

Traitez les exercices marqués en jaune. La solution est en bas.

STRUCTURES ALGÈBRIQUES ANNEAUX...

Exercice 1 :

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

On rappelle qu'un élément a de A est dit **nilpotent** si et seulement s'il existe un entier non nul n tel que $a^n = 0$.

- 1) Soient a et b deux éléments nilpotents de A et qui commutent.
Montrer que $(a + b)$ et ab sont aussi nilpotents.
- 2) Soient maintenant a et b deux éléments de A tels que ab soit nilpotent.
Montrer que ba est aussi nilpotent.
- 3) Soit a un élément nilpotent de A .
Montrer que $(1 - a)$ est inversible et préciser son inverse en fonction des puissances de a .

NB : Questions classiques rencontrées avec les anneaux particuliers $(\mathcal{M}_n(\mathbb{K}), +, \times)$ et $(\mathcal{L}(E), +, \circ)$.

Exercice 2 :

- 1) Quels sont les sous-corps de $\mathbb{Q}$?
- 2) Quels sont les idéaux d'un corps K ?

Exercice 3 :

Soit f un endomorphisme de l'anneau $(\mathbb{R}, +, \times)$.

- 1) i) Justifier que

$$\forall x \geq 0, f(x) \geq 0$$

- ii) En déduire que f est croissante sur $\mathbb{R}$.

- 2) Montrer que :

$$\text{i) } \forall r \in \mathbb{Q}, f(r) = r$$

$$\text{ii) } f = id_{\mathbb{R}}$$

Indice : vous pouvez utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.

Exercice 4 :

Un complexe est dit *entier de Gauss* quand sa partie réelle et sa partie imaginaire sont des entiers relatifs.

Considérons l'anneau des entiers de Gauss

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

Pour $z \in \mathbb{Z}[i]$, on note $\mathcal{N}(z) = |z|^2$. Remarquons que $\mathcal{N}(zz') = \mathcal{N}(z)\mathcal{N}(z')$. Déterminer le groupe des inversibles de $\mathbb{Z}[i]$.

Exercice 5 :

Définitions : $(A, +, \times)$ étant un anneau.

Un idéal I de A est dit *principal* s'il existe $a \in A$ tel que $I = aA$.

L'anneau $(A, +, \times)$ est dit *principal* quand tous ses idéaux sont principaux.

On se propose de montrer que l'anneau produit $(\mathbb{Z}^2, +, \times)$ est principal.

1) Soit I un idéal de $\mathbb{Z}^2$.

Notons $I_1 = \{a \in \mathbb{Z} \mid (a, 0) \in I\}$ et $I_2 = \{a \in \mathbb{Z} \mid (0, a) \in I\}$.

Montrer que

i) I_1 et I_2 sont des idéaux de l'anneau $(\mathbb{Z}, +, \times)$.

ii) $I = I_1 \times I_2$.

2) Conclure.

Exercice 6 :

L'objectif de l'exercice est de montrer la relation suivante

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

où φ désigne l'indicatrice d'Euler.

1) Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Montrer que H est de la forme $H = \langle \bar{a} \rangle$, où a divise n .

2) Soit d un entier divisant n . Notons $a = n/d$. Montrer que :

i) $\langle \bar{a} \rangle$ est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .

ii) $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d .

3) Conclure.

Exercice 7 :

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

Définition : Soit I un idéal de A . On appelle *radical* de I la partie $\sqrt{I}$ de A définie par

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

1) Montrer que $\sqrt{I}$ est un idéal de A contenant I .

2) Soient I et J deux idéaux de A et $n \in \mathbb{N}^*$. Montrer que

$$\text{a) } \sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}, \text{ b) } \sqrt{\sqrt{I}} = \sqrt{I}, \text{ c) } \sqrt{I^n} = \sqrt{I}$$

3) Ici $A = \mathbb{Z}$. Déterminer le radical de l'idéal $n\mathbb{Z}$, où $n \in \mathbb{N}^*$.

Exercice 8 :

Considérons la matrice carrée d'ordre n , $T = (T_{ij})$ définie par

$$T_{ij} = \begin{cases} 1 & \text{si } i|j \\ 0 & \text{sinon} \end{cases}$$

Notons $D = \text{diag}(\varphi(1), \dots, \varphi(n))$, où φ l'indicatrice d'Euler.

Admettons l'égalité

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

- 1) Calculer le (i, j) ème coefficient de la matrice tTDT en fonction de $i \wedge j$.
- 2) En déduire $\det(S)$; où $S = (i \wedge j)_{1 \leq i, j \leq n}$. Dite la matrice de *Smith*.

Exercice 9 :

Résoudre dans $\mathbb{Z}$ les systèmes suivants :

- 1) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{11} \end{cases}$
- 2) $\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{11} \\ x \equiv 4 \pmod{7} \end{cases}$
- 3) $\begin{cases} 8x \equiv 4 \pmod{10} \\ 9x \equiv 3 \pmod{21} \end{cases}$

CORRECTION

CORRECTION

CORRECTION

STRUCTURES ALGÈBRIQUES

ANNEAUX...

