



DEVOIR SURVEILLÉ 1

Proposition de corrigé

Donné le : 05-10-2026

Année scolaire :
2026-2027

Classe : MP*

Préliminaire

1. (a) - On a I_u est un idéal de $\mathcal{A}$ car $I_u = \ker(\Phi_u)$, avec $\Phi_u : \mathbb{K}[X] \rightarrow \mathcal{A}, P \mapsto \Phi_u(P) = P(u)$, on a vu que Φ_u est un morphisme d'algèbres, donc $I_u = \ker(\Phi_u)$ est un idéal de $\mathbb{K}[X]$.

Attention / Piège classique

- Certains candidats n'ont pas démontré que I_u est un idéal.
- Certains le démontrent mais oublient de signaler que $I_u \neq \emptyset$.
- D'autres citent que c'est un idéal et le démontrent même mais ne disent pas *non nul*

- On a et que $I_u \neq \{0\}$ car la famille $(1_{\mathcal{A}}, u, \dots, u^N)$ est liée car elle possède $N+1$ vecteurs, donc il existe $\alpha = (\alpha_0, \dots, \alpha_N) \in \mathbb{K}^{N+1} \setminus \{0\}$ tel que $\sum_{k=0}^N \alpha_k u^k = 0$, donc pour

$$P(X) = \sum_{k=0}^N \alpha_k X^k, \text{ on a } P \neq 0 \text{ et } P(u) = 0$$

- Il en découle que l'idéal I_u possède un et un seul générateur π_u qui est le polynôme minimal de u .
- En particulier on a $I_u = \pi_u \mathbb{K}[X]$ et π_u est unitaire.

Prestation élève

Un élève a donné une démonstration par l'absurde du fait que I_u est non nul, comme suit : Si I_u est nul alors la famille $\mathcal{C} = (u, \dots, u^N)$ est libre et comme elle possède N éléments c'est une base, donc pour le vecteur u^{N+1} , il existe un unique $(\alpha_1, \dots, \alpha_N) \in \mathbb{K}^N$ tel que $u^{N+1} = \sum_{k=1}^N \alpha_k u^k$, en conséquence le polynôme

$L = X^{N+1} - \sum_{k=1}^N \alpha_k X^k$ réalise $L \neq 0$ et $L \in I_u$, ce qui contredit l'hypothèse, donc cette dernière est fausse donc $I_u \neq \{0\}$.

- (b) Par définition de $\pi_u \mathbb{K}[X]$, on a I_u est l'ensemble des multiples de π_u , donc, pour tout $P \in \mathbb{K}[X]$, on a $P \in I_u \Leftrightarrow \pi_u | P$.
- (c) i. On a : $u^2 = u$, donc le polynôme $X^2 - X$ est un polynôme annulateur de u , donc $\pi_u | X(X-1)$, donc $\pi_u \in \{X, X-1, X^2-X\}$, et plus précisément, on a :

- $\pi_M = X$ si $M = 0$,
- $\pi_M = X - 1$ si $M = I_n$,
- $\pi_M = X^2 - X$ si $M \neq 0$ et $M \neq I_n$, car alors $\pi_u \neq X$ et $\pi_u \neq X - 1$.

ii. Pour simplifier le travail, pour tout $N \in \mathbb{N}$, notons $S_N = \sum_{k=0}^N \frac{M^k}{k!}$.

- Pour tout $k \in \mathbb{N}^*$, on a $M^k = M$ car vrai pour $k = 1$ et si $k \in \mathbb{N}^*$ et $M^k = M$ alors $M^{k+1} = M^2 = M$.
- Si $N = 0$, alors on a $S_N = S_0 = I_n$.
- Si $N \in \mathbb{N}^*$, alors $S_N = I_n + \left(\sum_{k=1}^N \frac{1}{k!} \right) M$.

Pour les 5/2

On verra, après que $\exp(M) = \lim_{N \rightarrow +\infty} S_N = I_n + (e - 1)M$.

(d) i. • On propose deux méthodes :

Première méthode : On écrit $M = PE_{1,1}Q$ avec $P, Q \in \mathbf{GL}_n(\mathbb{K})$ puis $E_{1,1} = E_1 E_1^\top$, où $E_1 = (1, 0, \dots, 0)^\top$ est le premier vecteur de la base canonique de $\mathbb{K}^n$. donc $M = (PE_1)(Q^\top E_1)^\top$, on pose $U = PE_1$ et $V = Q^\top E_1$. Comme $E_1 \neq 0$ et P et Q sont inversibles on a $U \neq 0$ et $V \neq 0$. Par ailleurs les calculs ci-dessus expliquent que $UV^\top = M$.

Deuxième méthode : On note $\mathcal{C} = (C_j)_{1 \leq j \leq n}$ la famille des colonnes de la matrice M , comme $\text{rg}(M) = 1$ alors $\dim(\text{Vect}(\mathcal{C})) = 1$, donc $\mathcal{W} = \text{Vect}(\mathcal{C})$ est une droite vectorielle de $\mathcal{M}_{n,1}(\mathbb{K})$ donc il existe $U \in \mathcal{M}_{n,1}(\mathbb{K})$ tel que $\mathcal{W} = \text{Vect}(U)$, donc il existe des scalaires $v_1, \dots, v_n \in \mathbb{K}$ tel que, pour tout $j \in [1, n]$, on aie $C_j = v_j U$. Posons $V = (v_j)_{1 \leq j \leq n}$, alors $V \neq 0$ car sinon on aurait $M = 0$, de plus il est aisé de voir que $UV^\top = M$ en observant ses colonnes.

- Il en découle que $M^2 = UV^\top UV^\top = (V^\top U)UV^\top = \text{Tr}(M)M$, en effet la matrice M est exactement $M = (m_{i,j})_{1 \leq i,j \leq n}$ avec $m_{i,j} = u_i v_j$, pour tous $i, j \in [1, n]$, en particulier $\text{Tr}(M) = \sum_{k=1}^n u_k v_k = V^\top U$.

ii. D'après la question précédente, si on note $\tau = \text{Tr}(M)$, le polynôme $X^2 - \tau X$ est un polynôme annulateur de M donc $\pi_M | X^2 - \tau X$, donc $\pi_M \in \{X, X - \tau, X^2 - \tau X\}$, et comme $\text{rg}(M) = 1$ et $n > 1$, la matrice M ne peut être scalaire donc on élimine deux cas et on retient le seul possible : $\pi_M = X^2 - \text{tr}(M)X$

Pour plus de précision

On précise que si $n \in \mathbb{N}$ et $n \geq 2$ et $A = \lambda I_n$ est une matrice scalaire alors soit $\lambda = 0$ et $A = 0$, soit $\lambda \neq 0$ et A est inversible donc $\text{rg}(A) \neq 1$.

iii. On a $M^2 = \tau M$, et généralement pour tout $k \in \mathbb{N}^*$, alors, si on note $\text{tr}(M) = \tau$, on a $M^k = \tau^{k-1} M$ qui se démontre facilement par récurrence $S_N = I_n +$

$$\tau \left(\sum_{k=1}^N \frac{\tau^{k-1}}{k!} \right) M = I_n + \left(\sum_{k=1}^N \frac{\tau^k}{k!} \right) M.$$

Pour les 5/2

Comme le cas des projecteurs on verra que pour une matrice de rang 1, on a

$$e^M = I_n + (e^\tau - 1)M$$

2. Si R est un corps alors R est un anneau intègre, si R est fini de cardinal N et intègre soit $x \in R$ tel que $x \neq 0$, alors en examinant la suite $(x^k)_{k \in \mathbb{N}^*}$, il existe $p, q \in \mathbb{N}^*$ tel que $x^p = x^q$ et $p < q$, donc $x^p(1 - x^{q-p}) = 0$ où $m = q - p$ et par intégrité et que $x \neq 0$, on a $x^m = 1$, donc $xx^{m-1} = 1$ donc x est inversible et $x^{-1} = x^{m-1}$.
3. Si p est premier alors pour tous $k, \ell \in \mathbb{Z}$, on a $\bar{k} \bar{\ell} = \bar{0} \Rightarrow p | k\ell$ et comme p est premier $p | k\ell \Rightarrow p | k$ ou $p | \ell$, donc $\bar{k} \bar{\ell} = \bar{0} \Rightarrow \bar{k} = \bar{0}$ ou $\bar{\ell} = \bar{0}$. Donc $\mathbb{Z}/n\mathbb{Z}$ est intègre. Si n n'est pas premier il s'écrit $n = mm'$ avec $m, m' \in [1, n-1]$ donc $\bar{0} = \bar{m} \bar{m'}$ et $\bar{m} \neq \bar{0}$ et $\bar{m'} \neq \bar{0}$, donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre. On a prouvé donc que n est premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est intègre et comme $\mathbb{Z}/n\mathbb{Z}$ est fini on a $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps, ce qui termine la réponse à cette question.
4. (a) On propose $f : R_1 \times R_2 \times R_3 \rightarrow (R_1 \times R_2) \times R_3; (x_1, x_2, x_3) \mapsto ((x_1, x_2), x_3)$.
(b) Voici le rappel demandé :

Rappel de cours

Si m et n sont deux entiers naturels non nuls premiers entre eux alors les anneaux $\mathbb{Z}/mn\mathbb{Z}$ d'une part et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ d'autre part sont isomorphes.

