1 ★ Soit $(A, +, \times)$ un anneau tel que :

$$\forall (x, y) \in A^2,\ (xy = 0 \Rightarrow x = 0 \text{ ou } y = 0)$$

Montrer que :

$$\forall (a, b) \in A^2,\ (ab = 1 \Rightarrow ba = 1)$$

Corrigé : Soient $(a, b) \in A^2$ tels que $ab = 1$. On a :

$$a(ba - 1) = aba - a = (ab - 1)a = 0$$

Ainsi $a = 0$ ou $ba = 1$.

- Si $ba = 1$, on a le résultat voulu.
- Si $a = 0$ alors $ab = 0$ et comme $ab = 1$, on a : $0 = 1$, dans ce cas $ba = b \times 0 = 0 = 1$ comme voulu.

2 Soit $*$ la loi de composition interne sur $\mathbb{R}$ définie par :

$$\forall (x, y) \in \mathbb{R}^2,\ x * y = x + y + x^2y^2$$

1. Vérifier que $*$ est commutative.
2. La loi $*$ est-elle associative ?
3. Montrer que $*$ admet un neutre et déterminer cet élément neutre.
4. Résoudre l'équation d'inconnue $x \in \mathbb{R}$: $1 * x = 0$.
5. Résoudre l'équation d'inconnue $x \in \mathbb{R}$: $1 * x = 1$.

Corrigé :

1. Soient $(x, y) \in \mathbb{R}^2$, on a :
$$y * x = y + x + y^2x^2 = x + y + x^2y^2 = x * y$$
$$\boxed{* \text{ est commutative}}$$

2. On a :
$$(1 * 1) * (-1) = (1 + 1 + 1^2 1^2) * (-1) = 3 * (-1) = 3 + (-1) + 3^2(-1)^2 = 11$$
$$1 * (1 * (-1)) = 1 * (1 + (-1) + 1^2(-1)^2) = 1 * 1 = 1 + 1 + 1^2 1^2 = 3$$
Ce contre exemple démontre que :
$$\boxed{* \text{ n'est pas associative}}$$

3. Soit $x \in \mathbb{R}$, on a tout de suite :
$$x * 0 = 0 * x = x$$
$$\boxed{0 \text{ est le neutre de } *}$$

4. Soit $x \in \mathbb{R}$, on a :
$$1 * x = 0 \Leftrightarrow 1 + x + x^2 = 0$$
Cette équation du second degré n'a pas de solution dans $\mathbb{R}$ car son discriminant est strictement négatif.
$$\boxed{\mathcal{S} = \emptyset}$$

5. Soit $x \in \mathbb{R}$, on a :
$$1 * x = 1 \Leftrightarrow x + x^2 = 0$$
Cette équation a pour solutions -1 et 0.
$$\boxed{\mathcal{S} = \{-1, 0\}}$$

3 ★ Soit G un groupe, e son élément neutre et $(a,b) \in G^2$ tels que : $ba = ab^2$ et $ab = ba^2$. Démontrer que $a = b = e$.

Corrigé : On a :

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

On peut simplifier par ba puisque dans un groupe tout élément est inversible donc régulier pour obtenir : $e = ab$. Ainsi $b = a^{-1}$ et on a aussi $ba = e$. On en déduit que :

$$e = ab = ba^2 = (ba)a = ea = a$$

Ce qui donne $a = e$ et $b = a^{-1} = e^{-1} = e$.

$$\boxed{a = b = e}$$

4 ★ Soit $(A, +, \times)$ un anneau. On suppose que pour tout $x \in A$, on a : $x^2 = x$.

1. Démontrer que : $\forall x \in A,\ 2x = 0$.
2. En déduire que A est commutatif.

Corrigé :

1. Soit $x \in A$, on peut appliquer l'hypothèse à $1 + x$ pour obtenir :

$$1 + x = (1 + x)^2 = (1 + x)(1 + x) = 1^2 + 2x + x^2 = 1 + 2x + x$$

Ce qui donne bien $2x = 0$.

$$\boxed{\forall x \in A,\ 2x = 0}$$

2. Soient $(x, y) \in A^2$, on a :

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

Ainsi $xy + yx = 0$. Or d'après la question 1, nous avons $xy + xy = 0$. En soustrayant ces deux dernières égalités, nous obtenons bien $xy = yx$.

