Corrigé du DS1

Problème : Anneau des entiers de Gauss

Un anneau A commutatif est dit principal lorsque tout idéal de A est engendré par un élément.

Q1. On sait que les idéaux de l'anneau $(\mathbb{Z},+,\times)$ sont les $n\mathbb{Z}$ avec $n\in\mathbb{N}$ et les idéaux de l'anneau $(\mathbb{R}[X],+,\times)$ sont les $P\mathbb{R}[X]$ avec $P\in\mathbb{R}[X]$; donc

$\boxed{\mathbb{Z} \text{ et } \mathbb{R}[X] \text{ sont des anneaux principaux.}}$

Propriétés de l'anneau $\mathbb{Z}[i]$

On appelle entier de Gauss un nombre complexe dont la partie réelle et la partie imaginaire sont des entiers relatifs : $u=a+ib,(a,b)\in\mathbb{Z}^2$. On désigne par $\mathbb{Z}[i]$ l'ensemble des entiers de Gauss.

Q2. • $\mathbb{Z}[i]\subset\mathbb{C}$;

- $1=1+0i\in\mathbb{Z}[i]$ car $1,0\in\mathbb{Z}$;
- soit $u,v\in\mathbb{Z}[i]$, donc il existe $a,b,c,d\in\mathbb{Z}$ tels que $u=a+ib, v=c+id$, donc :

$$u-v=(a-c)+(b-d)i\in\mathbb{Z}[i]$$

car $a-c,b-d\in\mathbb{Z}$ ($\mathbb{Z}$ est un anneau) ; et

$$uv=(ac-bd)+(ad+bc)\in\mathbb{Z}[i]$$

donc :

$\boxed{\mathbb{Z}[i] \text{ est un sous-anneau de } \mathbb{C}.}$

De plus $\mathbb{C}$ est un corps, donc intègre donc :

$\boxed{\mathbb{Z}[i] \text{ est intègre.}}$

Enfin : $2=2+0i\in\mathbb{Z}[i]$, mais $\frac{1}{2}\notin\mathbb{Z}[i]$ (par unicité de la partie réelle), donc

$\boxed{\mathbb{Z}[i] \text{ n'est pas un corps.}}$

Q3. a) Soit $u\in\mathbb{Z}[i]$, donc il existe $a,b\in\mathbb{Z}$ tels que $u=a+ib$ et

$$|u|^2=a^2+b^2\in\mathbb{Z} \text{ car } a,b\in\mathbb{Z}$$

et a^2,b^2 sont positifs comme carrés de réels ; donc : $|u|^2\in\mathbb{N}$. D'où :

$\boxed{\text{pour tout } u\in\mathbb{Z}[i], |u|^2 \text{ est un entier naturel.}}$

b) Soit $u\in\mathbb{Z}[i]$;

- on suppose u inversible dans $\mathbb{Z}[i]$, donc il existe $v\in\mathbb{Z}[i]$ tel que $uv=1$, donc : $|u|\,|v|=|1|$, donc $|u|^2|v|^2=1$. Or $|u|^2,|v|^2\in\mathbb{N}$ d'après la question précédente, donc $|u|^2$ est inversible dans $\mathbb{Z}$, donc $|u|^2\in\{-1,1\}$ et $|u|^2\geqslant 0$, donc $|u|^2=1$ et $|u|=1$.
- réciproquement, on suppose $|u|=1$, donc $|u|^2=1$, donc $u\times\bar{u}=1$, donc u est inversible dans l'anneau (commutatif) $\mathbb{Z}[i]$.

D'où :

$\boxed{u \text{ est inversible dans } \mathbb{Z}[i] \text{ si et seulement si } |u|=1.}$

c) Les inversibles de $\mathbb{Z}[i]$ sont les éléments de $\mathbb{Z}[i]$ de module 1, c'est à dire $1,-1,i,-i$, ils forment un groupe (le groupe des inversibles de l'anneau $\mathbb{Z}[i]$) cyclique engendré par i.

