STRUCTURES ALGÉBRIQUES
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 $a^p = 0$.

1) Soient a et b deux éléments nilpotents de A et qui commuttent.
   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 1ère 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 $(\mathbb{Q},+,\times)$

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

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

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

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

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

D'où $\mathbb{Q} \subset B$

Et donc $\boxed{B = \mathbb{Q}}$ (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 :

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

Sous-corps

Déf :

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

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

Supp H s-gr de $(G,\cdot)$. On a :
$(a \in H) \Rightarrow (\forall m \in \mathbb{Z},\ a^m \in H)$

Supp H s-gr de $(G,+)$. 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 $i \neq 0$.

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 $(K,+,\times)$.

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

$\Rightarrow$ i inversible, car K Corps.

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

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)

$= (f(\sqrt{x}))^2 \geq 0$. □

---

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

M que $f(x) \leq f(y)$.

On a :

$f(y) = f((y-x)+x)$

$= f(y-x) + f(x)$ (car f morph d'anneaux)

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

Alors $f(y) \geq f(x)$ □

---

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

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

Ainsi :

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

$= m \times f\left(\frac{1}{n}\right)$ (car f morph d'ann)

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

D'autre part, on a :

$1 = f(1)$ (f morph d'ann)

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

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

D'où $f\left(\frac{1}{n}\right) = \frac{1}{n}$

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

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

$= r$ □

---

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

Soit $x \in \mathbb{R}$. Montrons 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 croissante $\Rightarrow \underbrace{f(r)}_{= r} \leqslant f(x)$

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

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

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

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

$\Rightarrow \boxed{f(x) \leqslant r}$, ce qui contredit $r < f(x)$.

□

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 $H = <\overline{a}>$, où a divise n.

2) Soit d un entier divisant n. Notons $a = n/d$. Montrer que :
   i) $<\overline{a}>$ 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 $\begin{cases} H = <\bar{a}> \\ a/n \end{cases}$

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

On a $H = \{\bar{0}\}$

$= <\bar{0}>$ (Mais $0 \times n$)

$= <\bar{n}>$, et n/n

$a = n$ convient alors.

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

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

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

Supposons l'existence d'un tel a.

On a alors $H = <\bar{a}> = \{\bar{0}, \bar{a}, \overline{2a}, \overline{3a}, \ldots\}$

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

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

Fin brouillon

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

Notons $a = \min\left(\{k \geq 1 \,/\, \bar{k} \in H\}\right)$.

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

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

$a = \min\left(\{k \geq 1 \,/\, \bar{k} \in H\}\right)$

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 $\bar{x} \in H$.

$\langle \bar{a} \rangle = \{k\bar{a} \,/\, k \in \mathbb{Z}\}$ Rappel

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

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

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

$$\Rightarrow \bar{x} = k.\bar{a} + \bar{r}$$

($\bar{x} \in H$, $k.\bar{a} \in H$)

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

Ainsi on a | $\bar{r} \in H$; $0 \leq r < a$; $a = \min(\{k \geq 1 / \bar{k} \in H\})$

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

D'où $\boxed{r = 0}$.

Et $\bar{x} = k.\bar{a} + \bar{r}$ devient $\bar{x} = k.\bar{a}$

CQFD

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

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

i) $< \bar{a} >$ 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 $o(\langle \bar{a} \rangle) = o(\bar{a})$.

Rappels

Si $(G,.)$ groupe et $x \in G$. On a :
$o(x) = d \Leftrightarrow \left(\forall k \in \mathbb{Z},\ x^k = e \Leftrightarrow d/k\right)$

Si $(G,+)$ groupe et $x \in G$. On a :
$o(x) = d \Leftrightarrow \left(\forall k \in \mathbb{Z},\ kx = 0 \Leftrightarrow d/k\right)$

On a :

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

$\Leftrightarrow (\forall k \in \mathbb{Z},\ \overline{ka} = \bar{0} \Leftrightarrow d/k)$

$\Leftrightarrow (\forall k \in \mathbb{Z},\ n/ka \Leftrightarrow d/k)$

$\Leftrightarrow (\forall k \in \mathbb{Z},\ da/ka \Leftrightarrow d/k)$

Ce qui est vrai

D'où $\boxed{o(\bar{a}) = d}$ □

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

Montrons que : $H = \langle \bar{a} \rangle$

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

Notons $n = a' \cdot d'$

On a
- $o(\overline{a'}) = d'$ (comme dans A))
- $o(\overline{a'}) = o(\langle a' \rangle) = o(H) = d$

D'où $d = d'$

Et $\begin{pmatrix} n = ad \\ n = a'd' \end{pmatrix} \Longrightarrow \boxed{a = a'}$

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

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

i) $< \bar{a} >$ 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 $A_d = \{ \bar{x} \in \mathbb{Z}/n\mathbb{Z} \ / \ o(\bar{x}) = d \}$

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.

On a :

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

$\iff \langle \bar{x} \rangle = \langle \bar{a} \rangle$ (car $\langle \bar{a} \rangle$ est l'unique 1-groupe d'ordre d)

pour dire

$\iff \bar{x}$ est un générateur de $\langle \bar{a} \rangle$

D'où

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

Enfin : Card $(A_d) = \varphi(d)$. CQFD

---

3) Conclure.

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

En effet :

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

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

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

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

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.

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

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

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

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

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

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

(α) $0 \in \sqrt{I}$?