$$\boxed{A \text{ est commutatif}}$$

5 ★★ Soit $(E, \times)$ un magma associatif. On suppose qu'il existe $a \in E$ tel que :

$$\forall y \in E,\ \exists x \in E,\ y = axa$$

1. Démontrer que E admet un neutre.
2. Démontrer que a est inversible et donner a^{-1}.

Corrigé :

1. On peut appliquer l'hypothèse à a (à la place de y), on sait qu'il existe $b \in E$ tel que $a = aba$. Soit $y \in E$, on lui associe $x \in E$ tel que $y = axa$. En utilisant l'associativité, on a :

$$(ab)y = (ab)(axa) = (aba)(xa) = axa = y$$

$$y(ba) = (axa)(ba) = ax(aba) = axa = y$$

Ainsi ab est un neutre à gauche et ba est un neutre à droite. On a alors $(ab)(ba) = ab$ car ba est neutre à droite et $(ab)(ba) = ba$ car ab est neutre à gauche d'où $ab = ba$. On pose $e = ab$, qui est bien le neutre de $\times$.

$$\boxed{ab \text{ est le neutre de } \times}$$

2. On a :

$$a(bab) = (ab)(ab) = ee = e$$
$$(bab)a = baba = ee = e$$

Ainsi a est inversible et $a^{-1} = bab$.

$$\boxed{a^{-1} = bab}$$

6 ★★★ Soit A un anneau non nul et $M = \{x \in A,\ x^2 = x\}$. Démontrer que si M est fini alors son cardinal est pair.

Corrigé : Soit $x \in M$, c'est-à-dire $x^2 = x$. On a :

$$(1-x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x$$

ainsi $1 - x \in M$. Ce qui démontre que dans l'ensemble M chaque élément x peut être appareillé avec $1 - x$, cela va nous permettre de conclure que le cardinal de M est pair lorsque M est fini. Il reste juste à démontrer que x et $1 - x$ sont distincts afin de pouvoir compter effectivement les éléments de M par paires. Soit $x \in M$, par l'absurde si $x = 1 - x$ alors $x = x^2 = x - x^2 = 0$, cependant si $x = 0$ alors x n'est pas égal à $1 - x$ puisque $0 \neq 1$ dans un anneau non nul.

$$\boxed{\text{Si } M \text{ est fini alors } M \text{ est de cardinal pair}}$$

7 ★★ Soit A un anneau et $(x, y) \in A^2$, on suppose que $1 - xy$ est inversible. Démontrer que $1 - yx$ est inversible.

Corrigé : Par hypothèse, il existe $v \in A$ tel que :

$$\begin{cases} v(1-xy) = 1 \\ (1-xy)v = 1 \end{cases} \Leftrightarrow \begin{cases} vxy = v - 1 \\ xyv = v - 1 \end{cases}$$

On a :

$$(1 + yvx)(1 - yx) = 1 + yvx - yx - yvxyx = 1 + yvx - yx - y(v-1)x = 1$$

On vérifie de même que $(1 - yx)(1 + yvx) = 1$. On a bien démontré que $1 - yx$ est inversible et $(1 - yx)^{-1} = 1 + yvx$.

8 ★

1. Démontrer que $A = \{a + b\sqrt{2},\ (a, b) \in \mathbb{Q}^2\}$ est un corps.
2. Démontrer que $B = \{a + b\sqrt{2} + c\sqrt{3},\ (a, b) \in \mathbb{Q}^2\}$ n'est pas un corps.

Corrigé :

1. Montrons pour cela que A est un sous-corps de $\mathbb{R}$ pour les opérations usuelles. Dans cette question, on note $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $(a, b, c, d) \in \mathbb{Q}^4$.

   • Déjà $A \subset \mathbb{R}$

   • -$0 = 0 + 0\sqrt{2}$ ainsi $0 \in A$.

   -On a $x + y = \underbrace{(a+c)}_{\in\mathbb{Q}} + \underbrace{(b+d)}_{\in\mathbb{Q}}\sqrt{2} \in A$.