- (c) Par le lemme des restes chinois rappelé ci-dessus on a $\mathbb{Z}/mns\mathbb{Z} \simeq \mathbb{Z}/mn\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$. Appliqué une deuxième fois on a $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ il en découle que $\mathbb{Z}/mns\mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \times \mathbb{Z}/s\mathbb{Z}$, or la première question donne $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \simeq (\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) \times \mathbb{Z}/s\mathbb{Z}$. Il en découle que $\mathbb{Z}/mns\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$.
5. Un calcul direct donne $M = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, donc

$$M^2 = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \times \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} a^2 + bc & ac + cd \\ ab + bd & bc + d^2 \end{pmatrix}.$$

Par ailleurs on a :

$$(a + d)M = \begin{pmatrix} a^2 + ad & ac + dc \\ ab + db & ad + d^2 \end{pmatrix},$$

il en découle que $M^2 - (a + d)M = - \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix}$, donc $M^2 = \tau M - \delta I_2$.

NOTE

On retrouve le théorème de Cayley-Hamilton qu'on vient de voir dans le cours du chapitre II, car le polynôme caractéristique de M est $\chi_M = X^2 - \text{Tr}(M)X + \det(M)$, donc par le théorème de Cayley-Hamilton $\chi_M(M) = M^2 - \tau M + \delta I_2 = 0$

Partie I

1. (a) Si R est intègre alors pour tout $a \in R$, on a $a \in \mathcal{J}(R) \Leftrightarrow a(a-1) = 0 \Leftrightarrow a = 0$ ou $a = 1$, donc $\mathcal{J}(R) = \{0, 1\}$.
- (b) p premier et $\alpha \in \mathbb{N}^*$, pour tout $k \in \mathbb{Z}$, si $\bar{k} \in \mathcal{J}(R)$ alors $\bar{k}^2 = \bar{k}$, donc $p^\alpha | k(k-1)$, par suite $p | k$ ou $p | (k-1)$, or $k \wedge (k-1) = 1$ donc $p | k$ et $p \nmid (k-1)$ ou $p | (k-1)$ et $p \nmid k$.
 - Si $p | k$ et $p \nmid (k-1)$, comme $p^\alpha | k(k-1)$, on a $p^\alpha | k$, donc $\bar{k} = \bar{0}$.
 - Si $p | (k-1)$ et $p \nmid k$ comme $p^\alpha | k(k-1)$, on a $p^\alpha | (k-1)$, donc $\bar{k} = \bar{1}$. Donc $\mathcal{J}(R) \subset \{\bar{0}, \bar{1}\}$ et comme $\bar{0}^2 = \bar{0}$ et $\bar{1}^2 = \bar{1}$, on a $\mathcal{J}(R) = \{\bar{0}, \bar{1}\}$.

Prestation élève

Un élève propose : Si $p^\alpha | k$ et $p^\alpha | (k-1)$ alors comme $p | p^\alpha$, on aurait $p | k$ et $p | (k-1)$, or $k \wedge (k-1) = 1$, c'est impossible.

- (c) Soit $a \in \mathcal{J}(R)$, alors :

$$(1-a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - a,$$

donc $1-a \in \mathcal{J}(R)$.

- Si R est fini, pour tout $a \in R$, si $a = 1-a$ alors

$$a = a^2 = a(1-a) = a - a^2 = 0,$$

donc $a = 0$ et $1-a = 1 = a = 0$, chose impossible car l'anneau R est supposé non trivial ($0 \neq 1$).

- Ainsi pour tout $x \in A$, on a $x \neq 1-x$, la relation

$$x \mathcal{R} y \Leftrightarrow y = x \quad \text{ou} \quad y = 1-x$$

est une relation d'équivalence dont les classes d'équivalence sont des paires donc $\text{card}(R)$ est pair.

- (d) Si R est supposé commutatif alors pour tout $(x, y) \in (\mathcal{J}(R))^2$ on a $x^2 = x$ et $y^2 = y$, donc $(xy)^2 = x^2 y^2 = xy$, donc $xy \in \mathcal{J}(R)$ et par suite $\mathcal{J}(R)$ est stable par la multiplication.

- Supposons que l'on a $\forall x \in R, x \in \mathcal{J}(R) \Rightarrow -x \in \mathcal{J}(R)$. Comme $1 \in \mathcal{J}(R)$, on a $-1 \in \mathcal{J}(R)$, donc $-1 = (-1)^2 = 1$, donc $2 = 0$.

- Réciproquement si $2 = 0$, alors $\forall x \in R, 2x = 0$ alors

$$\forall x \in R, x \in \mathcal{J}(R) \Rightarrow (-x)^2 = x = -x.$$

Conclusion : $[\forall x \in R, x \in \mathcal{I}(R) \Rightarrow -x \in \mathcal{I}(R)] \iff 2 = 0$.

Remarque

Autrement dit ce sont les anneaux de caractéristique 2. Si R est un anneau et si 1 est d'ordre fini dans le groupe additif $(R, +)$ l'ordre de a s'appelle la caractéristique de R . Si 1 n'est pas d'ordre fini on dit que l'anneau R est de caractéristique 0.

2. (a) Si $A \in \mathcal{I}(\mathcal{M}_2(\mathbb{K}))$ alors $A^2 = A$, donc $X^2 - X$ est un polynôme annulateur de A , or d'après la question 5) du préliminaire, on a $P = X^2 - (a + d)X + ad - bc$ est un polynôme annulateur de M , donc si $A \neq 0_2$ et $A \neq I_2$, le polynôme minimal de A est $\pi_A = X^2 - X$, donc divise P , et comme $\deg(P) = 2$, les racines de P sont 0 et 1, donc $P = X(X - 1) = X^2 - X$, donc $a + d = 1$ et $ad - bc = 0$.
- (b) On $a + d = 1$ et $ad = bc$, donc $d = 1 - a$ et $a(1 - a) = bc$.
- Si $a = 0$ alors $d = 1$ et $bc = 0$ donc $b = 0$ ou $c = 0$ donc $A = \begin{pmatrix} 0 & 0 \\ c & 1 \end{pmatrix}$ ou $A = \begin{pmatrix} 0 & b \\ 0 & 1 \end{pmatrix}$: $2p - 1$ possibilités
 - Si $a = 1$ alors $d = 0$ et $bc = 0$ donc $b = 0$ ou $c = 0$ donc $A = \begin{pmatrix} 1 & 0 \\ c & 0 \end{pmatrix}$ ou $A = \begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$: $2p - 1$ possibilités.
 - Si $a(a - 1) \neq 0$, ce qui est possible pour $p - 2$ valeurs de a , on a b arbitraire dans $\mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ et c s'en déduit $c = a(1 - a)b^{-1}$, donc $(p - 2)(p - 1)$ possibilité.
- Au total $2 + 2(2p - 1) + (p - 2)(p - 1) = p^2 + p + 2$, donc

$$\text{card}(\mathcal{I}(\mathcal{M}_2(\mathbb{Z}/p\mathbb{Z}))) = p^2 + p + 2.$$

3. (a) Puisque p et q sont premiers et distincts ils sont premiers entre eux, donc par le lemme des restes chinois les anneaux $\mathbb{Z}/pq\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ sont isomorphes, l'isomorphisme naturel étant :

$$f : \begin{cases} \mathbb{Z}/pq\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \\ \bar{x}^{[pq]} \longmapsto f(\bar{x}^{[pq]}) = (\bar{x}^{[p]}, \bar{x}^{[q]}) \end{cases},$$

où, pour tout $n \in \mathbb{N}^*$, on a noté $\bar{x}^{[n]}$, la classe d'équivalence de l'entier relatif x modulo n .