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

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

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

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

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

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

Car $a^i = \underbrace{a^n}_{\in I} \times \underbrace{a^{i-n}}_{\in A} \in I$, car I 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 : $(\forall\, 0 \leq i \leq s,\ a^i b^{s-i} \in I)$

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

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

Reste à ce que le s cherché vérifie :

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

Il suffit que l'on ait :

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

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

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

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

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

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

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

Et on a :

$$(a+b)^{n+p} = \sum_{i=0}^{n+p} C_{n+p}^{i}\, a^i \times b^{n+p-i}$$

$$= \underbrace{\sum_{i=0}^{n-1} C_{n+p}^{i}\, \underbrace{a^i}_{\in A} \times \underbrace{b^{n+p-i}}_{\in I \text{ car } n+p-i \geq p}}_{\in I} + \underbrace{\sum_{i=n}^{n+p} C_{n+p}^{i}\, \underbrace{a^i}_{\in I \text{ car } i \geq n} \times \underbrace{b^{n+p-i}}_{\in A}}_{\in I}$$

$\in I$

D'où $\boxed{(a+b)^{n+p} \in I}$

Et donc $\boxed{(a+b) \in \sqrt{I}}$

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

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

Et on a : $(ab)^n = \underbrace{a^n}_{\in I} \times \underbrace{b^n}_{\in A} \in I$ (A ann commutatif)

D'où $(ab)^n \in I$

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

Fin 1°)

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

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

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

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

"$\subset$"

Soit $a \in \sqrt{IJ}$. M 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 m que : $(\exists p \in \mathbb{N}^*,\ a^p \in I$ et $a^p \in J)$

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

C'est fini ($p = n$ convient) □

"$\supset$"

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

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

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

On a : $a^n \times a^n = a^{2n}$ ($a^n \in I$, $a^n \in J$), alors c'est fini : | i c'est a^n ; j c'est a^n ; $p = 2n$

□

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

"$\subset$"

Revient 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 $a \in \sqrt{I \cap J}$. M que $a \in \sqrt{I}$

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

$\Rightarrow a \in \sqrt{I}$ □

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

" $\supset$ "

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

On a : $\begin{pmatrix} \exists n \in \mathbb{N}^*, a^n \in I \\ \exists p \in \mathbb{N}^*, a^p \in J \end{pmatrix}$ et on veut m. que : $(\exists s \in \mathbb{N}^*, a^s \in I \text{ et } a^s \in J)$

On a $\begin{pmatrix} \forall k \geq n, a^k \in I \\ \forall k \geq p, a^k \in J \end{pmatrix}$

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 $a \in \sqrt{\sqrt{I}}$. Mque $a \in \sqrt{I}$.

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

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

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

$\Rightarrow a \in \sqrt{I}$ □

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 $a \in \sqrt{I^n}$. M.q. $a \in \sqrt{I}$

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

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

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

On a $i^n \in I$ (car $i^n = i \cdot i^{n-1} \in I$, $i \in I$, $i^{n-1} \in A$)

D'où $a^p \in I$

$\Rightarrow a \in \sqrt{I}$ □

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

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

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

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

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

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

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

Et c'est fini $(s = np)$ □

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.

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

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

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

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

D'où $\boxed{\sqrt{n\mathbb{Z}} \subset (q_1 \cdots q_s)\mathbb{Z}}$

Voyons l'autre inégalité :

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

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

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

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

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

Par exemple $\boxed{r = \max(m_1, \ldots, m_s) \text{ convient.}}$ □

Enfin :

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

□

Fin Exercice 7

Exercice 8 :

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

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

Notons $D = diag(\varphi(1), \ldots, \varphi(n))$, 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 coéfficient 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) $\boxed{({}^tT\,D\,T)_{ij} = i \wedge j}$; en effet :

On a :

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

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

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

$$= \sum_{k=1}^{n} T_{ki}\, \varphi(k)\, T_{kj} \quad \text{car} \quad \begin{cases} \forall s \neq k,\ D_{ks} = 0 \\ D_{kk} = \varphi(k) \end{cases}$$

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

Alors Si $\begin{pmatrix} k \nmid i \\ ou \\ k \nmid j \end{pmatrix}$ on aura $T_{ki}\ \varphi(k)\ T_{kj} = 0$

Ainsi :

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

$T_{ki} = 1$ car $k|i$; $T_{kj} = 1$ 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 : $\left(\forall i, j \in [\![1, n]\!], ({}^tT D T)_{ij} = i \wedge j = S_{ij}\right)$

D'où $S = {}^tT . D . T$

Alors :

$$det(S) = det({}^tT . D . T)$$

$$= \underbrace{det({}^tT)}_{= det(T)} \times det(D) \times det(T) \quad \left(\text{car det est multiplicatif}\right)$$

$$= (det(T))^2 \times det(D)$$

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

Alors si $i \not| j$ on aura $T_{ij} = 0$

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

D'où : $T = \begin{pmatrix} T_{11} & & * \\ T_{21} & T_{22} & \\ \vdots & & \ddots \\ T_{n1} & \cdots & T_{nn} \end{pmatrix} \overset{T_{ii} = 1}{=\!=} \begin{pmatrix} 1 & & * \\ & \ddots & \\ & & 1 \end{pmatrix}$

Car i / i

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

Et on a $\det(D) = \prod_{k=1}^{n} \varphi(k)$

Car $D = diag(\varphi(1), \ldots, \varphi(n))$

Enfin !

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

Fin