Anneaux

Marc SAGE

3 novembre 2011

Table des matières

On utilisera pour tous objets a et b le ***symbole de Kronecker***[1] $\delta_a^b := \begin{cases} 1 \text{ si } a = b \\ 0 \text{ si } a \neq b \end{cases}$.

Les anneaux sont supposés unitaires (l'unité est notée 1) mais pas nécessairement commutatifs. Une ***unité*** désigne un élément inversible.

On dire qu'un élément a ***divise*** un élément b si on peut écrire $b = \lambda a$ pour un certain élément λ. On écrira alors $a \mid b$.

1 Mise en jambe

1. *À quelle condition une homothétie dans un anneau commutatif A est-elle un endomorphisme de A ?*
2. *On se donne deux anneaux commutatifs A et B ainsi qu'une application $f : A \longrightarrow B$ qui préserve la somme et le carré. En supposant 2 régulier dans B, montrer que f préserve le produit. Est-ce que f est un morphisme d'anneaux ?*
3. *Trouver un anneau qui est isomorphe à l'un de ses sous-anneaux stricts.*
4. *Déterminer les nilpotents de l'anneau $\mathbb{Z}/n$.*

Solution proposée.

1. Considérons une homothétie $\lambda\cdot$ qui soit un morphisme d'anneaux. L'additivité ne posant aucun problème[2], utilisons la multiplicativité : pour tous a, b dans A on doit avoir $\lambda(ab) = (\lambda a)(\lambda b) = \lambda^2 ab$; prenant $a = b = 1$, on voit que λ est un idempotent, condition qui réciproquement suffit.

2. Il s'agit d'écrire un produit à l'aide de somme et de carré. Une possibilité est d'invoquer l'identité $2a\alpha = (a+\alpha)^2 - a^2 - \alpha^2$ valable pour tous $a, \alpha \in A$. Appliquer f donne $2f(a\alpha) = (f(a) + f(\alpha))^2 - f(a)^2 - f(\alpha)^2$; or le membre de droite vaut aussi $2f(a)f(\alpha)$ d'après la même identité[3], ce qui conclut en invoquant la régularité de 2 dans B.

   Notre f sera un morphisme d'anneaux s'il préserve l'unité. Le morphisme nul est un contre-exemple trivial. On peut même en trouver des non nuls[4] : on a toujours l'idempotence de $f(1)$ (puisque $f(1)^2 = f(1^2) = f(1)$), donc il faut chercher un B possédant d'autres idempotents que 0 et 1, par exemple un anneau produit. Ainsi, tout morphisme d'anneaux $\varphi : A \longrightarrow B$ induit un morphisme $\begin{cases} A & \longrightarrow & B^2 \\ a & \longmapsto & (\varphi(a), 0) \end{cases}$ préservant somme et produit mais pas l'unité.

3. On doit clairement chercher dans les anneau infinis. Des anneaux classiques sont les anneaux de polynômes $P_I := \mathbb{Z}[(X_i)]_{i\in I}$ pour tout ensemble I : il est immédiat de vérifier que P_I et P_J sont isomorphes dès que I et J sont équipotents. Ainsi, en choisissant un ensemble d'indéterminées qui soit équipotent à l'une de ses parties stricte (par exemple $I := \mathbb{Z} \simeq \mathbb{N} =: J \subsetneq I$), on obtient un isomorphime de P_I sur le sous-anneau strict P_J.

4. Soit $a = \prod p^{v_p}$ un nilpotent décomposé en facteurs premiers. Il y a un entier $k \geq 1$ tel que a^k soit nul modulo n, *i. e.* tel que n divise $\prod p^{kv_p}$. Ainsi, tous les facteurs premiers de n sont compris dans ceux de a. Réciproquement, si a contient tous les facteurs premiers de n, alors a^k sera multiple de n pour k plus grand que toutes les valuations p-adiques de n.