Exercice 1 :

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

On rappelle qu'un élément a de A est dit **nilpotent** si et seulement s'il existe un entier non nul n tel que $a^n = 0$.

- 1) Soient a et b deux éléments nilpotents de A et qui commutent.
Montrer que $(a + b)$ et ab sont aussi nilpotents.
- 2) Soient maintenant a et b deux éléments de A tels que ab soit nilpotent.
Montrer que ba est aussi nilpotent.
- 3) Soit a un élément nilpotent de A .
Montrer que $(1 - a)$ est inversible et préciser son inverse en fonction des puissances de a .

NB : Questions classiques rencontrées avec les anneaux particuliers $(\mathcal{M}_n(\mathbb{K}), +, \times)$ et $(\mathcal{L}(E), +, \circ)$.

Solution

Voir la partie de 1^{ère} année sur le site

Exercice 2 :

- 1) Quels sont les sous-corps de $\mathbb{Q}$?
- 2) Quels sont les idéaux d'un corps K ?

Solution

1) Soit B un sous-corps de $(\mathbb{Q}, +, \times)$

$$\text{On a } \left(\begin{array}{l} B \text{ sous-groupe de } (\mathbb{Q}, +) \\ 1 \in B \end{array} \right)$$

$$\Rightarrow (\forall m \in \mathbb{Z}, m \cdot 1 = m \in B)$$

$$\text{Et on a : } (\forall n \in \mathbb{N}^*, n \in B \setminus \{0\})$$

$$\text{D'où } (\forall n \in \mathbb{N}^*, n^{-1} = \frac{1}{n} \in B)$$

$$\text{Ainsi } \left(\forall m \in \mathbb{Z}, \forall n \in \mathbb{N}^*, \underbrace{m}_{\in B} \times \underbrace{\frac{1}{n}}_{\in B} = \frac{m}{n} \in B \right)$$

$$\text{D'où } \mathbb{Q} \subset B$$

$$\text{Et donc } \boxed{B = \mathbb{Q}} \quad (\text{car } B \subset \mathbb{Q})$$

Ainsi : Si B sous-corps de $(\mathbb{Q}, +, \times)$ alors $B = \mathbb{Q}$.

Réciproquement, $\mathbb{Q}$ est un sous-corps de $\mathbb{Q}$.

Enfin :

Le seul sous-corps de $\mathbb{Q}$ est $\mathbb{Q}$ lui-même

Sous-corps

Déf :

Soit $(K, +, \times)$ un corps. Soit B une partie de K .
 B est dite *sous-corps* de K si et ssi

- a) $1 \in B$
- b) $\forall x, y \in B, x - y \in B$
- c) $\forall x, y \in B, x \times y \in B$
- d) $\forall x \in B \setminus \{0\}, x^{-1} \in B$

$$\text{Supp } H \text{ s-pr } \downarrow (G, \cdot) \cdot \text{On a :} \\ (a \in H) \Rightarrow (\forall m \in \mathbb{Z}, a^m \in H)$$

$$\text{Supp } H \text{ s-pr } \downarrow (G, +) \cdot \text{On a :} \\ (a \in H) \Rightarrow (\forall m \in \mathbb{Z}, ma \in H)$$

Exercice 2 :

1) Quels sont les sous-corps de $\mathbb{Q}$?

2) Quels sont les idéaux d'un corps K ?

Solution

Voici comment j'ai réfléchi pour répondre :

Soit I un idéal du Corps $(K, +, \times)$.

On voit que si $i \in I \setminus \{0\}$, alors i est inversible, car K Corps et $i \neq 0$.

$$\text{Et on a } \underbrace{i}_{\in I} \times \underbrace{i^{-1}}_{\in K} = 1$$

et puisque I idéal, on aura $1 \in I$

Par suite $I = K$

Déf : Soit $I \subset A$.

I est un idéal de A si et ssi les trois conditions suivantes sont satisfaites :

- 1) $0 \in I$
- 2) $\forall x, y \in I, x + y \in I$
- 3) $\forall x \in I, \forall y \in A, x \times y \in I$

Soit I un idéal de A . On a

$$I = A \Leftrightarrow 1 \in I$$

Rédaction :

Soit I un idéal non nul du Corps $(K, +, \times)$.

$$\text{On a } I \neq \{0\} \Rightarrow (\exists i \in I \text{ tel que } i \neq 0)$$

$\Rightarrow i$ inversible, car K Corps.

$$\text{On } \begin{cases} 1 = i \times i^{-1} \\ i \in I \text{ et } i^{-1} \in K, \text{ alors } 1 \in I \\ I \text{ idéal de } K \end{cases}$$

$$\text{D'où } \boxed{I = K}$$

Ainsi, K est le seul idéal non nul de K .