$\boxed{\text{l'ensemble des éléments inversibles de l'anneau } \mathbb{Z}[i] \text{ est le groupe cyclique } \mathrm{gr}(i).}$

Q4. a) Soit $u,v\in\mathbb{Z}[i]$ tles que $u\mid v$ dans $\mathbb{Z}[i]$,
donc il existe $q\in\mathbb{Z}[i]$ tel que $v=qu$, donc $|v|^2=|q|^2|u|^2$, or $|v|^2,|q|^2,|u|^2\in\mathbb{N}$, donc : $|u|^2\mid|v|^2$ dans $\mathbb{N}$.

$\boxed{\text{si } u \text{ divise } v \text{ dans } \mathbb{Z}[i], \text{ alors } |u|^2 \text{ divise } |v|^2 \text{ dans } \mathbb{N}.}$

b) $4+7i=(2+i)(3+2i)$, donc

$\boxed{2+i \text{ divise } 4+7i \text{ dans } \mathbb{Z}[i]\,;}$

et pour $a,b\in\mathbb{Z}$:

$$4+7i=(2-i)(a+ib)\Leftrightarrow\begin{cases}4=2a+b\\7=-a+2b\end{cases}\quad L_2\leftarrow 2L_2+L_1$$
$$\Leftrightarrow\begin{cases}4=2a+b\\18=5b\end{cases}$$

or l'équation $5b=18$ d'inconnue $b\in\mathbb{Z}$ n'a pas de solution, donc l'équation $4+7i=(2-i)(a+ib)$ n'a pas de solution, donc

$\boxed{(2-i) \text{ ne divise pas } (4+7i) \text{ dans } \mathbb{Z}[i],}$

pourtant $|2-i|^2=5$ divise $|4+7i|^2=65$, donc :

$\boxed{\text{la réciproque de la question précédente est fausse.}}$

c) On considère la relation binaire : $u\mathcal{R}v\Leftrightarrow u$ et v sont associés.

- $\forall u \in \mathbb{Z}[i], u \mid u$, donc $u\mathcal{R}u$; $\mathcal{R}$ est refléxive ;
- soit $u, v \in \mathbb{Z}[i]$ tels que $u\mathcal{R}v$, donc $u \mid v$ et $v \mid u$ donc $v\mathcal{R}u$; $\mathcal{R}$ est symétrique.
- soit $u, v, w \in \mathbb{Z}[i]$ tels que $u\mathcal{R}v$ et $v\mathcal{R}w$, donc $u \mid v$ et $v \mid w$ et (par transitivité de la relation $|$,) $u \mid w$ et de même $w \mid u$, donc $u\mathcal{R}w$; $\mathcal{R}$ est transitive.

Donc :

$\mathcal{R}$ est une relation d'équivalence.

Soit $u = a + ib \in \mathbb{Z}[i]$ avec $a, b \in \mathbb{Z}$, et $v \in \mathbb{Z}[i]$

$$\begin{aligned} v \in Cl(u) &\Leftrightarrow u \text{ et } v \text{ sont associés} \\ &\Leftrightarrow \exists q \in \mathbb{Z}[i]^* \mid v = qu \\ &\Leftrightarrow v = u \text{ ou } v = -u \text{ ou } v = iu \text{ ou } v = -iu \end{aligned}$$

car $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$. D'où

$$Cl(a + ib) = \{a + ib, -b + ia, -a - ib, b - ia\}.$$

Q5. a) Soit $z \in \mathbb{C}$, donc il existe $x, y \in \mathbb{R}$ tels que $z = x + iy$; on sait que $\lfloor x \rfloor \leqslant x < \lfloor x \rfloor + 1$, on pose :

$$a = \begin{cases} \lfloor x \rfloor & \text{si } \lfloor x \rfloor \leqslant x < \lfloor x \rfloor + \frac{1}{2} \\ \lfloor x \rfloor + 1 \text{ si } \lfloor x \rfloor + \frac{1}{2} \leqslant x < \lfloor x \rfloor + 1 \end{cases}$$