Remarque. Le lecteur versé en algèbre commutative pourra apprécier une solution plus « pédestre » pour la dernière question : les nilpotents constituent le nilradical, lequel vaut l'intersection des idéaux premiers. Or d'une part les idéaux premiers d'un quotient A/I sont les idéaux premiers de A contenant I, d'autre part les idéaux premiers de $\mathbb{Z}$ sont les (p) pour p premier. Ainsi, les idéaux premiers concernés sont les (p) contenant (n), à savoir les (p) pour p divisant n. Enfin, l'intersection d'un nombre fini d'idéaux principaux (a_i) est l'idéal engendré par le ppcm des a_i (lorsqu'il existe) : dans notre cas, l'intersection recherchée est donc l'idéal engendré par les premiers divisant n, à savoir tous les entiers dont les facteurs premiers contiennent tous ceux de n.

[1] Certains notent le $\delta_{a,b}$. Il me semble plus lisible de comparer deux expressions – nécessairement écrites dans une dimension selon le sens de l'écriture – en utilisant l'autre dimension du papier. De même, il est plus facile de comparer des couples $\binom{a}{b}$ et $\binom{\alpha}{\beta}$ plutôt que des couples (a, b) et (α, β), surtout si les coordonnées sont longues.

[2] la distribuvité dans un anneau s'exprime exactement en disant que toutes ses homothéties sont additives

[3] remplacer (a, b) par $(f(a); f(b))$

[4] cela revient à la non-nullité de $f(1)$

2 « Morpher » des anneaux

On se demande s'il est possible de trouver un morphisme d'un anneau donné A vers n'importe quel anneau B.

1. *Montrer que seuls les anneaux B possibles doivent vérifier* $\operatorname{car} B \mid \operatorname{car} A$. *Donner des exemples.*
2. *Montrer que la réponse au problème est affirmative (avec les restrictions de la questions précédentes) si elle l'est pour l'anneau* $B = {}^{\mathbb{Z}}\!/_{\operatorname{car} A}$.
3. *Répondre à la question lorsque A est :*
   (a) *un corps de caractéristique nulle ;*
   (b) *l'anneau $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$ des entiers de Gauss ;*
   (c) *l'anneau de matrices*[5] *$M_2(\mathbb{Z})$.*

Solution proposée.

1. Étant donné un morphisme $A \longrightarrow B$, la composée $\mathbb{Z} \longrightarrow A \longrightarrow B$ est un morphisme, donc est *le* morphisme $\mathbb{Z} \longrightarrow B$. Or, $\operatorname{car} A$ est tué (au passage dans A), *i. e.* est dans $\operatorname{Ker}(\mathbb{Z} \longrightarrow B) = \mathbb{Z} \operatorname{car} B$, *CQFD.*

   Par exemple, on pourra réduire modulo 2 n'importe quel entier défini modulo un pair, ou réduire modulo un premier p tout entier défini modulo une puissance de p, ce qui revient à définir des morphismes ${}^{\mathbb{Z}}\!/_{2n} \longrightarrow {}^{\mathbb{Z}}\!/_{2}$ et ${}^{\mathbb{Z}}\!/_{p^k} \longrightarrow {}^{\mathbb{Z}}\!/_{p}$.
2. Si l'on dispose d'un morphisme $A \longrightarrow {}^{\mathbb{Z}}\!/_{\operatorname{car} A}$, on obtientra pour tout anneau B tel que $\operatorname{car} B \mid \operatorname{car} A$ d'un morphisme $A \longrightarrow B$ à l'aide des composées $A \longrightarrow {}^{\mathbb{Z}}\!/_{\operatorname{car} A} \longrightarrow {}^{\mathbb{Z}}\!/_{\operatorname{car} B} \longrightarrow B$.
   (a) Lorsque A est un corps K de caractéristique nulle, on cherche un morphisme $K \longrightarrow \mathbb{Z}$. Or $1 = 2\frac{1}{2}$ est un double dans K, donc son image 1 doit être un double dans $\mathbb{Z}$, ce qui n'est pas.
   (b) Si un élément de A est racine d'un polynôme entier qui n'a pas de racine dans $\mathbb{Z}$, comme c'est le cas de i dans $\mathbb{Z}[i]$, alors l'image de cet élément ne peut exister.
   (c) Pour étudier un morphisme d'anneaux $M_2(\mathbb{Z}) \longrightarrow \mathbb{Z}$, on regarde des générateurs, par exemples les matrices $1 := \begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix}$, $p := \begin{pmatrix} 1 & \cdot \\ \cdot & \cdot \end{pmatrix}$, $n := \begin{pmatrix} \cdot & \cdot \\ 1 & \cdot \end{pmatrix}$ et $\nu := \begin{pmatrix} \cdot & 1 \\ \cdot & \cdot \end{pmatrix}$. Vu les relations $n^2 = \nu^2 = 0$, les images de n et ν sont nilpotentes dans $\mathbb{Z}$, donc nulles. De même, l'image de l'idempotent p est un entier idempotent, à savoir 0 ou 1. Une matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = d1 + (a-d)\,p + cn + b\nu$ sera donc envoyée sur sur d ou $d + (a-d) = a$. Mais aucune de ces applications coordonnées ne commute au produit comme le montre l'égalité $\begin{pmatrix} 1 & 1 \\ 1 & \cdot \end{pmatrix}^2 = \begin{pmatrix} 2 & ? \\ ? & 1 \end{pmatrix}$.