On sait que $\{0\}$ est un idéal de K , alors on conclut que :

$\{0\}$ et K sont les seuls idéaux du Corps K .

Fin Exercice 2

Exercice 3 :

Soit f un endomorphisme de l'anneau $(\mathbb{R}, +, \times)$.

1) i) Justifier que

$$\forall x \geq 0, f(x) \geq 0$$

ii) En déduire que f est croissante sur $\mathbb{R}$.

2) Montrer que :

i) $\forall r \in \mathbb{Q}, f(r) = r$

ii) $f = id_{\mathbb{R}}$

Indice : vous pouvez utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$.

1) i) $f(x) = f(\sqrt{x} \times \sqrt{x})$
 $= f(\sqrt{x}) \times f(\sqrt{x})$ (car f morph d'anneaux)
 $= (f(\sqrt{x}))^2 \geq 0. \quad \square$

ii) Soient $x, y \in \mathbb{R}$ tels que $x \leq y$.
Alors $f(x) \leq f(y)$.

On a :

$$\begin{aligned} f(y) &= f((y-x) + x) \\ &= f(y-x) + f(x) \quad (\text{car } f \text{ morph d'anneaux}) \end{aligned}$$

Or $f(y-x) \geq 0$ car $(y-x) \geq 0$ et d'après 1) i)

$$\text{Alors } f(y) \geq f(x) \quad \square$$

2) i) Soit $r \in \mathbb{Q}$. Alors $f(r) = r$.

$$r \in \mathbb{Q} \Rightarrow \exists (m, n) \in \mathbb{Z} \times \mathbb{N}^*, r = \frac{m}{n}$$

Ainsi :

$$f(r) = f\left(m \times \frac{1}{n}\right)$$

$$= m \times f\left(\frac{1}{n}\right) \quad \left(\begin{array}{l} \text{car } f \\ \text{morph d'anne} \end{array} \right)$$

Si f morph d'anne de A vers B , alors:
 $\forall m \in \mathbb{Z}, \forall x \in A$, on a:
 $f(mx) = m f(x)$

2) autre part, on a:

$$1 = f(1) \quad (f \text{ morph d'anne})$$

$$= f\left(n \times \frac{1}{n}\right)$$

$$1 = n \times f\left(\frac{1}{n}\right) \quad (f \text{ morph})$$

$$\text{Donc } f\left(\frac{1}{n}\right) = \frac{1}{n}$$

$$\text{Ainsi : } f(x) = m \times f\left(\frac{1}{n}\right)$$

$$= m \times \frac{1}{n}$$

$$= x \quad \square$$

2) iii) $f = \text{id}_{\mathbb{R}}$?

Soit $x \in \mathbb{R}$. M. que $f(x) = x$

Raisonnons par l'absurde, et supposons que $f(x) \neq x$.

Cas 1 : si $f(x) < x$

$$\exists r \in \mathbb{Q}, f(x) < r < x$$

$$f \text{ croissante} \Rightarrow \underbrace{f(r)}_{= f(x)} \leq f(x)$$

$$\Rightarrow \boxed{r \leq f(x)}, \text{ ce qui contredit } \underline{f(x) < r}$$

Cas 2 : si $x < f(x)$

$$\exists r \in \mathbb{Q}, x < r < f(x)$$

$$f \text{ croissante} \Rightarrow f(x) \leq \underbrace{f(r)}_{= r}$$

$$\Rightarrow \boxed{f(x) \leq r}, \text{ ce qui contredit } \underline{x < f(x)},$$

$\square$

Exercice 6 :

L'objectif de l'exercice est de montrer la relation suivante

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

où φ désigne l'indicatrice d'Euler.

1) Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.

Montrer que H est de la forme $H = \langle \bar{a} \rangle$, où a divise n .

2) Soit d un entier divisant n . Notons $a = n/d$. Montrer que :

i) $\langle \bar{a} \rangle$ est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .

ii) $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d .

3) Conclure.

1) Soit H un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$.
Montrons qu'il existe $a \in \mathbb{N}$ tel que $\begin{cases} H = \langle \bar{a} \rangle \\ a/n \end{cases}$

Cas 1 : Si $H = \{ \bar{0} \}$

$$\begin{aligned} \text{On a } H &= \{ \bar{0} \} \\ &= \langle \bar{0} \rangle \quad (\text{Mais } 0 \nmid n) \\ &= \langle \bar{n} \rangle, \text{ et } n/n \\ a=n &\text{ convient alors.} \end{aligned}$$

Cas 2 : Si $H \neq \{ \bar{0} \}$

On cherche un entier $a \in \mathbb{N}$ tel que $\begin{cases} H = \langle \bar{a} \rangle \\ a/n \end{cases}$.

Ici mon brouillon, pour vous montrer comment j'ai choisi a .