ainsi, dans tous les cas $|x - a| \leqslant \frac{1}{2}$;
et de même pour

$$b = \begin{cases} \lfloor y \rfloor & \text{si } \lfloor y \rfloor \leqslant y < \lfloor y \rfloor + \frac{1}{2} \\ \lfloor y \rfloor + 1 \text{ si } \lfloor y \rfloor + \frac{1}{2} \leqslant y < \lfloor y \rfloor + 1 \end{cases}$$

on obtient : $|y - b| \leqslant \frac{1}{2}$. On pose $u = a + ib \in \mathbb{Z}[i]$, donc : $|z - u|^2 = |x - a|^2 + |y - b|^2 \leqslant (\frac{1}{2})^2 \times 2 = \frac{1}{2} < 1$;
donc : $|z - u| < 1$. Donc :

pour tout nombre complexe z, il existe un entier de Gauss u tel que $|z - u| < 1$.

b) Soit $(u, v) \in \mathbb{Z}[i]^2$, avec $v \neq 0$.
On pose $z = \frac{u}{v} \in \mathbb{C}$, d'après la question précédente, il existe $q \in \mathbb{Z}[i]$ tel que $|z - q| < 1$, on pose $r = u - qv$, on a alors : $u = qv + r$ et $|r| = |v(z - q)| = |v| \times |z - q| < |v|$ (car $|z - q| < 1$ et $|v| > 0$). D'où

pour tout couple $(u, v) \in \mathbb{Z}[i]^2$, avec $v \neq 0$, il existe un couple $(q, r) \in \mathbb{Z}[i]^2$ tel que $u = vq + r$ avec $|r| < |v|$.

c) Soit $u = 1 - i$ et $v = 2i$, et $q, r \in \mathbb{Z}[i]^2$,
analyse, on suppose $u = qv + r$ et $|r| < |v|$, donc : $\frac{u}{v} = q + \frac{r}{v}$ et $\left|\frac{u}{v} - q\right| < 1$ or $\frac{u}{v} = -\frac{1}{2} - \frac{1}{2}i$, donc $q \in \{0, -1, -1 - i, -i\}$;
ce qui donne $(q, r) \in \{(0, 1 - i), (-1, 1 + i), (-1 - i, -1 + i), (-i, -1 - i)\}$.
synthèse : on vérifie que les 4 couples sont bien solutions.

D'où :

le couple (q, r) n'est pas unique, pour $u = 1 - i$ et $v = 2i$, les solutions sont : $(0, 1 - i), (-1, 1 + i), (-1 - i, -1 + i), (-i, -1 - i)$.

Q6. Soit I un idéal de $\mathbb{Z}[i]$.

1er cas : $I = \{0\}$, donc : $I = 0\mathbb{Z}[i]$ est engendré par 0.

2e cas : $I \neq \{0\}$, donc $A = \left\{|x|^2 ; \text{ avec } x \in I \setminus \{0\}\right\}$ est une partie non vide de $\mathbb{N}$ (d'après **Q0.a**), donc A a un minimum n_0 et il existe $x \in A$ tel que $|x|^2 = n_0$. Ainsi : $\forall u \in I \setminus \{0\}, |u| \geqslant |x|$.

Par propriété d'idéal $x\mathbb{Z}[i] \subset I$. Réciproquement, soit $u \in I$, comme $x \neq 0$, d'après la question **Q0.b**, il existe $q, r \in \mathbb{Z}[i]$ tels que $u = qx + r$ avec $|r| < |x|$. Or $u, q \in I$ et I est un idéal, donc $r = u - qx \in I$ et $|r| < |x|$; donc $r = 0$, donc $u = qx \in x\mathbb{Z}[i]$.

Ce qui montre que $I = x\mathbb{Z}[i]$.

Conclusion :

L'anneau $\mathbb{Z}[i]$ est principal.