- (b) Un élément $X \in \mathbb{Z}/pq\mathbb{Z}$ est idempotent si et seulement si son image (X_1, X_2) par f est idempotent si et seulement si $(X_1, X_2)^2 = (X_1, X_2)$ si et seulement si $X_1^2 = X_1$ et $X_2^2 = X_2$, donc $\text{card}(\mathcal{I}(\mathbb{Z}/pq\mathbb{Z})) = \text{card}(\mathcal{I}(\mathbb{Z}/p\mathbb{Z})) \text{card}(\mathcal{I}(\mathbb{Z}/q\mathbb{Z})) = 2 \cdot 2 = 4$ (on a utilisé la question **1)1)b)**) et les idempotants sont exactement $(\bar{0}, \bar{0})$, $(\bar{0}, \bar{1})$, $(\bar{1}, \bar{0})$ et

$(\bar{1}, \bar{1})$. De même on a par le même argument :

$$\begin{aligned}\text{card}(\mathcal{I}(\mathcal{M}_2(\mathbb{Z}/pq\mathbb{Z})) &= \text{card}(\mathcal{I}(\mathcal{M}_2(\mathbb{Z}/p\mathbb{Z})) \text{card}(\mathcal{I}(\mathcal{M}_2(\mathbb{Z}/q\mathbb{Z})) \\ &= (p^2 + p + 2)(q^2 + q + 2)\end{aligned}$$

4. (a) – Montrons que la relation $\preceq$ est une relation d'équivalence sur $\mathcal{I}(R)$.
- La relation $\preceq$ est *reflexive* : Soit $x \in \mathcal{I}(R)$, comme $x^2 = x$, on a clairement $x \preceq x$.
 - La relation $\preceq$ est *symétrique* : Soit $x, y \in \mathcal{I}(R)$ tel que $x \preceq y$ et $y \preceq x$, donc $xy = yx = x$ et $yx = xy = y$, donc $x = y$.
 - La relation $\preceq$ est *transitive* : Soit $x, y, z \in \mathcal{I}(R)$ tel que $x \preceq y$ et $y \preceq z$, alors

$$\begin{cases} xy = yx = x \\ yz = zy = y \end{cases}, \text{ donc,}$$
 - D'une part, $xz = (xy)z = x(yz) = xy = x$,
 - et d'autre part, $zx = z(yx) = (zy)x = yx = x$,
 - il en découle que $xz = zx = x$ donc $x \preceq z$.
- Ainsi la relation $\preceq$ est une relation d'équivalence sur $\mathcal{I}(R)$.
- Montrons que 0 est un minimum et 1 est un maximum :
 - Tout d'abord $0 \in \mathcal{I}(R)$ et $1 \in \mathcal{I}(R)$.
 - Soit $x \in \mathcal{I}(R)$, alors $0.x = x.0 = 0$, donc $0 \preceq x$.
 - Soit $x \in \mathcal{I}(R)$, alors $x.1 = 1.x = x$, donc $x \preceq 1$.
 - Ainsi $\forall x \in \mathcal{I}(R)$, $0 \preceq x \preceq 1$, donc 0 est un minimum et 1 est un maximum de l'ensemble ordonné $(\mathcal{I}(R), \preceq)$.

(b) On va prouver deux implications :

- Si $1 \in \mathcal{S}(R)$, soit $x \in \mathcal{I}(R)$, comme 1 est un majorant on a $x \preceq 1$ et comme $1 \in \mathcal{S}(R)$, on a $x \neq 1 \Rightarrow x = 0$, ce qui veut dire que $x = 1$ ou $x = 0$. Inversement, on a bien $0, 1 \in \mathcal{I}(R)$, donc $\mathcal{I}(R) = \{0, 1\}$.
- Réciproquement si $\mathcal{I}(R) = \{0, 1\}$ alors $1 \in \mathcal{S}(R)$ car 0 est le seul élément de $\{0, 1\}$ qui minore 1 strictement.

(c) Soit $a \in \mathcal{I}(R)$ tel que $a \neq 0$.

- (i) $\Rightarrow$ (ii) : Supposons que $a \notin \mathcal{S}(R)$, alors il existe $b \in \mathcal{I}(R)$ tel que $b \preceq a$ et $b \neq 0$ et $b \neq a$. De $b^2 = b$ et $ba = ab = b$, si on pose $c = a - b$ alors $a = b + c$ et $c \in \mathcal{I}(R)$ car $c^2 = a^2 + b^2 - 2ab = a + b - b = a - b = c$ et b et c sont orthogonaux car $bc = b(a - b) = ba - b^2 = ba - b = 0$ et $cb = (a - b)b = ab - b = 0$, et $a = b + c$.
- (ii) $\Rightarrow$ (i) : Supposons qu'il existe $b, c \in \mathcal{I}(R)$ non nuls tel que $a = b + c$ et $bc = cb = 0$ alors $b \neq a$ et $ba = b^2 + bc = b$ et $ab = b^2 + cb = b$ et $b \neq 0$, donc $a \in \mathcal{S}(R)$.

(d) **Note** : Dans cette question on va adopter trois nouveaux symboles :

- $x \perp y$ pour x et y sont orthogonaux,
- $x \prec y$ et $y \succ x$ pour $x \preceq y$ et $x \neq y$.
- Soit $a \in \mathcal{I}(R)$, $a \neq 0$, $a \notin \mathcal{S}(R)$.

Principe. On construit une décomposition de a en somme d'idempotents deux à deux

orthogonaux. Tant qu'au moins un terme de la somme n'est pas dans $\mathcal{S}(R)$, on le remplace par une somme de deux idempotents non nuls orthogonaux. La condition (★) garantit que ce processus s'arrête.

Initialisation. Comme $a \notin \mathcal{S}(R)$, a n'est pas minimal non nul : il existe $a_1 \in \mathcal{J}(R)$ non nul tel que

$$a_1 \preceq a, \quad a_1 \neq a.$$

Posons $a_2 = a - a_1$. Comme en I.4.c, on montre que $a_2 \in \mathcal{J}(R)$ et que $a_1 \perp a_2$. On a donc

$$a = a_1 + a_2, \quad a_1 \perp a_2.$$

Hérédité. Supposons construit

$$a = a_1 + \cdots + a_n + b,$$

avec $a_1, \dots, a_n, b \in \mathcal{J}(R)$ deux à deux orthogonaux, et $b \notin \mathcal{S}(R)$. Comme $b \notin \mathcal{S}(R)$, il existe $a_{n+1} \in \mathcal{J}(R)$ non nul tel que

$$a_{n+1} \preceq b, \quad a_{n+1} \neq b.$$

Posons $a_{n+2} = b - a_{n+1}$. Comme précédemment, $a_{n+1}, a_{n+2} \in \mathcal{J}(R)$ et $a_{n+1} \perp a_{n+2}$. On a donc

$$b = a_{n+1} + a_{n+2}, \quad a_{n+1} \perp a_{n+2}.$$

En particulier $\begin{cases} a_{n+1}b = ba_{n+1} = a_{n+1} \\ a_{n+2}b = ba_{n+2} = a_{n+2} \end{cases}$, donc $(\star) : \forall j \in \{n+1, n+2\}, \quad a_j b = b a_j = a_j$. Montrons que pour tout $j \in \{n+1, n+2\}$ et pour tout $k \in \{1, \dots, n\}$ on a $a_j \perp a_k$. On a $b a_k = 0$ car b et a_k sont orthogonaux (par hypothèse de récurrence). Donc, compte tenu de $(\star)$ ci-dessus :

$$a_j a_k = (a_j b) a_k = a_j (b a_k) = a_j \cdot 0 = 0,$$

et de même :

$$a_k a_j = a_k (b a_j) = (a_k b) a_j = 0 \cdot a_j = 0.$$

Donc $a_j \perp a_k$ pour tout $(j, k) \in \{n+1, n+2\} \times \{1, \dots, n\}$, ce qui permet de dire que

$$a = a_1 + \cdots + a_n + a_{n+1} + a_{n+2},$$

où les termes $a_1, \dots, a_{n+2}$ sont deux à deux orthogonaux.