Supposons l'existence d'un tel a .

$$\text{On a alors } H = \langle \bar{a} \rangle = \{ \bar{0}, \bar{a}, \bar{2a}, \bar{3a}, \dots \}$$

a est le plus petit des entiers $a, 2a, 3a, \dots$

Autrement dit, $a = \min(\{k \geq 1 \mid \bar{k} \in H\})$

Fin brouillon

On cherche un entier $a \in \mathbb{N}$ tel que $\begin{cases} H = \langle \bar{a} \rangle \\ a/n \end{cases}$.

Notons $a = \min(\{k \geq 1 \mid \bar{k} \in H\})$.

Montrons que $\begin{cases} H = \langle \bar{a} \rangle \\ a/n \end{cases}$

i) $H = \langle \bar{a} \rangle$?

$$a = \min(\{k \geq 1 \mid \bar{k} \in H\})$$

On a bien que $\bar{a} \in H$

D'où $\langle \bar{a} \rangle \subset H$.

Montrons maintenant que $H \subset \langle \bar{a} \rangle$.

Soit alors $\bar{x} \in H$.

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

Rappel

Montrons que : $(\exists k \in \mathbb{Z}, x = k\bar{a})$

D'après la division euclidienne de x par a , on a :

$$x = ka + r, \text{ où } 0 \leq r < a$$

$$\Rightarrow \bar{x} = \underbrace{k \cdot \bar{a}}_{\in H} + \underbrace{\bar{r}}_{\in H}$$

$$\Rightarrow \bar{r} = \bar{x} - k \cdot \bar{a} \in H \quad (\text{car } H \text{ s-groupe de } \mathbb{Z}/n\mathbb{Z})$$

$$\text{Ainsi on a} \quad \left| \begin{array}{l} \bar{r} \in H \\ 0 \leq r < a \\ a = \min(\{k \geq 1 / \bar{k} \in H\}) \end{array} \right.$$

Alors " $r \geq 1$ " est impossible, car sinon on aurait $a \leq r$

2) où $\boxed{r=0}$.

et $\bar{x} = k \cdot \bar{a} + \bar{r}$ devient $\bar{x} = k \cdot \bar{a}$
CQFD

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

2) Soit d un entier divisant n . Notons $a = n/d$. Montrer que :
i) $\langle \bar{a} \rangle$ est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .

On montrera que :

A) $o(\langle \bar{a} \rangle) = d$

B) Si H sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d
(càd de cardinal d).

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

A) $o(\langle \bar{a} \rangle) = d$?

On a $o(\langle \bar{a} \rangle) = o(\bar{a})$.

Rapports

Si $(G, \cdot)$ groupe et $x \in G$. On a :

$$o(x) = d \Leftrightarrow (\forall k \in \mathbb{Z}, x^k = e \Leftrightarrow d \mid k)$$

Si $(G, +)$ groupe et $x \in G$. On a :

$$o(x) = d \Leftrightarrow (\forall k \in \mathbb{Z}, kx = 0 \Leftrightarrow d \mid k)$$

On a :

$$o(\bar{a}) = d \Leftrightarrow (\forall k \in \mathbb{Z}, k \cdot \bar{a} = \bar{0} \Leftrightarrow d \mid k)$$

$$\Leftrightarrow (\forall k \in \mathbb{Z}, k a = 0 \Leftrightarrow d \mid k)$$

$$\Leftrightarrow (\forall k \in \mathbb{Z}, n \mid k a \Leftrightarrow d \mid k)$$

$$\Leftrightarrow (\forall k \in \mathbb{Z}, d a \mid k a \Leftrightarrow d \mid k)$$

Ce qui est vrai

D'où

$$o(\bar{a}) = d$$



B) Soit H sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, +)$ d'ordre d .

Il faut : $H = \langle \bar{a} \rangle$

D'après 1°), il existe a' divisant n tel que $H = \langle \bar{a}' \rangle$.

$$\text{Notons } n = a' \cdot d'$$

$$\begin{array}{l|l} \text{On a} & o(\bar{a}') = d' \text{ (comme dans A)} \\ & o(\bar{a}') = o(\langle \bar{a}' \rangle) = o(H) = d \end{array}$$

D'où $d = d'$

$$\text{et } \begin{pmatrix} n = ad \\ n = a'd' \end{pmatrix} \Rightarrow \boxed{a = a'}$$

En fin, $H = \langle \bar{a}' \rangle \Rightarrow \boxed{H = \langle \bar{a} \rangle}$ CQFD

2) Soit d un entier divisant n . Notons $a = n/d$. Montrer que :

i) $\langle \bar{a} \rangle$ est l'unique sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ d'ordre d .

ii) $\mathbb{Z}/n\mathbb{Z}$ possède $\varphi(d)$ éléments d'ordre d .

Notons $A_d = \{ \bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid o(\bar{x}) = d \}$

Il s'agit de montrer que $\text{Card}(A_d) = \varphi(d)$.



$\varphi(d)$ laisse penser au nombre de générateurs de $\mathbb{Z}/d\mathbb{Z}$ ou en général d'un groupe cyclique d'ordre d .