   -On a : $-x = \underbrace{-a}_{\in\mathbb{Q}} + \underbrace{(-b)}_{\in\mathbb{Q}}\sqrt{2} \in A$

   On en déduit que $(A, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

   • -$1 = 1 + 0\sqrt{2}$ appartient à A.

• -On a :

$$xy = (a+b\sqrt{2}) \times (c+d\sqrt{2}) = \underbrace{ac+2bd}_{\in\mathbb{Q}} + \underbrace{(ad+bc)}_{\in\mathbb{Q}}\sqrt{2} \in A$$

On en déduit que $(A,+,\times)$ est un sous-anneau de $(\mathbb{R},+,\times)$.

• Soit $x \in A \setminus \{0\}$, nous devons démontrer que $\dfrac{1}{x} \in A$. On a :

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \underbrace{\frac{a}{a^2-2b^2}}_{\in\mathbb{Q}} - \underbrace{\frac{b}{a^2-2b^2}}_{\in\mathbb{Q}}\sqrt{2} \in A$$

Au cours de ce calcul, on a multiplié par $a-b\sqrt{2}$ qui est non nul car sinon :
• soit $b=0$ et dans ce cas $a=0$ ce qui est absurde puisque $x \neq 0$.
• soit $b \neq 0$ et dans ce cas : $\sqrt{2} = \dfrac{a}{b}$ ce qui est absurde car $\sqrt{2}$ est irrationnel.

$\boxed{A \text{ est un corps}}$

2. L'ensemble B n'est pas stable par multiplication, en effet $\sqrt{2} \times \sqrt{3} = \sqrt{6} \notin B$. En effet, raisonnons par l'absurde en supposant que $\sqrt{6} = p + q\sqrt{2} + r\sqrt{3}$ avec $(p,q,r) \in \mathbb{Q}^3$. On a :

$$\sqrt{6} - p = q\sqrt{2} + r\sqrt{3}$$

On élève au carré :

$$6 + p^2 - 2\sqrt{6}p = 2q^2 + 3r^2 + 2qr\sqrt{6}$$

Ce qui donne :

$$6 + p^2 - 2q^2 - 3r^2 = (2qr+2p)\sqrt{6}$$

Si jamais $2qr+2p \neq 0$ alors $\sqrt{6} = \dfrac{6+p^2-2q^2-3r^2}{2qr+2p}$ ce qui est absurde car $\sqrt{6}$ est irrationnel. On a donc $2qr+2p=0$ et par suite $6+p^2-2q^2-3r^2=0$, c'est-à-dire $(2-r^2)(q^2-3)=0$. Cette dernière relation est absurde car elle implique que $r=\pm\sqrt{2}$ ou $q=\pm\sqrt{3}$ ce qui n'est pas le cas car q et r sont rationnels.

$\boxed{B \text{ n'est pas un corps}}$

Problème

Dans tout l'exercice $(A, +, \times)$ désigne un anneau **commutatif** non nul. On note 0 et 1 les éléments neutres respectifs de l'addition et de la multiplication. Pour tous $(x, y) \in A^2$, on s'autorise à noter xy au lieu de $x \times y$. On dit qu'une partie, I, de A est un **idéal** de A si et seulement si les trois conditions suivantes sont vérifiées :

i) $0 \in I$
ii) $\forall (x, y) \in I^2,\ x + y \in I$
iii) $\forall \lambda \in A,\ \forall x \in I,\ \lambda x \in I$

1. **Un exemple.** On se place dans l'anneau $\mathcal{F}(\mathbb{R}, \mathbb{R})$ des fonctions de $\mathbb{R}$ dans $\mathbb{R}$ muni de l'addition et de la multiplication usuelles sur les fonctions. Pour tout $a \in \mathbb{R}$, on pose :

$$I_a = \{f \in \mathcal{F}(\mathbb{R}, \mathbb{R}),\ f(a) = 0\}$$

Démontrer que I_a est un idéal de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

2. **Idéaux de** $\mathbb{Z}$. Dans cette question, on considère l'anneau $\mathbb{Z}$ muni de l'addition et la multiplication usuelles.
   (a) Soit $n \in \mathbb{Z}$, démontrer que $n\mathbb{Z} = \{nk,\ k \in \mathbb{Z}\}$ est un idéal de $\mathbb{Z}$.
   (b) Soit I un idéal de $\mathbb{Z}$. On suppose que $I \neq \{0\}$.
      i. Justifier que $n = \min(I \cap \mathbb{N}^*)$ existe.
      ii. Soit $a \in I$, démontrer que le reste de la division euclidienne de a par n est nul. En déduire que $I \subset n\mathbb{Z}$.
      iii. Réciproquement démontrer que $n\mathbb{Z} \subset I$.
   (c) Caractériser les idéaux de $\mathbb{Z}$.