Irréductibles de $\mathbb{Z}[i]$

Un entier de Gauss u, non nul est non inversible, est dit irréductible lorsque : $\forall x, y \in \mathbb{Z}[i]$,

$$xy = u \Rightarrow x \in (\mathbb{Z}[i])^* \text{ ou } y \in (\mathbb{Z}[i])^*.$$

Q7. Soit $u \in \mathbb{Z}[i]$ non irréductible, donc il existe $x, y \in \mathbb{Z}[i]$ non inversibles tels que $u = xy$. Donc $|u|^2 = |x|^2 |y|^2$, or $|u|^2, |x|^2, |y|^2 \in \mathbb{N}$; de plus x et y ne sont pas inversibles, donc $|x|^2 \neq 1, |y|^2 \neq 1$; donc $|x|^2$ n'est pas premier dans $\mathbb{N}$.
Conclusion, par contraposée :

si $\lvert u\rvert^2$ est premier dans $\mathbb{N}$, alors u est irréductible dans $\mathbb{Z}[i]$.

Q8. $2 = (1+i)(1-i)$ avec $1+i, 1-i \in \mathbb{Z}[i]$ non inversibles, donc 2 n'est pas irréductible dans $\mathbb{Z}[i]$.
On suppose par l'absurde que 3 n'est pas irréducitble dans $\mathbb{Z}[i]$, donc il existe $x, y \in \mathbb{Z}[i]$ tels que $3 = x \times y$ et $|x| \neq 1$, $|y| \neq 1$. Donc : $|x|^2 |y|^2 = 9 = 3^2$ et $|x|^2, |y|^2 \in \mathbb{N} \setminus \{1\}$, donc $|x| = 3$ et $|y|^2 = 3$. On pose $x = a + ib$ avec $a, b \in \mathbb{Z}$, donc $a^2 + b^2 = 3$; ce qui impose $|a| \leqslant 1$ et $|b| \leqslant 1$ et aucune des combinaison possible n'est solution. D'où la contradiction.
Donc : 3 est irréductible ; pourtant $|3|^2 = 9$ n'est pas premier.
Donc :

2 est irréductible, 3 n'est pas irréductible, la réciproque de la question précédente est fausse.

Q9. Montrons par récurrence forte : $\forall n \in \mathbb{N}$ avec $n \geqslant 2, \mathcal{P}(n) : \forall x \in \mathbb{Z}[i], |x|^2 = n \Rightarrow$ x a un diviseur irréductible dans $\mathbb{Z}[i]$.

Initialisation pour $n = 2$;
Soit $x \in \mathbb{Z}[i]$ tel que $|x|^2 = 2$, donc $|x|^2$ est premier dans $\mathbb{N}$, donc x est irréductible dans $\mathbb{Z}[i]$.

Hérédité soit $n \geqslant 2$, on suppose : $\forall k \in [\![2 ; n]\!], \mathcal{P}(n)$; soit $x \in \mathbb{Z}[i]$ tel que $|x|^2 = n+1$.

1er cas : x est irréductible , donc x a un diviseur irréductible : lui même.

2e cas : sinon alors il existe $u, v \in \mathbb{Z}[i]$ non inversibles tels que $x = uv$ et u, v non nuls car $uv = x \neq 0$. Donc : $|u|^2 > 1$ et $|v|^2 > 1$, donc : $2 \leqslant |u|^2 < |x|^2 = n + 1$ et par hypothèse de récurrence, u a un diviseur irréductible dans $\mathbb{Z}[i]$.

D'où $\mathcal{P}(n+1)$ dans tous les cas.

Conclusion : par principe de récurrence :

tout élément de $\mathbb{Z}[i]$ a un diviseur irréductible dans $\mathbb{Z}[i]$.

Q10. Soit $x \in \mathbb{Z}[i]$ irréductible dans $\mathbb{Z}[i]$ et $u, v \in \mathbb{Z}[i]$ tels que $\bar{x} = uv$; donc $x = \bar{u}\bar{v}$, or x est irréductible, donc $\bar{u} \in \mathbb{Z}[i]^* = \{1, -1, i, -1\}$ ou $\bar{v} \in \mathbb{Z}[i]^* = \{1, -1, i, -1\}$; donc : $u \in \{1, -1, -i, i\} = \mathbb{Z}[i]$ ou $v \in \mathbb{Z}[i]$.
On a montré que $\bar{x}$ est irréductible. D'où :

si $x \in \mathbb{Z}[i]$ est irréductible dans $\mathbb{Z}[i]$, alors $\bar{x}$ est irréductible dans $\mathbb{Z}[i]$.