Où a :

$$o(\bar{x}) = d \Leftrightarrow o(\langle \bar{x} \rangle) = d$$

$$\Leftrightarrow \langle \bar{x} \rangle = \langle \bar{a} \rangle \left(\begin{array}{l} \text{car } \langle \bar{a} \rangle \text{ est l'unique s-groupe} \\ \text{d'ordre } d \end{array} \right)$$

par déf

$$\Leftrightarrow \bar{x} \text{ est un } \underline{\text{générateur}} \text{ de } \langle \bar{a} \rangle$$

D'où

$A_d = \{ \bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid o(\bar{x}) = d \}$ est exactement l'ensemble des générateurs du groupe cyclique $\langle \bar{a} \rangle$.

en fin :

$$\text{Card}(A_d) = \varphi(d).$$

CQFD

3) Conclure.

On conclut que $\sum_{d|n} \varphi(d) = n$.

en effet :

gardons la notation $A_d = \{ \bar{x} \in \mathbb{Z}/n\mathbb{Z} \mid o(\bar{x}) = d \}$.

On a que $(A_d)_{d|n}$ forment une partition de $\mathbb{Z}/n\mathbb{Z}$.

$$\text{D'où } \text{Card}(\mathbb{Z}/n\mathbb{Z}) = \sum_{d|n} \underbrace{\text{Card}(A_d)}_{=\varphi(d)}$$

Ainsi :

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

Exercice 7 : (D'après Centrale)

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

Définition : Soit I un idéal de A . On appelle **radical** de I la partie $\sqrt{I}$ de A définie par

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

1) Montrer que $\sqrt{I}$ est un idéal de A contenant I .

2) Soient I et J deux idéaux de A et $n \in \mathbb{N}^*$. Montrer que

$$\text{a) } \sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}, \text{ b) } \sqrt{\sqrt{I}} = \sqrt{I}, \text{ c) } \sqrt{I^n} = \sqrt{I}$$

3) Ici $A = \mathbb{Z}$. Déterminer le radical de l'idéal $n\mathbb{Z}$, où $n \in \mathbb{N}^*$.

Solution

1) Montrer que $\sqrt{I}$ est un idéal de A contenant I .

$$\text{On a : } a \in \sqrt{I} \iff (\exists n \in \mathbb{N}^*, a^n \in I)$$

i) $I \subset \sqrt{I}$?

Soit $a \in I$. Montrons que $a \in \sqrt{I}$.

$$\text{On a } a^1 = a \in I \text{ alors } a \in \sqrt{I}$$

Déf : Soit $I \subset A$.

I est un idéal de A si et ssi les trois conditions suivantes sont satisfaites :

1) $0 \in I$

2) $\forall x, y \in I, x + y \in I$

3) $\forall x \in I, \forall y \in A, x \times y \in I$

ii) Montrons que $\sqrt{I}$ est un idéal de A .

(a) $0 \in \sqrt{I}$?

$$\text{On a } 0^1 = 0 \in I, \text{ donc } 0 \in \sqrt{I}$$

(b) Soient $a, b \in \sqrt{I}$. Montrons que $(a+b) \in \sqrt{I}$:

$$a, b \in \sqrt{I} \Rightarrow \begin{cases} \exists n \in \mathbb{N}^*, a^n \in I \\ \exists p \in \mathbb{N}^*, b^p \in I \end{cases}$$

$$a \in \sqrt{I} \iff (\exists n \in \mathbb{N}^*, a^n \in I)$$

Pour finir, déterminons un entier $s \in \mathbb{N}^*$ tel que $(a+b)^s \in I$:

$$\text{Notons d'abord que : } \begin{cases} \forall i \geq n, a^i \in I \\ \forall i \geq p, b^i \in I \end{cases}$$

$$\text{Car } a^i = \underbrace{a^n}_{\in I} \times \underbrace{a^{i-n}}_{\in A} \in I, \text{ car } I \text{ idéal de } A.$$

De même pour $b^i \in I$.

Pour $s \in \mathbb{N}^*$, on a :

$$(a+b)^s = \sum_{i=0}^s C_s^i a^i b^{s-i}$$

Puisque I idéal, alors pour avoir $(a+b)^s \in I$, il suffit que l'on ait : $(\forall 0 \leq i \leq s, a^i b^{s-i} \in I)$

$$\text{On a : } \begin{cases} \forall i \geq n, a^i \in I \\ \forall i \geq p, b^i \in I \end{cases}$$

$$\text{Alors } (\forall n \leq i \leq s, \underbrace{a^i}_{\in I} \times \underbrace{b^{s-i}}_{\in A} \in I)$$