3. **Idéaux et éléments inversibles.** Démontrer que si I est un idéal de A alors :

$$I \text{ contient un élément inversible } \Leftrightarrow I = A$$

4. **Idéaux et morphismes.** Soit $f : A \to \widehat{A}$ un morphisme d'anneaux, avec $\widehat{A}$ un anneau également commutatif et non nul.
   (a) Soit J un idéal de $\widehat{A}$, démontrer que $f^{-1}(J)$ est un idéal de A.
   (b) Trouver un exemple montrant que si I est un idéal de A, $f(I)$ n'est pas toujours un idéal de $\widehat{A}$.

5. **Radical d'un idéal.** Soit I un idéal de A. On appelle radical de I et on note $\sqrt{I}$ l'ensemble :

$$\sqrt{I} = \{x \in A,\ \exists n \in \mathbb{N}^*,\ x^n \in I\}$$

   (a) Démontrer que $I \subset \sqrt{I}$.
   (b) Démontrer que $\sqrt{I}$ est un idéal de A. On pensera à utiliser la formule du binôme de Newton.
   (c) Vérifier que $\sqrt{\sqrt{I}} = \sqrt{I}$.
   (d) Dans cette question $A = \mathbb{Z}$. Déterminer l'ensemble des entiers naturels $m \in \mathbb{Z}$ tels que $\sqrt{m\mathbb{Z}} = m\mathbb{Z}$.

6. **Idéaux premiers**. On dit qu'un idéal I est premier si et seulement si :

$$\forall (x, y) \in A^2,\ xy \in I \Rightarrow x \in I \text{ ou } y \in I$$

   (a) Donner un idéal premier de $\mathbb{Z}$.
   (b) On suppose que tous les idéaux de A sont premiers. Démontrer que A est intègre puis que A est un corps.

Corrigé du problème

1. Soit $a \in \mathbb{R}$, I_a est inclus dans $\mathcal{F}(\mathbb{R},\mathbb{R})$ par définition. Il reste à vérifier les trois conditions requises pour que I_a soit un idéal :
   ▶ i) Notons θ la fonction nulle de $\mathbb{R}$ dans $\mathbb{R}$, on a $\theta(a) = 0$ ainsi $\theta \in I_a$.
   ▶ ii) Soient $(f,g) \in I_a^2$, c'est-à-dire que $f(a) = g(a) = 0$. On a $(f+g)(a) = 0$ ainsi $f+g \in I_a$.
   ▶ iii) Soit $\lambda \in \mathcal{F}(\mathbb{R},\mathbb{R})$ et $f \in I_a$, c'est-à-dire que $f(a) = 0$. On a $(\lambda f)(a) = \lambda(a)f(a) = 0$ ainsi $\lambda f \in I_a$.

$$\boxed{I_a \text{ est un idéal de } \mathcal{F}(\mathbb{R},\mathbb{R})}$$

2. (a) Soit $n \in \mathbb{Z}$, par définition $n\mathbb{Z} \subset \mathbb{Z}$. Vérifions les trois propriétés requises pour avoir un idéal :
   ▶ i) On a : $0 \in n\mathbb{Z}$ puisque $0 = n \times 0$.
   ▶ ii) Soient $(x,y) \in (n\mathbb{Z})^2$, il existe $(k,k') \in \mathbb{Z}^2$ tels que $x = nk$ et $y = nk'$. Ainsi $x + y = n(k+k') \in n\mathbb{Z}$ puisque $k + k' \in \mathbb{Z}$.
   ▶ iii) Soient $\lambda \in \mathbb{Z}$ et $x \in n\mathbb{Z}$, il existe $k \in \mathbb{Z}$ tel que $x = nk$. On a : $\lambda x = n(\lambda k) \in n\mathbb{Z}$ puisque $\lambda k \in \mathbb{Z}$.