Terminaison. Tant qu'au moins un terme de la somme n'est pas dans $\mathcal{S}(R)$, le processus se poursuit et le nombre de termes de la somme augmente nécessairement (on remplace un terme $b \notin \mathcal{S}(R)$ par deux termes non nuls a_{n+1}, a_{n+2} , et la somme des termes reste égale à a). Or, la condition (★) interdit l'existence d'une suite infinie strictement décroissante dans $\mathcal{J}(R)$ pour $\preceq$. Ici, chaque nouveau terme a_{n+1} est un minorant strict du reste b , donc la suite des restes

$$a \succ a_1 \succ a_2 \succ \cdots$$

est strictement décroissante. Elle ne peut donc pas être infinie.

Il existe donc une étape où tous les termes de la somme sont dans $\mathcal{S}(R)$. On obtient alors :

$$a = a_1 + \cdots + a_N,$$

avec $a_1, \dots, a_N \in \mathcal{S}(R)$ deux à deux orthogonaux.

Conclusion. Si R vérifie la condition (★), tout élément non nul de $\mathcal{J}(R)$ qui n'est pas dans $\mathcal{S}(R)$ s'écrit comme somme finie d'éléments de $\mathcal{S}(R)$ deux à deux orthogonaux.

5. (a) Soient a et b deux éléments distincts de $\mathcal{S}(R)$ alors $a, b \in \mathcal{J}(R)$ et 0 est le seul minorant strict de a et de b pour $\preceq$, or par (C) supposée ci-dessus, on a $ab = ba$. On a $(ab)a = a^2b = ab$ et $a(ab) = a^2b = ab$, donc $(ab)a = a(ab) = ab$ donc $ab \preceq a$ et comme $a \in \mathcal{S}(R)$ on a $ab = a$ ou $ab = 0$, or si $ab = a$ alors $ab = ba = a$ donc $a \preceq b$ et comme $b \in \mathcal{S}(R)$ on aurait $a = 0$ ou $a = b$, ce qui est faux car on a supposé $a \neq b$ et comme $a \in \mathcal{S}(R)$ on a 0 est le seul minorant strict de a , en particulier $a \neq 0$, il reste alors $ab = ba = 0$, donc a et b sont orthogonaux. Ainsi avec les hypothèses faites on a *deux éléments distincts de $\mathcal{S}(R)$ sont nécessairement orthogonaux*.
- Dédution : Si $a, b \in \mathcal{S}(R)$ et $a \neq b$ alors $(a + b)^2 = a^2 + 2ab + b^2 = a + b$ car $ab = 0$, donc $a + b \in \mathcal{J}(R)$.

- (b) Pour tout $k \in [1, n]$, on a :

$$b_k(b_1 + \cdots + b_n) = b_k^2 = b_k \quad \text{et} \quad (b_1 + \cdots + b_n)b_k = b_k,$$

donc : $b_k \preceq b_1 + \cdots + b_n$.

Inversement soit $x \in \mathcal{J}(R)$ tel que $x \preceq b_1 + \cdots + b_n$, alors $x(b_1 + \cdots + b_n) = x$, il en découle que $x = \sum_{i=1}^n xb_i$, or pour tout $i \in [1, n]$, on a $(xb_i)^2 = x^2b_i^2$ et on sait que b_i est

idempotent et x aussi comme somme d'éléments distincts de $\mathcal{S}(R)$, donc $(xb_i)^2 = xb_i$, donc $xb_i \in \mathcal{J}(R)$ et $xb_ib_i = b_ixb_i = xb_i$ donc $xb_i \preceq b_i$ et comme $b_i \in \mathcal{S}(R)$, on a $xb_i = 0$ ou $xb_i = b_i$, il en découle qu'il existe une partie J de $[1, n]$ tel que $x = \sum_{k \in J} b_k$,

or si $\text{card}(J) \geq 2$ alors si $j \in J$ on a $x \neq b_j$ et $b_j \neq 0$ et $b_j \preceq x$ car $b_jx = xb_j = b_j$, donc si $\text{card}(J) \geq 2$ on a $x \notin \mathcal{S}(R)$, il en découle que les seuls éléments de $\mathcal{S}(R)$ qui minorent $b_1 + \cdots + b_n$ sont ceux pour lesquels J est un singleton donc les éléments de $\{b_1, \dots, b_n\}$.

- (c) • (i) Unicité de la décomposition : Si $x \in \mathcal{J}(R)$ s'écrit

$$x = b_1 + \cdots + b_m = c_1 + \cdots + c_n,$$

avec les b_k deux à deux orthogonaux et les c_k deux à deux orthogonaux alors les ensembles $\{b_1, \dots, b_m\}$ et $\{c_1, \dots, c_n\}$ sont égaux car ils sont en même temps les seuls éléments de $\mathcal{S}(R)$ qui minorent x .

• (ii) Montrons que $\mathcal{S}(R)$ est fini : Par l'absurde, si $\mathcal{S}(R)$ est infini alors on considère une suite infinie (s_n) d'éléments de $\mathcal{S}(R)$ et on considère les somme $t_n = s_1 + \cdots + s_n$

pour tout $n \in \mathbb{N}^*$ alors en adoptant la notation $x \prec y \Leftrightarrow x \preceq y$ et $x \neq y$, on a $t_n \in \mathcal{J}(R)$ et

$$t_1 \prec t_2 \prec \cdots \prec t_n \prec t_{n+1} \prec \dots,$$

ce qui contredit la condition (★) supposée ci-dessus.

• (iii) $\mathcal{J}(R)$ est fini : On a vu que tout élément de $\mathcal{J}(R)$ s'écrit comme somme fini d'éléments de $\mathcal{S}(R)$ et ce dernier est fini donc $\mathcal{J}(R)$ est fini aussi.

• (iv) Isomorphisme avec l'ensemble des parties de $\mathcal{S}(R)$ D'après (i), tout élément $a \in \mathcal{J}(R)$ s'écrit de manière unique comme somme d'un sous-ensemble $B \subseteq \mathcal{S}(R)$ (éventuellement vide pour $a = 0$) :

$$a = \sum_{b \in B} b.$$

On peut donc définir une application :

$$\Phi : \mathcal{J}(R) \rightarrow \mathcal{P}(\mathcal{S}(R)), \quad a \mapsto B,$$

où B est l'ensemble des $b \in \mathcal{S}(R)$ qui minorent a (ou, de façon équivalente, les éléments de $\mathcal{S}(R)$ apparaissant dans la décomposition unique de a).

Montrons que Φ est un isomorphisme d'ensembles munis de la multiplication entre $(\mathcal{J}(R), \cdot)$ et $(\mathcal{P}(\mathcal{S}(R)), \cap)$.

Φ est bijective : claire par unicité de la décomposition.

Soient $a, b \in \mathcal{J}(R)$, avec $a = \sum_{x \in A} x$ et $b = \sum_{y \in B} y$, où $A, B \subseteq \mathcal{S}(R)$. Comme les idempotents commutent deux à deux (hypothèse de la question 1.5), on a :

$$ab = \left(\sum_{x \in A} x \right) \left(\sum_{y \in B} y \right) = \sum_{x \in A, y \in B} xy.$$

Or, deux éléments distincts de $\mathcal{S}(R)$ sont orthogonaux (1.5.a), donc $xy = 0$ si $x \neq y$. Si $x = y$, alors $xy = x^2 = x$. Ainsi :

$$ab = \sum_{z \in A \cap B} z.$$

Donc $\Phi(ab) = A \cap B = \Phi(a) \cap \Phi(b)$. Ainsi Φ est un isomorphisme entre $(\mathcal{J}(R), \cdot)$ et $(\mathcal{P}(\mathcal{S}(R)), \cap)$.