On admet pour la suite que pour $u \in \mathbb{Z}[i]$ irréductible dans $\mathbb{Z}[i]$ et $x, y \in \mathbb{Z}[i]$:

$$u \mid (x \times y) \Rightarrow u \mid x \text{ ou } u \mid y.$$

Q11. Soit $u = a + ib$, avec $a \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z} \setminus \{0\}$, irréductible dans $\mathbb{Z}[i]$ et on suppose par l'absurde que $|u|^2$ n'est pas premier. Donc il existe $k, n \geqslant 2$ tels que $|u|^2 = k \times n$ (quitte à échanger k et n, on suppose $k \leqslant n$, donc $k \leqslant |u| \leqslant n$) et d'après la question **Q9** il existe y un diviseur irréductible de k dans $\mathbb{Z}[i]$, donc y est un diviseur irréductible de $|u|^2 = u \times \bar{u}$, donc $y \mid u$ ou $y \mid \bar{u}$.

1er cas : $y \mid u$ donc il existe $q \in \mathbb{Z}[i]$ tel que $u = qy$ or u est irréductible et y est irréductible, donc $q \in \mathbb{Z}[i]^* = \{1, -1, i, -i\}$, donc u et y sont associés. Or $y \mid k$, donc $u \mid k$. Or $k \neq 0$, donc $|u| \leqslant |k|$.
Or $|k| \leqslant |u|$, donc $|k| = |u|$ et u et k sont associés, ce qui est absurde car $k \in \mathbb{N}$ et u n'est ni réel ni imaginaire pur ; d'où la contradiction.

2e cas $y \mid \bar{u}$: de même en remplaçant u par $\bar{u}$.

Donc : $|u|^2$ est premier dans $\mathbb{N}$.

si $u = a + ib$, avec $a \in \mathbb{Z} \setminus \{0\}, b \in \mathbb{Z} \setminus \{0\}$, est irréductible dans $\mathbb{Z}[i]$, alors $\lvert u\rvert^2$ est premier dans $\mathbb{N}$.

Q12. Soit $a, b \in \mathbb{Z}$.

1er cas : a, b sont pairs.
donc : a^2 et b^2 sont pairs et $a^2 + b^2$ est pair, donc $a^2 + b^2 \not\equiv 3$ [4].

2e cas : a, b sont impairs.
donc : a^2 et b^2 sont impairs et $a^2 + b^2$ est pair, donc $a^2 + b^2 \not\equiv 3$ [4].

3e cas : a pair et b impair.
Donc il existe $c, d \in \mathbb{Z}$ tels que $a = 2c$ et $b = 2d + 1$, donc :

$$a^2 + b^2 = 4c^2 + 4d^2 + 4d + 1 \equiv 1 \text{ [4]}$$

4e cas : a impair et b pair ; de même que dans le cas précédent, $a^2 + b^2 \equiv 1$ [4].

Donc :

la somme de deux carrés d'entiers relatifs n'est jamais congrue à 3 modulo 4.

Soit p premier dans $\mathbb{N}$, on suppose par l'absurde que p n'est pas irréductible dans $\mathbb{Z}[i]$. Donc il existe $u, v \in \mathbb{Z}[i]$ non inversibles tels que $p = uv$; donc $|u|^2 |v|^2 = p^2$ avec $|u|^2, |v|^2 \in \mathbb{N}$ et $\left|u^2\right| \neq 1, |v|^2 \neq 1$. Comme p est premier, on en déduit $|u|^2 = p \equiv 3\ [4]$. Or $|u|^2$ est la somme de deux carrés d'entiers relatifs, d'où la contradiction. Donc :

un entier naturel congru à 3 modulo 4 premier dans $\mathbb{N}$ est irréductible dans $\mathbb{Z}[i]$.