$$\boxed{n\mathbb{Z} \text{ est un idéal de } \mathbb{Z}}$$

   (b) i. Comme l'idéal $I \neq \{0\}$, il existe un entier non nul appartenant à I, notons-le m.
   • Si $m > 0$, il appartient à $I \cap \mathbb{N}^*$.
   • Si $m < 0$, on a $-1 \times m = -m \in I$ d'après la condition iii) et $-m > 0$.
   Ce raisonnement démontre que $I \cap \mathbb{N}^*$ est non vide et bien sûr $I \cap \mathbb{N}^* \subset \mathbb{N}$. Or toute partie non vide de $\mathbb{N}$ possède un minimum.

$$\boxed{n = \min(I \cap \mathbb{N}^*) \text{ existe}}$$

   ii. Soit $a \in I$, effectuons la division euclidienne de a par n qui est bien non nul par définition. Il existe $(q,r) \in \mathbb{Z}^2$ tels que :

$$a = qn + r \text{ avec } 0 \leq r < n$$

   On a $n \in I$ donc $(-q) \times n \in I$ d'après la propriété iii). De plus comme $a \in I$, on a $r = a + (-qn) \in I$ d'après la propriété ii).
   Si $r \neq 0$, on a $r \in I \cap \mathbb{N}^*$ et $r < n$, ceci est absurde comme n est le minimum de $I \cap \mathbb{N}^*$. On a nécessairement $r = 0$ et par suite $a = qn \in n\mathbb{Z}$. Ce qui démontre que :

$$\boxed{I \subset n\mathbb{Z}}$$

   iii. Réciproquement, soit $x \in n\mathbb{Z}$, il existe $k \in \mathbb{N}$ tel que $x = nk$. Comme $n \in I$, la propriété iii) implique que $x = nk \in I$. Par double inclusion, on a démontré que :

$$\boxed{I = n\mathbb{Z}}$$

   (c) C'est un bilan des questions 2.(a) et 2.(b), les idéaux de $\mathbb{Z}$ sont exactement les parties de $\mathbb{Z}$ de la forme $n\mathbb{Z}$ où $n \in \mathbb{N}$. La question 2.(a) démontre en effet que $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ et la question 2.(b) démontre la réciproque, à savoir qu'un idéal de $\mathbb{Z}$ s'écrit sous la forme $n\mathbb{Z}$ où $n \in \mathbb{N}^*$. Enfin il faut tenir compte de l'idéal $\{0\}$ qui est obtenu pour $n = 0$.

$$\boxed{I \text{ idéal de } \mathbb{Z} \Leftrightarrow \exists n \in \mathbb{N},\ I = n\mathbb{Z}}$$

3. On procède par double implication.
   ($\Rightarrow$) On suppose que I est un idéal de A qui contient un élément inversible que l'on note x. D'après la propriété iii), on a $1 = x^{-1}x \in I$ puisque $x^{-1} \in A$. Soit $\lambda \in A$, on a $\lambda = \lambda \times 1 \in I$ toujours d'après la propriété iii) puisque $1 \in I$. Ce qui démontre que $A \subset I$ et par définition $I \subset A$ d'où $I = A$.
   ($\Leftarrow$) Réciproquement si $I = A$ (qui est bien un idéal de A), on a $1 \in I$ qui est inversible.

$$\boxed{I \text{ contient un élément inversible } \Leftrightarrow I = A}$$

4. (a) On rappelle la caractérisation de l'image réciproque qui va nous servir dans toute cette question, pour tout $x \in A$:

$$x \in f^{-1}(J) \Leftrightarrow f(x) \in J$$

On a $f^{-1}(J) \subset A$. Vérifions les trois conditions requises pour que $f^{-1}(J)$ soit un idéal de A :
► i) $0_A \in f^{-1}(J)$ car $f(0_A) = 0_{\widehat{A}} \in J$ car f est un morphisme et J est un idéal de $\widehat{A}$.
► ii) Soient $(x, y) \in f^{-1}(J)$, on a $f(x+y) = f(x) + f(y) \in J$ puisque $f(x)$ et $f(y)$ sont deux éléments de J qui est un idéal de $\widehat{A}$. Ce qui démontre que $x + y \in f^{-1}(J)$.
► iii) Enfin, soit $\lambda \in A$ et $x \in f^{-1}(J)$, on a $f(\lambda x) = f(\lambda)f(x)$. Or $f(\lambda) \in \widehat{A}$ et $f(x) \in J$, d'après la propriété iii) cela implique que $f(\lambda x) \in J$ et par suite $\lambda x \in f^{-1}(J)$.