Remarque. La même question est triviale pour les monoïdes (*a fortiori* les groupes et donc les espaces vectoriels) qui sont toujours muni du morphisme constamment égal au neutre.

Dans les trois exercices suivants, le lecteur pourra s'exercer au calcul annelé (essentiellement développer des produits et regrouper intelligemment les termes d'une même somme).

[5] Il s'agit de $\mathbb{Z}^4$ muni de la somme produit et de la multiplication $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} := \begin{pmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{pmatrix}$.

3 Calcul de sommes dans $\mathbb{Z}$

On se donne un entier $n \geq 0$. *Calculer les sommes suivantes :*

1. $\sum_{a=0}^{n} a^2$;
2. $\sum_{a=0}^{n} a^3$;
3. $\sum_{1\leq a,b\leq n} \max\{a,b\} \min\{a,b\}$;
4. $\sum_{1\leq a,b\leq n} \max\{a,b\}^2$.

Solution proposée.

1. Une idée est de créer un télescopage en décalant les indices ainsi que l'exposant. On obtient ainsi une équation en la somme S cherchée :

$$\begin{aligned}
\sum_{a=0}^{n+1} a^3 &= \sum_{a=1}^{n+1} a^3 = \sum_{a=0}^{n} (a+1)^3 = \sum_{a=0}^{n} a^3 + 3\sum_{a=0}^{n} a^2 + 3\sum_{a=0}^{n} a + \sum_{a=0}^{n} 1 \\
\text{d'où } (n+1)^3 &= 3S + 3\frac{n(n+1)}{2} + n + 1, \\
\text{puis } \frac{6S}{n+1} &= 2(n+1)^2 - 3n - 2 = n(2n+1) \text{ et } S = \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

   L'avantage de cette méthode est qu'elle se généralise immédiatement pour calculer récurisivement les sommes de Bernoulli $\sum_{a=0}^{n} a^k$ pour tout entier naturel k.

2. On applique ce qui précède, en étant plus finaud : on fait apparaître la somme S cherchée en réindexant la somme dans l'autre sens, l'imparité de l'exposant 3 assurant que S ne disparaîtra dans le processus :

$$\begin{aligned}
\sum_{a=0}^{n} a^3 &= \sum_{a=0}^{n} (n-a)^3 = n^3 \sum_{a=0}^{n} 1 - 3n^2 \sum_{a=0}^{n} a + 3n \sum_{a=0}^{n} a^2 - \sum_{a=0}^{n} a^3, \\
\text{d'où } S &= n^3(n+1) - 3n^2 \frac{n(n+1)}{2} + 3n \frac{n(n+1)(2n+1)}{6} - S \\
\text{et } 2S &= n(n+1)\left(n^2 - \frac{3}{2}n^2 + n^2 + \frac{1}{2}n\right) = \frac{1}{2}n^2(n+1)^2.
\end{aligned}$$

   La somme des a^3 vaut donc le carré de celle des a.