Reste à ce que le s cherché vérifie :

$$(\forall 0 \leq i \leq n-1, a^i \times b^{s-i} \in I)$$

Il suffit que l'on ait :

$$(\forall 0 \leq i \leq n-1, s-i \geq p) \text{ vu que } \boxed{\forall i \geq p, b^i \in I}$$

$$\text{Càd : } (\forall 0 \leq i \leq n-1, \boxed{s \geq i+p})$$

$$\text{Or : } (\forall 0 \leq i \leq n-1, p \leq \boxed{i+p \leq n+p-1})$$

$$\text{Alors il suffit que le } s \text{ vérifie : } \boxed{s \geq n+p-1}$$

$$\boxed{s = n+p-1} \text{ conviendra alors.}$$

NB : J'ai répondu en montant à l'étrier comment j'ai réfléchi. Toutefois, on peut rédiger rapidement de la manière suivante :

$$a, b \in \sqrt{I} \Rightarrow \begin{cases} \exists n \in \mathbb{N}^*, a^n \in I \\ \exists p \in \mathbb{N}^*, b^p \in I \end{cases} \quad \left(\begin{array}{l} \forall k \geq n, a^k \in I; \\ \forall k \geq p, b^k \in I \end{array} \right) \quad a^k = \underbrace{a^n}_{\in I} \times \underbrace{a^{k-n}}_{\in A} \in I$$

On a :

$$\begin{aligned} (a+b)^{n+p} &= \sum_{i=0}^{n+p} \binom{n+p}{i} a^i \times b^{n+p-i} \\ &= \underbrace{\sum_{i=0}^{n-1} \binom{n+p}{i} a^i \times b^{n+p-i}}_{\in I} + \underbrace{\sum_{i=n}^{n+p} \binom{n+p}{i} a^i \times b^{n+p-i}}_{\in I} \end{aligned}$$

Annotations for the first sum: $a^i \in A$, $b^{n+p-i} \in I$ (because $n+p-i \geq p$), so $a^i \times b^{n+p-i} \in I$.
 Annotations for the second sum: $a^i \in I$ (because $i \geq n$), $b^{n+p-i} \in A$, so $a^i \times b^{n+p-i} \in I$.

Donc $(a+b)^{n+p} \in I$

Donc $(a+b) \in \sqrt{I}$

(6) Soient $a \in \sqrt{I}$ et $b \in A$. Montrer que $(ab) \in \sqrt{I}$

$$a \in \sqrt{I} \Rightarrow (\exists n \in \mathbb{N}^*, a^n \in I)$$

On a : $(ab)^n = a^n \times b^n \in I$ (A ann commutatif)
 $\downarrow \quad \downarrow$
 $\in I \quad \in A$

Donc $(ab)^n \in I$

$\Rightarrow (ab) \in \sqrt{I}$

Fin 10)

2) Soient I et J deux idéaux de A et $n \in \mathbb{N}^*$. Montrer que

a) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$ b) $\sqrt{\sqrt{I}} = \sqrt{I}$, c) $\sqrt{I^n} = \sqrt{I}$

$$IJ = \{ij / i \in I \text{ et } j \in J\}$$

i) $\sqrt{IJ} = \sqrt{I \cap J}$?

"C"

Soit $a \in \sqrt{IJ}$. Montrons que $a \in \sqrt{I \cap J}$

$$(\exists n \in \mathbb{N}^*, a^n \in IJ) \Rightarrow (\exists n \in \mathbb{N}^*, \exists (i, j) \in I \times J, a^n = i \cdot j)$$

On veut montrer que : $(\exists p \in \mathbb{N}^*, a^p \in I \text{ et } a^p \in J)$

$$\text{On a } a^n = i \times j \implies \begin{cases} a^n \in I \text{ (car } I \text{ idéal)} \\ a^n \in J \text{ (car } J \text{ idéal)} \end{cases}$$

$\downarrow \quad \downarrow$
 $\in I \quad \in J$

C'est fini ($p = n$ convient) □

"D"

Soit $a \in \sqrt{I \cap J}$. Montrons que $a \in \sqrt{IJ}$.

$$(\exists n \in \mathbb{N}^*, a^n \in I \text{ et } a^n \in J)$$

On veut montrer que : $(\exists p \in \mathbb{N}^*, \exists (i, j) \in I \times J, a^p = i \times j)$

$$\text{On a : } \begin{matrix} a^n & \times & a^n & = & a^{2n} \\ \downarrow & & \downarrow & & \\ \in I & & \in J & & \end{matrix} \text{ , alors c'est fini : } \left| \begin{array}{l} i \text{ c'est } a^n \\ j \text{ c'est } a^n \\ p = 2n \end{array} \right.$$

□

ii) $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$?

"C"

Reviens à montrer que $\sqrt{I \cap J} \subset \sqrt{I}$ et $\sqrt{I \cap J} \subset \sqrt{J}$

$\sqrt{I \cap J} \subset \sqrt{I}$?