$$\boxed{f^{-1}(J) \text{ est un idéal de } \widehat{A}}$$

(b) Considérons le morphisme suivant, avec $\mathbb{Z}$ et $\mathbb{R}$ munis de l'addition et la multiplication usuelles :

$$\begin{array}{rccc} f & : & \mathbb{Z} & \to & \mathbb{R} \\ & & x & \mapsto & x \end{array}$$

Le morphisme f va fournir un contre exemple, prenons $I = \mathbb{Z}$ qui est bien un idéal de $\mathbb{Z}$, par contre $f(\mathbb{Z}) = \mathbb{Z}$ n'est pas un idéal de $\mathbb{R}$ puisque la propriété iii) n'est pas vérifiée. En effet $\frac{1}{2} \in \mathbb{R}$ et $1 \in \mathbb{Z}$ pourtant $\frac{1}{2} \times 1 = \frac{1}{2} \notin \mathbb{Z}$.

$$\boxed{\text{L'image directe d'un idéal par un morphisme d'anneaux n'est pas toujours un idéal}}$$

5. (a) Soit $x \in I$, on a $x = x^1 \in I$ ainsi $x \in \sqrt{I}$ avec $n = 1$.

$$\boxed{I \subset \sqrt{I}}$$

(b) Par définition, on a : $\sqrt{I} \subset A$. Il reste à vérifier les trois propriétés :
► i) $0 \in \sqrt{I}$ car $0 = 0^1 \in I$.
► ii) Soient $(x, y) \in (\sqrt{I})^2$, c'est-à-dire qu'il existe $(m, n) \in (\mathbb{N}^*)^2$ tels que $x^m \in I$ et $y^n \in I$. Comme l'anneau A est commutatif, x et y commutent et on peut appliquer la formule du binôme de Newton :

$$(x+y)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k} = \underbrace{\sum_{k=0}^{m} \binom{m+n}{k} x^k y^{m+n-k}}_{(1)} + \underbrace{\sum_{k=m+1}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}}_{(2)}$$

• Etude de (1). On a $0 \leq k \leq m \Leftrightarrow n \leq m+n-k \leq m+n$. Ceci montre que l'on peut mettre y^n en facteur dans la somme (1) :

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

L'expression (1) appartient à I d'après la propriété iii) puisque c'est le produit d'un élément λ de A par y^n qui appartient à I.

• Etude de (2). Là aussi, on peut réécrire la somme (2) en mettant x^m en facteur :

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

On conclut que même que précédemment que (2) appartient à I puisque c'est le produit d'un élément de I par un élément de A.
Ainsi $(x+y)^{m+n} = (1) + (2)$ est un élément de I comme somme de deux éléments de I d'après la propriété ii). Ce qui démontre que $x + y \in \sqrt{I}$.
► iii) Enfin, soit $\lambda \in A$ et $x \in \sqrt{I}$, il existe $n \in \mathbb{N}^*$ tel que $x^n \in I$. En utilisant le fait que A est commutatif, on a :

$$(\lambda x)^n = \lambda^n x^n \in I \text{ d'après la propriété iii) car } x^n \in I$$

$$\boxed{\sqrt{I} \text{ est un idéal de } I}$$

(c) D'après la question (a), si I est un idéal de A alors $I \subset \sqrt{I}$. En appliquant cette propriété à $\sqrt{I}$ qui est bien un idéal d'après la question précédente, on a $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Pour l'autre inclusion, prenons $x \in \sqrt{\sqrt{I}}$, cela signifie qu'il existe $n \in \mathbb{N}^*$ tel que $x^n \in \sqrt{I}$. Ceci implique l'existence de $p \in \mathbb{N}^*$ tel que $(x^n)^p \in I$, c'est-à-dire $x^{np} \in I$. Comme $np \in \mathbb{N}^*$, ceci démontre que $x \in \sqrt{I}$. Par double inclusion, on conclut que :

$$\boxed{\sqrt{\sqrt{I}} = \sqrt{I}}$$

(d) Si $m = 0$ ou $m = 1$, on a bien $\sqrt{m\mathbb{Z}} = m\mathbb{Z}$. On remarque également que d'après la question (a), on a toujours $m\mathbb{Z} \subset \sqrt{m\mathbb{Z}}$.