Q13. On admet qu'un entier naturel congru à 1 modulo 4 premier dans $\mathbb{N}$ est toujours somme de deux carrés d'entiers naturels.

Soit p premier dans $\mathbb{N}$ tel que $p \equiv 1\ [4]$; donc il existe $a, b \in \mathbb{Z}^2$ tels que $p = a^2 + b^2 = (a+ib)(a-ib)$ et $|a+ib| = |a-ib| = p \neq 1$, donc $a+ib$ et $a-ib$ ne sont pas inversibles. Donc : p n'est pas irréductible dans $\mathbb{Z}[i]$.

Donc :

si p est un nombre premier congru à 1 modulo 4, alors il n'est pas irréductible dans $\mathbb{Z}[i]$.

Q14. Les éléments de $\mathbb{Z}[i]$ réels ou imaginaires purs sont associés à un entier naturel ; or un entier naturel non premier n'est pas irréductible dans $\mathbb{Z}[i]$, 2 est le seul nombre premier pair et il n'est pas irréductible, les nombres premiers impairs sont soit congrus à 1 modulo 4 et ne sont pas irréductibles, soit congru à 3 modulo 4 et sont premiers. Donc :

les éléments irréductibles de $\mathbb{Z}[i]$ sont : • les nombres premiers p congrus à 3 modulo 4 et leurs associés : $-p, ip, -ip$; • les éléments de la forme $a+ib$ avec a, b entiers non nuls tels que a^2+b^2 sont premiers.

Exercice : Nilpotents

Q15. a) Soit A un anneau intègre.

- Soit a un élément nilpotent de A, donc il existe $n \in \mathbb{N}$ tel que $a^n = 0_A$.
  Or $a^0 = 1_A \neq 0_A$, donc $n \geqslant 1$ et $a^n = a \times \cdots \times a = 0$. Donc par intégrité de A, au moins un des facteurs de ce produit est nul, donc $a = 0$.
  On a montré que $\mathcal{N}_A \subset \{0_A\}$.
- Réciproquement $0_A^1 = 0_A$, donc $0_A \in \mathcal{N}_A$.

Donc :

$$\boxed{\mathcal{N}_A = \{0_A\}.}$$

b) Soit $\beta \in \mathbb{Z}/21\mathbb{Z}$ nilpotent et $b \in \mathbb{Z}$ tel que $\bar{b} = \beta$.
Il existe $n \in \mathbb{N}$ tel que $\beta^n = \bar{0}$, donc $21 \mid b^n$.
Donc : $3 \mid b^n$ et $7 \mid b^n$; et comme 3 et 7 sont premiers, $3 \mid b$ et $7 \mid b$
De plus : $3 \wedge 7 = 1$, donc, d'après le lemme de Gauss, $21 \mid b$, donc $\beta = \bar{0}$.
Réciproquement, $\bar{0}$ est nilpotent car $\bar{0}^1 = \bar{0}$.
Donc :

$$\boxed{\mathcal{N}_{\mathbb{Z}/21\mathbb{Z}} = \{\bar{0}\}.}$$

Remarque : On pouvait également remarquer qu'un inversible ne peut pas être nilpotent, car l'ensemble des inversible est un groupe multiplicatif (qui ne contient pas 0_A), il ne reste plus qu'à tester les non inversibles $\bar{0}, \bar{3}$ et $\bar{7}$.

c) Soit $\beta \in \mathbb{Z}/9\mathbb{Z}$ nilpotent et $b \in \mathbb{Z}$ tel que $\bar{b} = \beta$.
Il existe $n \in \mathbb{N}$ tel que $\beta^n = \bar{0}$, donc $9 = 3^2 \mid b^n$.
Donc : $3 \mid b^n$, or 3 est premier, donc $3 \mid b$, donc $\beta \in \{\bar{0}, \bar{3}, \bar{6}\}$.
Réciproquement, $\bar{0}^1 = \bar{0}, \bar{3}^2 = \bar{0}, \bar{6}^2 = \bar{0}$.
Donc :