Soit $a \in \sqrt{I \cap J}$. Montrons que $a \in \sqrt{I}$

$$(\exists n \in \mathbb{N}^*, a^n \in I \cap J) \Rightarrow a^n \in I$$

$$\Rightarrow a \in \sqrt{I} \quad \text{span style="color: red;">□}$$

Pareil pour $\sqrt{I \cap J} \subset \sqrt{J}$ □

" $\supset$ "

Soit $a \in \sqrt{I} \cap \sqrt{J}$. Montrer que $a \in \sqrt{I \cap J}$

On a: $\left(\begin{array}{l} \exists n \in \mathbb{N}^*, a^n \in I \\ \exists p \in \mathbb{N}^*, a^p \in J \end{array} \right)$ et on veut m. pr: $\left(\exists s \in \mathbb{N}^*, a^s \in I \cap J \right)$

On a $\left(\begin{array}{l} \forall k \geq n, a^k \in I \\ \forall k \geq p, a^k \in J \end{array} \right)$

Alors en prenant $s = \max(n, p)$ (ou $s = n + p$), on aura $\begin{pmatrix} a^s \in I \\ a^s \in J \end{pmatrix}$ □

2) Soient I et J deux idéaux de A et $n \in \mathbb{N}^*$. Montrer que

a) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$, b) $\sqrt{\sqrt{I}} = \sqrt{I}$, c) $\sqrt{I^n} = \sqrt{I}$

i) $\sqrt{I} \subset \sqrt{\sqrt{I}}$

Ça vient de 1), vu que $\sqrt{I}$ est un idéal.

ii) $\sqrt{\sqrt{I}} \subset \sqrt{I}$

Soit $a \in \sqrt{\sqrt{I}}$. Montrer que $a \in \sqrt{I}$.
 $(\exists n \in \mathbb{N}^*, a^n \in \sqrt{I})$

$$\Rightarrow \exists n \in \mathbb{N}^*, \exists p \in \mathbb{N}^*, (a^n)^p \in I$$

$$\Rightarrow a^{np} \in I$$

$$\Rightarrow a \in \sqrt{I} \quad \square$$

2) Soient I et J deux idéaux de A et $n \in \mathbb{N}^*$. Montrer que

a) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$, b) $\sqrt{\sqrt{I}} = \sqrt{I}$, c) $\sqrt{I^n} = \sqrt{I}$

Notation (naturelle)

$$I^n = \{i^n / i \in I\}$$

i) $\sqrt{I^n} \subset \sqrt{I}$

Soit $a \in \sqrt{I^n}$. Montrer $a \in \sqrt{I}$

$$(\exists p \in \mathbb{N}^*, a^p \in I^n)$$

$$\Rightarrow (\exists p \in \mathbb{N}^*, \exists i \in I, a^p = i^n)$$

On veut montrer: $(\exists s \in \mathbb{N}^*, a^s \in I)$

$$\text{On a } i^n \in I \quad (\text{car } i^n = \underbrace{i}_{\in I} \cdot \underbrace{i^{n-1}}_{\in A} \in I)$$

$$\text{Donc } a^p \in I$$

$$\Rightarrow a \in \sqrt{I} \quad \square$$

ii) $\sqrt{I} \subset \sqrt{I^n}$?

Soit $a \in \sqrt{I}$. Montrer $a \in \sqrt{I^n}$

$$\text{On veut: } (\exists p \in \mathbb{N}^*, a^p \in I)$$

On veut montrer: $(\exists s \in \mathbb{N}^*, a^s \in I^n)$

$$\text{C'est-à-dire: } (\exists s \in \mathbb{N}^*, \exists i \in I, a^s = i^n)$$

$$\text{On veut: } (\exists p \in \mathbb{N}^*, a^p \in I) \Rightarrow (\exists i \in I, a^p = i)$$

$$\Rightarrow a^{np} = i^n$$

$$\text{Et c'est fini } (s = np) \quad \square$$

3) Ici $A = \mathbb{Z}$. Déterminer le radical de l'idéal $n\mathbb{Z}$, où $n \in \mathbb{N}^*$.

$$\sqrt{n\mathbb{Z}} = ?$$

Soit $a \in \mathbb{Z}$.

$$a \in \sqrt{n\mathbb{Z}} \Leftrightarrow (\exists p \in \mathbb{N}^*, a^p \in n\mathbb{Z})$$

$$\Leftrightarrow (\exists p \in \mathbb{N}^*, n \mid a^p)$$

Notons $n = q_1^{m_1} \cdots q_s^{m_s}$: la décomposition de n en produit de

facteurs premiers.

$$a \in \sqrt{n}\mathbb{Z} \Leftrightarrow (\exists p \in \mathbb{N}^*, q_1^{m_1} \cdots q_s^{m_s} \mid a^p)$$

$$\Rightarrow (\forall 1 \leq i \leq s, q_i \mid a)$$

$$\Rightarrow (q_1 \cdots q_s) \mid a$$

$$\Rightarrow a \in (q_1 \cdots q_s)\mathbb{Z}$$

D'où

$$\sqrt{n}\mathbb{Z} \subset (q_1 \cdots q_s)\mathbb{Z}$$

Voyons l'autre inégalité :