3. Il est naturel de séparer la somme en deux selon que $a \leq b$ ou $a > b$ afin de calculer les max et min de la sommande[6] :

$$\sum_{a,b} \max\{a,b\} \min\{a,b\} = \left[\sum_{a<b} + \sum_{a=b} + \sum_{a>b}\right] \max\{a,b\} \min\{a,b\} = \sum_{a<b} ab + \sum_{a} aa + \sum_{a>b} b.$$

   À ce stade, on peut reparamétrer la troisième somme en échangeant les variables, ce qui donne $\sum a^2 + 2\sum_{a<b} ab$. On peut alors calculer chaque somme séparément : la première est déjà connue depuis la question 1 et la seconde peut se séparer en sommes à b constant :

$$\sum_{a<b} ab = \sum_{b} \sum_{a<b} ab = \sum_{b} b \sum_{a=1}^{b-1} a = \sum_{b} b\frac{b(b-1)}{2}, \text{ d'où } 2\sum_{a<b} ab = \sum a^3 - \sum a^2$$

   et le résultat $\sum a^3$.

   Une idée plus diabolique consiste à remonter les calculs une fois débarassés des et max : les trois sommes $\sum_{a\leq b} ab + \sum_{a} aa + \sum_{a>b} ba$ reviennent en effet à sommer le produit ab sur tous les couples (a,b) du carré entier $[1,n]^2$, ce qui donne la somme $\sum_{a,b} ab$. Sans condition liant a et b, on peut factoriser cette dernière en $\sum a \sum b = (\sum a)^2$, qui (sanity check) vaut bien $\sum a^3$ d'après la question 2.

[6] il est entendu que tous les indices sont compris entre 1 et n

4. On sépare la somme en trois bouts comme ci-dessus :

$$\sum_{a,b} \max\{a,b\}^2 = \sum_{a<b} b^2 + \sum_{a=b} a^2 + \sum_{a>b} a^2 \overset{\substack{a\leftrightarrow b \text{ dans} \\ \text{première } \Sigma}}{=} 2\sum_{a>b} a^2 + \sum_a a^2.$$

Or la première somme se calcule aisément en la séparant à a constant :

$$\sum_{a>b} a^2 = \sum_a a^2 \sum_{b<a} 1 = \sum_a a^2 (a-1) = \sum a^3 - \sum a^2.$$

Il en résulte que la somme cherchée vaut

$$\begin{aligned} 2\sum_{a>b} a^2 + \sum_a a^2 &= 2\left(\sum a^3 - \sum a^2\right) + \sum a^2 = 2\sum a^3 - \sum a^2 \\ &= \frac{n^2(n+1)^2}{2} - \frac{n(n+1)(2n+1)}{6} = \frac{n(n+1)}{6}\left(3n^2+3n-2n-1\right) \\ &= \frac{1}{6} n(n+1)\left(3n^2+n-1\right). \end{aligned}$$

Sanity check : pour $n=2$, les max valent $1,2,2,2$, donc la somme de leurs carrés vaut $1+4+4+4=13$, tandis que l'expression ci-dessus vaut $\frac{2\cdot 3}{6}(3\cdot 4+1) = 13$.

4 Pour apprendre à développer : matrices, polynômes exponentielles, fonctions symétriques

1. On se donne un entier $n \geq 1$ et un sur-anneau A de $\mathbb{R}$ muni de n^2 éléments spéciaux $(E_{i,j})_{1\leq i,j\leq n}$ au sens où tout élément de A s'écrive d'une unique façon comme combinaison linéaire des $E_{i,j}$ à coefficients réels :

$$\forall a \in A,\ \exists!\,(\lambda_{i,j}) \in \mathbb{R}^{n^2},\ a = \sum_{1\leq i,j\leq n} \lambda_{i,j} E_{i,j}.$$

Les scalaires $\lambda_{i,j}$ sont appelés les ***coordonnées*** de a.
Exprimer les coordonnées d'un produit ab en fonction de celles de a et de b.