• (v) Isomorphisme avec $(\mathbb{Z}/2\mathbb{Z}, \cdot)^n$

Soit $n = \text{Card}(\mathcal{S}(R))$. L'ensemble des parties de $\mathcal{S}$ muni de l'intersection est isomorphe à $\{0, 1\}^n$ muni de la multiplication composante par composante, où $\{0, 1\}$ est muni de la multiplication usuelle (qui est celle de $\mathbb{Z}/2\mathbb{Z}$). En effet, à chaque sous-ensemble $A \subseteq \mathcal{S}(R)$, on associe son vecteur caractéristique $(\varepsilon_1, \dots, \varepsilon_n) \in \{0, 1\}^n$, où $\varepsilon_i = 1$ si le i -ème élément de $\mathcal{S}(R)$ est dans A , et 0 sinon. L'intersection correspond alors au produit composante par composante. Ainsi, via Φ , on a un isomorphisme d'ensembles munis de la multiplication : $(\mathcal{J}(R), \cdot) \cong (\mathbb{Z}/2\mathbb{Z}, \cdot)^n$, où $n = \text{Card}(\mathcal{S})$.

Remarque

Ce résultat est fondamental : il montre que, dans un tel anneau, la structure des idempotents est essentiellement **booléenne**, ce qui est typique des anneaux commutatifs finis ou des produits d'anneaux locaux.

- (d) Supposons R commutatif fini. On sait que R vérifie alors la condition (★) : en effet, $\mathcal{I}(R)$ est fini (car R est fini), donc il ne peut exister de suite infinie strictement décroissante dans $\mathcal{I}(R)$. De plus, R étant commutatif, tous ses éléments commutent, donc en particulier les idempotents commutent deux à deux. Les hypothèses de I.5.c sont donc satisfaites.

D'après I.5.c.(v), on a un isomorphisme d'ensembles munis de la multiplication :

$$(\mathcal{I}(R), \cdot) \cong (\mathbb{Z}/2\mathbb{Z}, \cdot)^n,$$

où $n = \text{Card}(\mathcal{S}(R))$. Par suite,

$$\text{Card}(\mathcal{I}(R)) = 2^n.$$

Ainsi, le cardinal de $\mathcal{I}(R)$ est une puissance de 2.

De plus, d'après I.5.c.(ii), $\mathcal{S}(R)$ est fini, et $n = \text{Card}(\mathcal{S}(R))$ est le nombre d'idempotents minimaux non nuls. On a donc :

$$\text{Card}(\mathcal{I}(R)) = 2^{\text{Card}(\mathcal{S}(R))}.$$

Ce résultat s'étend-il au cas non commutatif ? En général non, vu le contre exemple suivant : Prenons $R = \mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$. C'est un anneau fini de cardinal 16, non commutatif.

Idempotents de $\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})$.

On cherche les matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $a, b, c, d \in \mathbb{Z}/2\mathbb{Z}$ telles que $M^2 = M$.

D'après I.2.a, M est un idempotent si et seulement si $M = 0_2$, ou $M = I_2$, ou

$$a + d = 1, \quad ad = bc.$$

Dans $\mathbb{Z}/2\mathbb{Z}$, le nombre des idempotents est d'après la question I)2)a) $2^2 + 2 + 2 = 8$, qui sont :

— $M = 0_2 : \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$

— $M = I_2 : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$

— $a + d = 1$ et $ad = bc$. Comme $a, d \in \{0, 1\}$ et $a + d = 1$, on a $(a, d) = (1, 0)$ ou $(0, 1)$.

— Si $(a, d) = (1, 0) : ad = 0$, donc $bc = 0$. Les matrices sont

$$\begin{pmatrix} 1 & b \\ c & 0 \end{pmatrix} \quad \text{avec } bc = 0.$$

Les couples $(b, c) \in \{0, 1\}^2$ avec $bc = 0$ sont $(0, 0), (0, 1), (1, 0)$. Cela donne 3 matrices.

— Si $(a, d) = (0, 1) : ad = 0$, donc $bc = 0$. Les matrices sont

$$\begin{pmatrix} 0 & b \\ c & 1 \end{pmatrix} \quad \text{avec } bc = 0.$$

Cela donne aussi 3 matrices.

Au total :

$$\mathcal{J}(\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z})) = \left\{ 0_2, I_2, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Donc

$$\text{Card}(\mathcal{J}(\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z}))) = 8 = 2^3.$$

Idempotents minimaux non nuls $\mathcal{S}(R)$.

On cherche les idempotents non nuls M tels que 0 soit le seul minorant strict de M pour $\preceq$, c'est-à-dire tels que M ne puisse pas s'écrire comme somme de deux idempotents non nuls orthogonaux.

Les idempotents minimaux non nuls sont les matrices de rang 1 :

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

Vérifions par exemple que $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est minimal non nul. Si $E_{11} = A + B$ avec A, B idempotents non nuls orthogonaux, alors A et B sont des matrices de rang 1 dont les images sont dans celle de E_{11} , qui est de dimension 1. Donc l'un des deux est nul, contradiction. Donc $E_{11} \in \mathcal{S}(R)$.

De même, toutes les matrices de rang 1 sont dans $\mathcal{S}(R)$. Donc

$$\text{Card}(\mathcal{S}(\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z}))) = 6.$$

Conclusion.

On a

$$\text{Card}(\mathcal{J}(\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z}))) = 8 = 2^3,$$

mais

$$\text{Card}(\mathcal{S}(\mathcal{M}_2(\mathbb{Z}/2\mathbb{Z}))) = 6,$$

et $8 \neq 2^6$. Donc le résultat de II.5.c.(v) ne s'étend pas au cas non commutatif : la structure de $\mathcal{J}(R)$ n'est plus nécessairement isomorphe à $(\mathbb{Z}/2\mathbb{Z}, \cdot)^n$.

- (e) **Application** : déterminer les entiers ≤ 60 dont les images dans $\mathbb{Z}/60\mathbb{Z}$ constituent les éléments de $\mathcal{I}(\mathbb{Z}/60\mathbb{Z})$ et ceux de $\mathcal{S}(\mathbb{Z}/60\mathbb{Z})$.

On rappelle que $\mathbb{Z}/60\mathbb{Z}$ est un anneau commutatif fini. On a la décomposition en facteurs premiers :

$$60 = 2^2 \cdot 3 \cdot 5.$$

Par le théorème chinois, on a un isomorphisme d'anneaux :

$$\mathbb{Z}/60\mathbb{Z} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Les idempotents de $\mathbb{Z}/60\mathbb{Z}$ correspondent donc aux triplets d'idempotents de chacun des facteurs.

Or, pour un corps fini $\mathbb{F}_p$ (ici $p = 3$ et $p = 5$), les seuls idempotents sont 0 et 1. Pour $\mathbb{Z}/4\mathbb{Z}$, les idempotents sont également 0 et 1 (car $4 = 2^2$, et on a montré en l.1.b que $\mathcal{I}(\mathbb{Z}/p^a\mathbb{Z}) = \{0, 1\}$).

Ainsi, les idempotents de $\mathbb{Z}/60\mathbb{Z}$ correspondent aux $2^3 = 8$ triplets :

$$(\varepsilon_1, \varepsilon_2, \varepsilon_3) \in \{0, 1\}^3.$$

Chaque triplet correspond à un unique entier $x \in \{0, 1, \dots, 59\}$ vérifiant les congruences :

$$\begin{cases} x \equiv \varepsilon_1 \pmod{4}, \\ x \equiv \varepsilon_2 \pmod{3}, \\ x \equiv \varepsilon_3 \pmod{5}. \end{cases}$$

Calculons ces 8 entiers.

