frac{1-\sqrt{5}}{2}$. Les racines de P sont donc 1, 2, $\frac{1+\sqrt{5}}{2}$ et $\frac{1-\sqrt{5}}{2}$.

Correction de l'exercice 23 ▲

Le polynôme est un polynôme "bicarré" : il s'écrit $P(X) = Q(X^2)$ où $Q(X) = 2X^2 + X - 3$. On commence par factoriser ce polynôme. Ses racines sont 1 et $-3/2$. Donc Q se factorise en

$$Q(X) = 2(X - 1)\left(X + \frac{3}{2}\right).$$

On en déduit que

$$P(X) = 2(X^2 - 1)\left(X^2 + \frac{3}{2}\right) = 2(X - 1)(X + 1)\left(X^2 + \frac{3}{2}\right).$$

Comme $X^2 + \frac{3}{2}$ est un polynôme de degré 2 sans racines réelles, on a bien obtenu la décomposition de P en produit d'irréductibles.

Correction de l'exercice 24 ▲

1. Comme P est de degré 3, s'il est réductible, il admet une racine dans \mathbb{Q} . Supposons donc que p/q est une racine de P avec $p \in \mathbb{Z}$, $q \in \mathbb{N}^*$ et $p \wedge q = 1$. On écrit que $P(p/q) = 0$ et on met au même dénominateur pour trouver

$$p^3 + 3p^2q + 2q^3 = 0.$$

Or, $q|3p^2q+2q^3$ et donc $q|p^3 = -3p^2q-2q^3$. Puisque $p \wedge q = 1$, on trouve $q = 1$. On a alors $p^3 + 3p^2 + 2 = 0$, et donc $p|2 = -p^3 - 3p^2$. Ainsi, $p = \pm 2$. Mais puisque si 2 ni -2 n'est une racine de P , on trouve que P est irréductible dans $\mathbb{Q}[X]$.

2. On remarque d'abord que Q n'a pas de racines dans \mathbb{R} , donc a fortiori pas de racines dans \mathbb{Q} . On vérifie ensuite que Q ne peut pas se factoriser comme produit de deux polynômes de degré 2 dans $\mathbb{Q}[X]$. Si tel était le cas, on pourrait écrire

$$X^4 + 1 = (X^2 + ax + b)(X^2 + cx + d)$$

avec $a, b, c, d \in \mathbb{Q}$. Développant le produit, et par unicité des coefficients, on obtiendrait le système

$$\begin{cases} a + c = 0 \\ ac + b + d = 0 \\ ad + cb = 0 \\ bd = 1 \end{cases}$$

Par conséquent, $a = -c$. Il n'est pas possible que $a = 0$ sinon on aurait $b = -d$ qui est incompatible avec $bd = 1$. La troisième ligne nous donne alors

$$ad + bc = 0 \iff a(d - b) = 0 \iff d = b.$$

Puisque $bd = 1$, on a $b = d = \pm 1$. Enfin, de $ac + b + d = 0$, on tire $a^2 = -b - d = \pm 2$. Dans tous les cas, il est impossible que $a \in \mathbb{Q}$. Ainsi, Q est irréductible dans $\mathbb{Q}[X]$.

Correction de l'exercice 25 ▲

Il suffit de démontrer que C est une sous-algèbre de $\mathcal{M}_n(\mathbb{R})$, c'est-à-dire à la fois un sous-anneau et un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$. Remarquons que la matrice nulle 0 et I_n sont membres de C . De plus, pour tous $M, N \in C$ et tout $\lambda \in \mathbb{R}$, alors on vérifie facilement que

1. $MN \in C$;
2. $\lambda M \in C$;
3. $M - N \in C$. C'est bien que C est une algèbre.

Correction de l'exercice 26 ▲

On va prouver que E est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$. Pour cela, notons

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Alors il est clair que $E = \text{vect}(I_3, A, B)$ et que la famille (I_3, A, B) est libre. On en déduit que E est un sous-espace vectoriel de $\mathcal{M}_3(\mathbb{R})$ de dimension 3. De plus, un calcul rapide montre que

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

E est stable par produit matriciel, et c'est une sous-algèbre de $\mathcal{M}_3(\mathbb{R})$.

Correction de l'exercice 27 ▲

1. Soit $a \in A \setminus \{0\}$. Alors $\phi : A \rightarrow A, x \mapsto ax$ est une application linéaire si l'on voit A comme un \mathbb{R} -espace vectoriel. Elle est injective, car A est intègre et donc son noyau est réduit à $\{0\}$. Comme A est de dimension finie, l'application est bijective. Il existe $x \in A$ tel que $ax = 1$, ce qui prouve que a est inversible.

2. 1 et a sont non-nuls et $a \notin \text{vect}(1)$. Donc $(1, a)$ est libre. Maintenant, puisque A est de dimension finie n , la famille $(1, a, a^2, \dots, a^n)$ qui est constituée par $n+1$ vecteurs est liée. Il existe un polynôme $P \in \mathbb{R}_n[X]$ tel que $P(a) = 0$. On factorise P en produit d'irréductibles, $P = P_1 \cdots P_r$. Alors

$$P_1(a) \cdots P_r(a) = 0.$$

Puisque A est intègre, il existe un k tel que $P_k(a) = 0$. Mais P_k est de degré au plus 2, et il ne peut pas être de degré 1 puisque $(1, a)$ est libre. Donc P_k est de degré 2 et $(1, a, a^2)$ est liée.

3. Soient α, β tels $a^2 + \alpha a + \beta = 0$, avec $\Delta = \alpha^2 - 4\beta < 0$ (conséquence de la question précédente). On a alors

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

ce qui entraîne

$$\left(\frac{2a + \alpha}{\sqrt{4\beta - \alpha^2}}\right)^2 = -1.$$

On a trouvé notre i !

4. Si $\dim(A) > 2$, on pourrait trouver b tel que la famille $(1, a, b)$ soit libre. Comme à la question précédente, on trouverait $j \in \text{vect}(1, b)$ tel que $j^2 = -1$. Mais alors,

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

et par intégrité de A , un des deux facteurs doit être nul. Dans un cas comme dans l'autre, cela implique $j \in \text{vect}(1, a)$ et donc $b \in \text{vect}(1, a)$, puisque qu'on peut aussi dire que $b \in \text{vect}(1, j)$. C'est une contradiction, et donc la dimension de A est deux.

5. L'isomorphisme est donné par $1_A \mapsto 1_{\mathbb{C}}$ et $i_A \mapsto i_{\mathbb{C}}$, dont on vérifie facilement que c'est un morphisme d'algèbre.