$$\boxed{\mathcal{N}_{\mathbb{Z}/9\mathbb{Z}} = \{\bar{0}, \bar{3}, \bar{6}\}.}$$

d) Soit p un nombre premier et $\alpha \geqslant 2$ un entier et $B = \mathbb{Z}/p^\alpha\mathbb{Z}$.
Soit $x \in B^\times$, comme $(B^\times, \times)$ est un groupe, pour tout $n \in \mathbb{N}, x^n \in B^\times$, donc $\forall n \in \mathbb{N}, x^n \neq \bar{0}$.
Donc : $B^\times \cap \mathcal{N}_B = \varnothing$.
Soit $x \notin B^\times$, et $k \in \mathbb{Z}$ tel que $\bar{k} = x$.
Donc : $k \wedge p^\alpha \neq 1$, or p est premier, donc $p \mid k$, donc il existe $q \in \mathbb{Z}$ tel que $k = pq$ et $k^\alpha = p^\alpha q^\alpha$, donc $x^\alpha = \bar{0}$: x est nilpotent.
Donc : $B^\times \cup \mathcal{N}_B = B$.
Conclusion :

$$\boxed{B^\times \text{ et } \mathcal{N}_B \text{ forment une partition de } B.}$$

Q16. a) On suppose que a et b sont des éléments nilpotents de A et commutent, donc il existe $n_1, n_2 \in \mathbb{N}$ tels que $a^{n_1} = 0_A$ et $b^{n_2} = 0_A$. Alors, d'après la formule du binôme, comme a et b commutent :

$$\begin{aligned}(a+b)^{n_1+n_2} &= \sum_{k=0}^{n_1+n_2} \binom{n_1+n_2}{k} a^k b^{n_1+n_2-k} \\ &= \sum_{k=0}^{n_1} \binom{n_1+n_2}{k} a^k b^{n_1+n_2-k} + \sum_{k=n_1+1}^{n_1+n_2} \binom{n_1+n_2}{k} a^k b^{n_1+n_2-k}\end{aligned}$$

Or, pour tout $k \in [\![0\,;n_1]\!], n_1 + n_2 - k \geqslant n_2$, donc $b^{n_1+n_2-k} = 0_A$ et

$$\sum_{k=0}^{n_1} \binom{n_1+n_2}{k} a^k b^{n_1+n_2-k} = 0_A$$

et, pour tout $k \in [\![0\,;n_1]\!], a^k = 0_A$, donc

$$\sum_{k=n_1+1}^{n_1+n_2} \binom{n_1+n_2}{k} a^k b^{n_1+n_2-k} = 0_A.$$

Donc : $(a+b)^{n_1+n_2} = 0_A$.
Donc :

si a et b de A sont nilpotents et commutent, alors $a+b$ est aussi nilpotent.

b) On suppose $a, b \in A$ et ab est nilpotent. Donc il existe $n \in \mathbb{N}$ tel que $(ab)^n = 0_A$.
Donc, par associativité :

$$(ba)^{n+1} = b(ab)^n a = b \times 0_A \times a = 0_A.$$

Donc :

Pour a et b dans A, si ab est nilpotent alors ba aussi.

c) On suppose que A est un anneau commutatif.

- $0_A \in \mathcal{N}_A$, car $0_A^1 = 0_A$;
- d'après **Q16**, $\mathcal{N}_A$ est stable par $+$;
- soit $a \in \mathcal{N}_A$ et $n \in \mathbb{N}$ tel que $a^n = 0_A$, donc $(-a)^n = (-1)^n 0_A = 0_A$. Donc $(-a) \in \mathcal{N}_A$.
- Soit $a \in \mathcal{N}_A$, $b \in A$ et $n \in \mathbb{N}$ tel que $a^n = 0_A$, comme A est commutatif, $(ab)^n = a^n b^n = 0_A \times b^n = 0_A$; donc $ab \in \mathcal{N}_A$.

Donc :

si A est un anneau commutatif, alors $\mathcal{N}_A$ est un idéal de A.