- $(0, 0, 0)$: $x = 0$.
- $(1, 0, 0)$: $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{5}$. Donc x multiple de 15, et $x \equiv 1 \pmod{4}$. Les multiples de 15 modulo 60 sont 0, 15, 30, 45. On a $15 \equiv 3 \pmod{4}$, $30 \equiv 2 \pmod{4}$, $45 \equiv 1 \pmod{4}$. Donc $x = 45$.
- $(0, 1, 0)$: $x \equiv 0 \pmod{4}$, $x \equiv 1 \pmod{3}$, $x \equiv 0 \pmod{5}$. Donc x multiple de 20, et $x \equiv 1 \pmod{3}$. Les multiples de 20 modulo 60 sont 0, 20, 40. On a $20 \equiv 2 \pmod{3}$, $40 \equiv 1 \pmod{3}$. Donc $x = 40$.
- $(0, 0, 1)$: $x \equiv 0 \pmod{4}$, $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{5}$. Donc x multiple de 12, et $x \equiv 1 \pmod{5}$. Les multiples de 12 modulo 60 sont 0, 12, 24, 36, 48. On a $12 \equiv 2 \pmod{5}$, $24 \equiv 4 \pmod{5}$, $36 \equiv 1 \pmod{5}$. Donc $x = 36$.
- $(1, 1, 0)$: $x \equiv 1 \pmod{4}$, $x \equiv 1 \pmod{3}$, $x \equiv 0 \pmod{5}$. Donc $x \equiv 1 \pmod{12}$, et $x \equiv 0 \pmod{5}$. Les solutions de $x \equiv 1 \pmod{12}$ modulo 60 sont 1, 13, 25, 37, 49. On a $25 \equiv 0 \pmod{5}$. Donc $x = 25$.
- $(1, 0, 1)$: $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{5}$. Donc $x \equiv 1 \pmod{20}$ (car $x \equiv 1 \pmod{4}$ et $x \equiv 1 \pmod{5}$), et $x \equiv 0 \pmod{3}$. Les solutions de $x \equiv 1 \pmod{20}$ modulo 60 sont 1, 21, 41. On a $21 \equiv 0 \pmod{3}$. Donc $x = 21$.
- $(0, 1, 1)$: $x \equiv 0 \pmod{4}$, $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$. Donc $x \equiv 1 \pmod{15}$ (car

$x \equiv 1 \pmod{3}$ et $x \equiv 1 \pmod{5}$), et $x \equiv 0 \pmod{4}$. Les solutions de $x \equiv 1 \pmod{15}$ modulo 60 sont 1, 16, 31, 46. On a $16 \equiv 0 \pmod{4}$. Donc $x = 16$.

• $(1, 1, 1) : x = 1$.

Ainsi, les idempotents de $\mathbb{Z}/60\mathbb{Z}$ sont :

$$\mathcal{I}(\mathbb{Z}/60\mathbb{Z}) = \{0, 1, 16, 21, 25, 36, 40, 45\}.$$

Éléments de $\mathcal{S}(\mathbb{Z}/60\mathbb{Z})$

Rappelons que $\mathcal{S}(R)$ est l'ensemble des idempotents minimaux non nuls, c'est-à-dire les idempotents $x \neq 0$ tels que 0 soit le seul minorant strict de x pour $\preceq$.

Dans $\mathbb{Z}/60\mathbb{Z}$, les idempotents minimaux non nuls correspondent aux triplets de $\{0, 1\}^3$ ayant exactement une composante égale à 1 et les autres nulles. En effet, un idempotent x est minimal non nul si et seulement s'il ne peut pas s'écrire comme somme de deux idempotents non nuls orthogonaux. Dans la décomposition en produit, cela correspond aux vecteurs de base.

Les triplets correspondants sont :

$$(1, 0, 0), \quad (0, 1, 0), \quad (0, 0, 1).$$

D'après les calculs précédents, ces triplets correspondent respectivement à :

$$45, \quad 40, \quad 36.$$

Ainsi,

$$\mathcal{S}(\mathbb{Z}/60\mathbb{Z}) = \{36, 40, 45\}.$$

On vérifie que ces trois idempotents sont deux à deux orthogonaux :

$$36 \cdot 40 \equiv 0 \pmod{60}, \quad 36 \cdot 45 \equiv 0 \pmod{60}, \quad 40 \cdot 45 \equiv 0 \pmod{60}.$$

Et leur somme vaut :

$$36 + 40 + 45 = 121 \equiv 1 \pmod{60}.$$

On a bien $\text{Card}(\mathcal{I}(\mathbb{Z}/60\mathbb{Z})) = 8 = 2^3$, et $n = \text{Card}(\mathcal{S}(\mathbb{Z}/60\mathbb{Z})) = 3$.

Conclusion pour I.5.e)

Les entiers ≤ 60 dont les images dans $\mathbb{Z}/60\mathbb{Z}$ constituent les éléments de $\mathcal{I}(\mathbb{Z}/60\mathbb{Z})$ sont :

$$\{0, 1, 16, 21, 25, 36, 40, 45\}.$$

Ceux de $\mathcal{S}(\mathbb{Z}/60\mathbb{Z})$ sont :

$$\{36, 40, 45\}.$$

Partie II

1. (a) Soit $a \in \mathcal{P}(R)$ tel que $a^{\mu(a)+r} = a^{\mu(a)+r'}$, alors sans nuire à la généralité, on peut supposer que $r \leq r'$, on a : $a^{\mu(a)+r} a^{\pi(a)-r} = a^{\mu(a)+r'} a^{\pi(a)-r}$, donc

$$a^{\mu(a)+\pi(a)} = a^{\mu(a)+\pi(a)} a^{r'-r}$$

et finalement $a^{\mu(a)} = a^{\mu(a)+r'-r}$ avec $0 \leq r' - r < \pi$, donc $r' - r = 0$, donc $r = r'$.

- (b) Soit $a \in \mathcal{P}(R)$ et m, n des entiers avec n non nul. On veut montrer l'équivalence :

$$(i) \quad a^{m+n} = a^m \quad \Longleftrightarrow \quad (ii) \quad \mu(a) \leq m \text{ et } \pi(a) \mid n.$$

- $\boxed{(ii) \Rightarrow (i)}$. Supposons $\mu(a) \leq m$ et $\pi(a) \mid n$. Alors il existe $k \in \mathbb{N}$ tel que $n = k\pi(a)$. On a : $a^{m+n} = a^{\mu(a)+n+m-\mu(a)} = a^{\mu(a)+k\pi(a)+m-\mu(a)} = a^{\mu(a)+k\pi(a)} a^{m-\mu(a)}$, or une simple récurrence permet de prouver que l'on a la propriété $(\star\star)$ suivante :

$$(\star\star) \quad \forall k \in \mathbb{N}, \quad a^{\mu(a)+k\pi(a)} = a^{\mu(a)}$$

Il en découle que $a^{m+n} = a^{\mu(a)} a^{m-\mu(a)} = a^m$. Donc finalement $a^{m+n} = a^m$.

- $\boxed{(i) \Rightarrow (ii)}$ Supposons $a^{m+n} = a^m$. On veut montrer $\mu(a) \leq m$ et $\pi(a) \mid n$. Par définition de $\mu(a)$ on a tout de suite $\mu(a) \leq m$. La relation $a^{m+n} = a^m$ s'écrit aussi $a^{\mu(a)+n+m-\mu(a)} = a^{\mu(a)+m-\mu(a)}$. On effectue les divisions euclidiennes respectives de $n + m - \mu(a)$ et $m - \mu(a)$ par $\pi(a)$, il vient :

$$\begin{cases} n + m - \mu(a) = q\pi(a) + r \\ m - \mu(a) = q'\pi(a) + r' \end{cases}, \quad 0 \leq r, r' < \pi(a),$$

donc compte tenu de $(\star\star)$ ci-dessus on a $a^{\mu(a)+s\pi(a)} = a^{\mu(a)}$ pour tout entier s facile à prouver par récurrence, on a

$$a^{\mu(a)+r} = a^{\mu(a)+r'},$$

ce qui donne par la question précédente que $r = r'$, donc en revenant aux divisions euclidiennes ci-dessus on obtient $n = (q - q')\pi(a)$, donc on a bien $\pi(a) \mid n$.

Ainsi, l'équivalence est démontrée.