► Supposons que $m \geq 2$ soit divisible par le carré d'un entier, c'est-à-dire qu'il existe un entier $d \geq 2$ tel que $m = d^2k$ avec $k \in \mathbb{N}$. On a $dk \in \sqrt{m\mathbb{Z}}$ puisque $(dk)^2 = mk \in m\mathbb{Z}$, pourtant $dk \notin m\mathbb{Z}$ puisque m ne divise pas dk. Ceci montre que si m est divisible par le carré d'un entier alors $\sqrt{m\mathbb{Z}} \not\subset m\mathbb{Z}$ et par contraposition si $\sqrt{m\mathbb{Z}} \subset m\mathbb{Z}$ alors m n'est pas divisible par le carré d'un entier.

► Réciproquement supposons que $m \geq 2$ ne soit pas divisible par le carré d'un entier. Démontrons que $\sqrt{m\mathbb{Z}} \subset m\mathbb{Z}$, soit $x \in \sqrt{m\mathbb{Z}}$, il existe $n \in \mathbb{N}^*$ tel que $x^n \in m\mathbb{Z}$. Ceci implique que m divise x^n. Soit p un nombre premier qui divise m alors $p|x^n$ donc $p|x$ et par suite $m|x$ puisque p apparaît à la puissance 1 dans la décomposition en facteurs premiers de m. Or $m|x \Leftrightarrow x \in m\mathbb{Z}$, ce qui démontre l'inclusion souhaitée.

$$\boxed{\sqrt{m\mathbb{Z}} = m\mathbb{Z} \text{ si et seulement si } m \text{ n'est pas divisible par le carré d'un entier}}$$

6. (a) L'idéal $2\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$. En effet, si x et y sont deux entiers relatifs tels que $xy \in 2\mathbb{Z}$, c'est-à-dire que 2 divise xy, ceci implique que 2 divise x ou 2 divise y. Ce qui démontre que $x \in 2\mathbb{Z}$ ou $y \in 2\mathbb{Z}$.

$$\boxed{\text{Plus généralement, si } p \text{ est un nombre premier alors } p\mathbb{Z} \text{ est un idéal premier de } \mathbb{Z}}$$

(b) $I = \{0\}$ est un idéal de A et par hypothèse, il est premier. Ainsi pour $(x, y) \in A^2$, on a :

$$xy \in \{0\} \Rightarrow x \in \{0\} \text{ ou } y \in \{0\}$$

C'est-à-dire $xy = 0 \Rightarrow x = 0$ ou $y = 0$. Or l'anneau A est supposé commutatif, non nul et le calcul précédent montre que A est intègre. Soit $x \in A \setminus \{0\}$, démontrons que x est inversible ceci impliquera que A est un corps. On considère l'ensemble $x^2A = \{x^2y,\ y \in A\}$, on montre sans difficulté que x^2A est un idéal de A. Cet idéal est premier d'après l'hypothèse de l'énoncé, on a $x^2 \in x^2A$ donc $x \in x^2A$, c'est-à-dire que $x = x^2y$ où $y \in A$. Or l'anneau A est intègre comme nous l'avons démontré ci-dessus donc $x = x^2y$ et $x \neq 0$ implique que $1 = xy$. Ce qui démontre que x est inversible.

$$\boxed{A \text{ est un corps}}$$

La notion d'idéal est fondamentale en algèbre. On peut démontrer que si I est un idéal d'un anneau A alors la relation binaire $\mathcal{R}$ est une relation d'équivalence :

$$\forall (x, y) \in A^2,\ x\mathcal{R}y \Leftrightarrow x - y \in I$$

L'ensemble des classes d'équivalence pour cette relation a une structure d'anneau, on note cet anneau A/I. C'est de là que vient la notation $\mathbb{Z}/n\mathbb{Z}$.