Soit $x \in (q_1 \cdots q_s)\mathbb{Z}$. Existe-t-il $r \in \mathbb{N}^*$ tel que $x^r \in n\mathbb{Z}$.

$$\text{Càd : } n = q_1^{m_1} \cdots q_s^{m_s} \mid x^r$$

$$\text{On a } x = q_1 \cdots q_s \cdot d, \text{ où } d \in \mathbb{Z}.$$

$$\text{Alors existe-t-il } r \in \mathbb{N}^* \text{ tel que } (q_1^{m_1} \cdots q_s^{m_s}) \mid (q_1^r \cdots q_s^r \cdot d^r)$$

est bien, tout r vérifiant $(\forall 1 \leq i \leq s, m_i \leq r)$ convient.

Par exemple $r = \max(m_1, \dots, m_s)$ convient.



Bonfin :

$$\text{Avec } n = q_1^{m_1} \cdots q_s^{m_s}, \text{ on a } \sqrt{n}\mathbb{Z} = (q_1 \cdots q_s)\mathbb{Z}$$



Fin Exercice

Exercice 8 :

Considérons la matrice carrée d'ordre n , $T = (T_{ij})$ définie par

$$T_{ij} = \begin{cases} 1 & \text{si } i|j \\ 0 & \text{sinon} \end{cases}$$

Notons $D = \text{diag}(\varphi(1), \dots, \varphi(n))$, où φ l'indicatrice d'Euler.

Admettons l'égalité

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

- 1) Calculer le (i, j) ème coefficient de la matrice tTDT en fonction de $i \wedge j$.
- 2) En déduire $\det(S)$; où $S = (i \wedge j)_{1 \leq i, j \leq n}$. Dite la matrice de *Smith*.

1) $({}^tTDT)_{ij} = i \wedge j$; en effet !

On a :

$$({}^tTDT)_{ij} = \sum_{k=1}^n ({}^tT)_{ik} (DT)_{kj}$$

$$= \sum_{k=1}^n T_{ki} (DT)_{kj}$$

$$= \sum_{k=1}^n T_{ki} \cdot \left(\sum_{s=1}^n D_{ks} T_{sj} \right)$$

$$= \sum_{k=1}^n T_{ki} \varphi(k) T_{kj}$$

car $\left| \begin{array}{l} \forall s \neq k, D_{ks} = 0 \\ D_{kk} = \varphi(k) \end{array} \right.$

On a

$$T_{ij} = \begin{cases} 1 & \text{si } i|j \\ 0 & \text{sinon} \end{cases}$$



Alors

Si $\begin{pmatrix} k \chi_i \\ \text{ou} \\ k \chi_j \end{pmatrix}$ on aura $T_{ki} \varphi(k) T_{kj} = 0$

Ainsi :

$$({}^t T D T)_{ij} = \sum_{k/i \text{ et } k/j} T_{ki} \varphi(k) T_{kj}$$

$\downarrow$ $\downarrow$
 $=1$ $=1$
 Car $k|i$ Car $k|j$

$$= \sum_{k/i \text{ et } k/j} \varphi(k)$$

$(k|i \text{ et } k|j) \Leftrightarrow k|(i \wedge j)$
Rappel d'arithmétique

$$= \sum_{k/(i \wedge j)} \varphi(k)$$

$$= i \wedge j$$

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

Rappel

2) En déduire $\det(S)$; où $S = (i \wedge j)_{1 \leq i, j \leq n}$. Dite la matrice de Smith.

On a : $\left(\forall i, j \in [1, n], ({}^t T \mathcal{D} T)_{ij} = i \wedge j = S_{ij} \right)$

D'où $S = {}^t T \cdot \mathcal{D} \cdot T$

Alors :

$$\det(S) = \det({}^t T \cdot \mathcal{D} \cdot T)$$

$$= \underbrace{\det({}^t T)}_{= \det(T)} \times \det(\mathcal{D}) \times \det(T) \quad \left(\begin{array}{l} \text{car } \det \\ \text{est multiplicatif} \end{array} \right)$$

$$= (\det(T))^2 \times \det(\mathcal{D})$$

On a $T_{ij} = \begin{cases} 1 & \text{si } i|j \\ 0 & \text{sinon} \end{cases}$

Alors si $i \nmid j$ on a $T_{ij} = 0$

et c'est le cas si $i > j$ (la partie inférieure de la matrice T)

D'où :

$$T = \begin{pmatrix} T_{11} & & & \\ T_{21} & T_{22} & & \\ \vdots & & \ddots & \\ T_{n1} & & & T_{nn} \end{pmatrix} \xrightarrow[\text{Car } i/i]{T_{ii}=1} \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & \text{O} & \\ & & & 1 \end{pmatrix}$$

Alors $\boxed{\det(T) = 1}$

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

Can $D = \text{diag}(\varphi(1), \dots, \varphi(n))$.

On fin!

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



FIN