- (c) On va démontrer deux implications :

- Si $a \in \mathcal{P}(R)$ alors il existe $(m, n) \in \mathbb{N} \times \mathbb{N}^*$ tel que $a^m = a^{m+n}$. Donc $(a^m)^k = (a^{m+n})^k$, donc $(a^k)^m = (a^k)^{m+n}$, donc $a^k \in \mathcal{P}(R)$.
- Réciproquement si $a^k \in \mathcal{P}(R)$, il existe $(m, n) \in \mathbb{N} \times \mathbb{N}^*$ tel que $(a^k)^m = (a^k)^{m+n}$, donc $a^{km} = a^{km+kn}$, avec $(km, kn) \in \mathbb{N} \times \mathbb{N}^*$, donc $a^k \in \mathcal{P}(R)$.
- On a $(a^k)^{\mu(a)+\pi(a)} = (a^{\mu(a)+\pi(a)})^k = (a^{\mu(a)})^k = (a^k)^{\mu(a)}$, donc d'après la question II)1)b), on a $\mu(a^k) \leq \mu(a)$ et $\pi(a^k) \mid \pi(a)$.
- On a $a^{k\mu(a^k)+k\pi(a^k)} = (a^k)^{\mu(a^k)+\pi(a^k)} = (a^k)^{\mu(a^k)} = a^{k\mu(a^k)}$, donc toujours d'après II)1)b), on a $\mu(a) \leq k\mu(a^k)$ et $\pi(a) \mid k\pi(a^k)$.
- On résume : $\boxed{\mu(a^k) \leq \mu(a) \leq k\mu(a^k)}$ et $\boxed{\pi(a^k) \mid \pi(a) \mid k\pi(a^k)}$. Ainsi, toutes les relations sont démontrées.

(d) Soit $a \in \mathcal{P}(R)$, alors $\exists(m, n) \in \mathbb{N} \times \mathbb{N}^*$, $a^m = a^{m+n}$ et le couple $(\mu(a), \pi(a))$ existe en particulier. Prenons $k = \text{ppcm}(\mu(a), \pi(a))$, alors $\begin{cases} \mu(a) \leq k \\ \pi(a) | k \end{cases}$.

D'après la question II)1)c), on a $a^{k+k} = a^k$, donc $(a^k)^2 = a^k$, donc $a^k \in \mathcal{J}(R)$.

Soit maintenant $k \in \mathbb{N}^*$ tel que $a^k \in \mathcal{J}(R)$, alors $a^{k+k} = a^k$ et toujours d'après la question II)1)c), on a $\begin{cases} \mu(a) \leq k \\ \pi(a) | k \end{cases}$. Soit $k_0 = \min\{k \in \mathbb{N}^* / a^k \in \mathcal{J}(R)\}$.

On a montré ci-dessus que $\max(\mu(a), \pi(a)) \leq k_0$. Pour prouver l'autre inégalité, la division euclidienne de $\mu(a)$ par $\pi(a)$ s'écrit $\mu(a) = q\pi(a) + r$ avec $0 \leq r < \pi(a)$.

Soit alors $k = (q+1)\pi(a)$ alors $a^k \in \mathcal{J}(R)$, car on a $\begin{cases} \mu(a) \leq k \\ \pi(a) | k \end{cases}$ car

$$k - \mu(a) = (q+1)\pi(a) - q\pi(a) - r = \pi(a) - r > 0,$$

et il est clair que $\pi(a) | k$, donc, d'après la question II)1)c), on a $a^{k+k} = a^k$, donc $(a^k)^2 = a^k$. Par ailleurs on a $k \leq \mu(a) + \pi(a)$ car

$$\mu(a) + \pi(a) - k = q\pi(a) + r + \pi(a) - k = (q+1)\pi(a) - k + r = r \geq 0.$$

Il en résulte que $k_0 \leq \mu(a) + \pi(a)$.

(e) Soit $a \in \mathcal{P}(R)$. Si a est inversible alors $a \in \mathcal{U}(R)$ et dans ce groupe a est d'ordre fini, car comme $a \in \mathcal{P}(R)$, il existe $(m, n) \in \mathbb{N} \times \mathbb{N}^*$ tel que $a^m = a^{m+n}$, comme a est inversible $a^n = 1$, donc a est d'ordre fini et comme $a^n = e$, on a $a^0 = a^{0+n}$ donc $\mu(a) = 0$ et par définition de $\pi(a)$, on a

$$\pi(a) = \min\{n \in \mathbb{N}^* / a^n = 1\} = \text{ordre}(a)$$

en particulier $aa^{\pi(a)-1} = a^{\pi(a)-1}a = 1$, donc $a^{-1} = a^{\pi(a)-1}$.

(f) Si R est fini et $\text{card}(R) = N$, alors pour tout $a \in R$, la liste $a^0 = 1, a^2, \dots, a^N$ est une liste de $N+1$ éléments de R , donc par le principe des tiroirs de Dirichlet, il existe $m, q \in \{0, \dots, N\}$ tel que $m < q$ et $a^m = a^q$, donc en posant $n = q - m$, on a $a^m = a^{m+n}$ avec $(m, n) \in \mathbb{N} \times \mathbb{N}^*$, donc $a \in \mathcal{P}(R)$ et finalement $\mathcal{P}(R) = R$.

- On voit que $\mu(a) + \pi(a) \leq q$ et comme $q \leq N$, on a donc $\mu(a) + \pi(a) \leq \text{card}(R)$.

2. (a) Si b et c sont orthogonaux on a en particulier $bc = cb$, donc la formule du binôme de Newton donne :

$$(b+c)^n = \sum_{k=0}^n \binom{n}{k} b^k c^{n-k} = b^n + c^n,$$

car pour tout $k \in [1, n]$, $b^k c^{n-k} = bcb^{k-1}c^{n-k-1} = 0$.

- **Déduction** : si $b, c \in \mathcal{P}(R)$ et b et c sont orthogonaux alors $b+c \in \mathcal{P}(R)$ car si on note $q = \max(\mu(b), \mu(c))$ et $p = \text{ppcm}(\pi(b), \pi(c))$, alors d'après ce qui précède, on

a

$$\begin{aligned}
(b+c)^{q+p} &= b^{q+p} + c^{q+p} \\
&= b^{\mu(b)+p} b^{q-\mu(b)} + c^{\mu(c)+p} c^{q-\mu(c)} \\
&= b^{\mu(b)} b^{q-\mu(b)} + c^{\mu(c)} c^{q-\mu(c)} \\
&= b^q + c^q = (b+c)^q
\end{aligned}$$

Il en découle que $b+c \in \mathcal{P}(R)$ et en même temps que $\begin{cases} \mu(b+c) \leq \max(\mu(b), \mu(c)) \\ \pi(b+c) | \text{ppcm}(\pi(b), \pi(c)) \end{cases}$.

- (b) Soit $b \in \mathcal{P}(R)$ tel que $\mu(b) \leq 1$. Soit k un entier non nul : On va montrer que b et $1 - b^{\pi(b)}$ sont orthogonaux, pour cela effectuons $b(1 - b^{\pi(b)}) = b - b^{1+\pi(b)}$. Si $\mu(b) = 1$, alors $b^{1+\pi(b)} = b$, par suite $b(1 - b^{\pi(b)}) = b - b = 0$ et si $\mu(b) = 0$ alors $b^{0+\pi(b)} = b^0 = 1$, donc $b^{\pi(b)} = 1$ par suite dans ce cas aussi, en vertu de $(\star)$ on a $b(1 - b^{\pi(b)}) = 0$, il est clair qu'on a aussi $(1 - b^{\pi(b)})b = 0$, donc b et $1 - b^{\pi(b)}$ sont orthogonaux. Il en découle d'après la question a) ci-dessus que pour tout $k \in \mathbb{N}^*$, on a

$$(\star) \quad (b + 1 - b^{\pi(b)})^k = b^k + (1 - b^{\pi(b)})^k$$

et que b et $1 - b^{\pi(b)}$ sont des éléments de $\mathcal{P}(R)$.

- On va maintenant prouver l'autre relation, pour tout $k \in \mathbb{N}^*$,

$$(\star)' \quad b^k + (1 - b^{\pi(b)})^k = b^k + 1 - b^{\pi(b)}$$

- Notons que si $\mu(b) = 0$ alors $1 = b^{\pi(b)}$ et dans ce cas la relation $(\star)'$ est vraie.