Exercice

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

1. Dans cette question, on suppose que pour tout $x \in A$, $x^2 = x$.
   (a) Démontrer que : $\forall x \in A,\ 2x = 0$.
   (b) En déduire que A est commutatif.
2. Dans cette question, on suppose que $\forall x \in A,\ x^3 = x$.
   (a) Déterminer les éléments nilpotents de A.
   (b) Soit $c \in A$ tel que $c^2 = c$. Démontrer que c commute avec tous les élements $a \in A$, on pourra pour cela calculer b^2 où $b = ca(1-c)$.
   (c) En déduire que pour tout $x \in A$, on a x^2 qui commute avec tous les éléments de A.
   (d) En déduire que pour tout $x \in A$, on a $2x$ et $3x$ qui commutent avec tous les éléments de A.
   (e) En déduire que A est commutatif.

Remarque. Plus généralement, le théorème de Jacobson affirme que si dans un anneau A, on a :

$$\forall x \in A,\ \exists n \geq 2,\ x^n = x$$

alors A est commutatif.

1. (a) Soit $x \in A$, on peut appliquer l'hypothèse à $1 + x$ pour obtenir :

$$1 + x = (1 + x)^2 = (1 + x)(1 + x) = 1^2 + 2x + x^2 = 1 + 2x + x$$

Ce qui donne bien $2x = 0$.

$$\boxed{\forall x \in A,\ 2x = 0}$$

(b) Soient $(x, y) \in A^2$, on a :

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

Ainsi $xy + yx = 0$. Or d'après la question 1, nous avons $xy + xy = 0$. En soustrayant ces deux dernières égalités, nous obtenons bien $xy = yx$.

$$\boxed{A \text{ est commutatif}}$$

2. (a) Soit $x \in A$, en calculant les premières puissances de x, on a :

$$x^3 = x,\ x^4 = x^2,\ x^5 = x^3 = x...$$

On démontre par une récurrence immédiate que pour tout $n \in \mathbb{N}^*$, on a : $x^n \in \{x, x^2\}$. Ainsi, si x est nilpotent alors $x = 0$ ou $x^2 = 0$. Cependant si $x^2 = 0$, on a :

$$x = x^3 = x^2 x = 0$$

On en déduit que :

$$\boxed{0 \text{ est le seul élément nilpotent de } A}$$

(b) Puisque $c^2 = c$, on a :

$$b^2 = ca(1-c)ca(1-c) = ca((1-c)c)ca(1-c) = ca(c-c^2)a(1-c) = 0$$

D'après la question précédente, on en déduit que $b = 0$ puisque b est nilpotent. Or :

$$b = 0 \Leftrightarrow ca(1-c) = 0 \Leftrightarrow ca - cac = 0 \Leftrightarrow ca = cac$$

On répète cette méthode avec $b' = (1-c)ac$. On a également $b'^2 = 0$ donc $b' = 0$ et par suite $ac = cac$. Finalement $ac = ca$ et on en déduit que c commute avec tous les éléments de$A$.

(c) On a :

$$(x^2)^2 = x^4 = x^3x = x^2$$

On peut appliquer la question précédente avec $c = x^2$ pour en déduire que :

$\boxed{x^2 \text{ commute avec tous les éléments de } A}$

(d) Soit $x \in A$. On a :

$$2x = (x+1)^2 - x^2 - 1$$

ce qui permet de dire que $2x$ commute avec tous les éléments de A car $(x+1)^2$, x^2 et 1 commutent avec tous les éléments de A d'après la question précédente.

D'autre part, on a : $(x+1)^3 = (x+1)$ et en développant :

$$(x+1)^3 = x^3 + 3x^2 + 3x + 1 = x + 3x^2 + 3x + 1 = 3x^3 + 4x + 1$$

Ces deux égalités impliquent $3x = -3x^2$, ainsi $3x$ commute avec tous les éléments de A car $-3x^2$ commute avec tous les éléments de A d'après la question précédente.

$\boxed{2x \text{ et } 3x \text{ commute avec tous les éléments de } A}$

(e) Enfin $x = 3x - 2x$ commute avec tous les éléments de A car c'est le cas de $3x$ et $2x$. Étant donné que x est quelconque, on en déduit que A est commutatif.

$\boxed{A \text{ est commutatif}}$