- Si $\mu(b) = 1$, chose qu'on va supposer désormais, la relation $(\star)'$ est équivalente à la relation

$$(\star)'' \quad (1 - b^{\pi(b)})^k = 1 - b^{\pi(b)},$$

pour cela commençons par montrer que $1 - b^{\pi(b)}$ et $b^{\pi(b)}$ sont orthogonaux : Comme $\mu(b) = 1$, on a $b = b^{1+\pi(b)}$, donc

$$(1 - b^{\pi(b)})b^{\pi(b)} = b^{\pi(b)} - b^{1+\pi(b)}b^{\pi(b)-1} = b^{\pi(b)} - bb^{\pi(b)-1} = b^{\pi(b)} - b^{\pi(b)} = 0$$

et puisqu'ils commutent on a $b^{\pi(b)}(1 - b^{\pi(b)}) = (1 - b^{\pi(b)})b^{\pi(b)} = 0$, donc $b^{\pi(b)}$ et $(1 - b^{\pi(b)})$ sont orthogonaux et par suite pour tout entier non nul k on a

$$1 = (1 - b^{\pi(b)} + b^{\pi(b)})^k = (1 - b^{\pi(b)})^k + (b^{\pi(b)})^k$$

Il resté à prouver que $\forall k \in \mathbb{N}^*, (b^{\pi(b)})^k = b^{\pi(b)}$. Si $k = 1$, c'est clair, si $k \in \mathbb{N}^*$ tel que la relation est vraie, on a $(b^{\pi(b)})^{k+1} = b^{2\pi(b)} = b^{1+\pi(b)}b^{\pi(b)-1} = bb^{\pi(b)-1} = b^{\pi(b)}$. Finalement pour tout $k \in \mathbb{N}^*$, on a :

$$(\star\star) \quad (b + 1 - b^{\pi(b)})^k = b^k + (1 - b^{\pi(b)})^k = b^k + 1 - b^{\pi(b)}.$$

• Dédutions :

- Comme $\pi(b) \in \mathbb{N}^*$, on peut appliquer $(\star\star)$ pour le cas $k = \pi(b)$, ce qui donne :

$$(b + 1 - b^{\pi(b)})^{\pi(b)} = b^{\pi(b)} + (1 - b^{\pi(b)}) = 1,$$

donc $b + 1 - b^{\pi(b)} \in \mathfrak{U}(R)$ et $(b + 1 - b^{\pi(b)})^{-1} = (b + 1 - b^{\pi(b)})^{\pi(b)-1}$.

- Si on note $N = \text{card}(\mathfrak{U}(R))$ on va démontrer que $\pi(b)$ c'est l'ordre de $x = b + 1 - b^{\pi(b)}$, pour cela soit $k \in \mathbb{N}^*$ tel que $b + 1 - b^{\pi(b)} = 1$, d'après la dernière égalité du $(\star\star)$ on a $1 = 1 + b^k - b^{\pi(b)}$, donc $b^k = b^{\pi(b)}$. La division euclidienne de k par $\pi(b)$ donne $k = q\pi(b) + r$ avec $0 \leq r < \pi(b)$, on a $b^k = (b^{\pi(b)})^q \cdot b^r = b^{r+\pi(b)} = b^r$, donc $b^r = b^{\pi(b)}$, donc $b = b^{1+\pi(b)} = b^{1+r}$ et comme $r < \pi(b)$ et $\mu(b) = 1$, on a $r = 0$, donc $\pi(b) | k$, donc $\pi(b)$ c'est l'ordre de x donc $\pi(b) | N = \text{card}(\mathfrak{U}(R))$.

(c) On a posé $\mathcal{N}(R) = \{x \in R \mid \exists m \geq 1, x^m = 0\}$, c'est l'ensemble des éléments nilpotents de R .

• Soit $c \in \mathcal{N}(R)$. Il existe un entier $m \geq 1$ tel que $c^m = 0$. Considérons l'élément :

$$d = 1 + c + c^2 + \dots + c^{m-1},$$

et calculons $(1-c)d$, on a $(1-c)d = (1-c)(1+c+c^2+\dots+c^{m-1}) = 1-c^m = 1-0 = 1$. De même, $d(1-c) = 1$. Donc $(1-c) \in \mathfrak{U}(R)$ et $(1-c)^{-1} = d = 1 + c + \dots + c^{m-1}$.

• Dédution : Soit $c \in \mathcal{N}(R)$. Pour tout entier $k \geq 1$, l'élément c^k est encore nilpotent : en effet, si $c^m = 0$, alors $(c^k)^m = c^{km} = 0$ car $km \geq m$. Donc, d'après le point précédent appliqué à c^k , on a :

$$1 - c^k \in \mathfrak{U}(R).$$

Ainsi, la suite $(1 - c^k)_{k \geq 1}$ est une suite d'éléments du groupe fini $\mathfrak{U}(R)$. Posons $N = \text{Card}(\mathfrak{U}(R))$. Comme $\mathfrak{U}(R)$ est fini, cette suite ne peut pas être injective : parmi les $N + 1$ premiers termes $1 - c^1, 1 - c^2, \dots, 1 - c^{N+1}$, il existe deux indices distincts p, q avec $1 \leq p < q \leq N + 1$ tels que :

$$1 - c^p = 1 - c^q.$$

En simplifiant, on obtient $c^p = c^q$. Cela signifie que la suite (c^n) est périodique à partir du rang p , de période divisant $q - p$. Donc $c \in \mathcal{P}(R)$ et :

$$\mu(c) \leq p \leq N = \text{Card}(\mathfrak{U}(R)).$$

Ainsi, tout élément nilpotent c vérifie $\mu(c) \leq \text{Card}(\mathfrak{U}(R))$ lorsque $\mathfrak{U}(R)$ est fini.

(d) Soit $a \in \mathcal{P}(R)$ et choisissons $k \geq 1$ tel que $a^k \in \mathcal{J}(R)$, c'est-à-dire $a^{2k} = a^k$. Posons $b = a^{k+1}$ et $c = a(1 - a^k)$. On a $a = b + c$. Calculons bc :

$$bc = a^{k+1}a(1 - a^k) = a^{k+2} - a^{2k+2}.$$

Or

$$a^{2k+2} = a^{2k}a^2 = a^k a^2 = a^{k+2},$$

car $a^{2k} = a^k$. Donc

$$bc = a^{k+2} - a^{k+2} = 0.$$

Comme b et c sont tous deux des polynômes en a , ils commutent ; ainsi $bc = cb = 0$. Les éléments b et c sont donc orthogonaux.

- Montrons que $\mu(b) \leq 1$: Pour tout $n \in \mathbb{N}^*$, on a $b^n = a^{n+k}$. Il suffit de prouver qu'il existe $n \in \mathbb{N}^*$ tel que $b^{n+1} = b$, c'est-à-dire tel que $a^{n+k+1} = a^{k+1}$, pour cela remarquons que $a^{2k} = a^k$ donne $\mu(a) \leq k$. La division euclidienne de $k - \mu(a)$ par $\pi(a)$ donne $k = \mu(a) + q\pi(a) + r$ avec q, r des entiers et $r < \pi(a)$, donc $x^k = x^{\mu(a)+r}$. Prenons $n = \pi(a)$, on a $b^n = x^{n+k+1} = x^{\mu(a)+(q+1)\pi(a)+r+1} = x^{\mu(a)+r+1} = b$. Il en découle que $\mu(b) \leq 1$.

- Preuve que $c \in \mathcal{N}(R)$: On a : $c^k = (a(1 - a^k))^k = a^k(1 - a^k)^k$. Or, $a^k \in \mathcal{J}(R)$ signifie que a^k est idempotent. Donc $1 - a^k$ est aussi idempotent (d'après I.1.c), c'est-à-dire $(1 - a^k)^2 = 1 - a^k$. Par récurrence, simple on a : $\forall m \in \mathbb{N}^*, (1 - a^k)^m = 1 - a^k$. Donc $c^k = a^k(1 - a^k) = a^k - a^{2k} = 0$, donc $c \in \mathcal{N}(R)$.

- Si $\mathfrak{U}(R)$ est fini, posons $N = \text{card}(\mathfrak{U}(R))$. Par II.2.b, on a $\pi(b) \mid N$, et par II.2.c, on a $\mu(c) \leq N$. Comme $a = b + c$ avec b, c orthogonaux, II.2.a donne $\mu(a) \leq \max(\mu(b), \mu(c)) \leq N$ et $\pi(a) \mid \text{ppcm}(\pi(b), \pi(c))$. La composante nilpotente c n'a pas de partie périodique non triviale, donc $\pi(c) = 1$. Ainsi $\mu(a) \leq N$, et $\pi(a) \mid N$. Si R est un corps fini, alors $\mathfrak{U}(R)$ est un groupe de cardinal $\text{card}(R) - 1$. On retrouve donc $\pi(a) \mid \text{card}(R) - 1$, pour tout élément non nul, tandis que 0 a période 1.