2. On se donne un sur-anneau A de $\mathbb{R}$ muni d'un élément spécial $\alpha \in A$ au sens où tout élément de A s'écrive d'une unique façon comme combinaison linéaire des puissances de α à coefficients réels :

$$\forall a \in A,\ \exists!\,(\lambda_0, \lambda_1, ..., \lambda_n, 0, 0, 0, ...) \in \mathbb{R}^{(\mathbb{N})},\ a = \lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \cdots + \lambda_n\alpha^n.$$

Les scalaires $\lambda_0, ..., \lambda_n, 0, ...$ sont appelés les ***coordonnées*** de a.
Exprimer les coordonnées d'un produit ab en fonction de celles de a et de b.

3. On reprend le cadre de la question 2.
On dira qu'une famille $(a_1, ..., a_n) \in A^n$ est ***libre*** si toute combinaison linéaire nulle de la famille a tous ses coefficients nuls :

$$\overrightarrow{a} \text{ ***libre*** si } \forall \overrightarrow{\lambda} \in \mathbb{R}^n,\ \left(\sum \lambda_i a_i = 0 \implies \overrightarrow{\lambda} = \overrightarrow{0}\right).$$

Montrer la liberté de la famille $\left((\alpha+t)^p \alpha^q\right)_{p+q=n}$ où t est un réel non nul et n un entier naturel.

4. On se place dans un sur-anneau A de $\mathbb{Q}$. On appelle ***exponentielle*** d'un nilpotent $a \in A$ la somme

$$e^a := \sum_{n\geq 0} \frac{a^n}{n!}.$$

On se donne a et b deux nilpotents qui commutent. Montrer que la formule $e^a e^b = e^{a+b}$ fait sens et est valide.

5. Pour tout entier $k \geq 0$ et toute famille finie $\overrightarrow{a} = (a_1, ..., a_n)$, on note $e_k(\overrightarrow{a})$ la somme de tous les produits de k éléments[7] de $\overrightarrow{a}$:

$$e_k(\overrightarrow{a}) := \sum_{I \subset \{1,...,n\}}^{|I|=k} \prod_{i \in I} a_i.$$

On se donne un élément a_0 hors d'une famille $\overrightarrow{a} = (a_1, ..., a_n)$ Établir l'égalité $e_{k+1}(a_0, \overrightarrow{a}) = e_{k+1}(\overrightarrow{a}) + a_0 \sigma_k(\overrightarrow{a})$ puis en déduire le développement $\prod_{i=1}^{n}(1 + a_i) = \sum_{k=0}^{n} e_k(\overrightarrow{a})$.

Solution proposée.
(Par commodité d'écriture, tous les indices de sommation seront des entiers positifs ou nuls.)

1. Soient a et b deux élements de A dont on note $(a_{i,j})$ et $(b_{i,j})$ les coordonées. Leur produit vaut

$$ab = \sum_{i,j} a_{i,j} E_{i,j} \sum_{k,l} b_{k,l} E_{k,l} = \sum_{i,j,k,l} a_{i,j} E_{i,j} b_{k,l} E_{k,l} = \sum_{i,j,k,l} a_{i,j} b_{k,l} \delta_j^k E_{i,l}.$$

Vu le Kronecker dans la sommande, tout quadruplet (i, j, k, l) avec $j \neq k$ apporte une contribution nulle. On peut donc (sans changer sa valeur) restreindre la somme aux triplets $(i, j = k, l)$:

$$ab = \sum_{i,k,l} a_{i,k} b_{k,l} E_{i,l} = \sum_{i,l} \left(\sum_k a_{i,k} b_{k,l} \right) E_{i,l}.$$

Ainsi, en notant $[c]_{i,j}$ la coordonnée d'un élément $c \in A$, on obtient la formule

$$[ab]_{i,j} = \sum_x [a]_{i,x} [b]_{x,j}.$$

2. Soient $a = \sum_{p \leq n} a_p X^p$ et $b = \sum_{q \leq n} b_q X^q$ deux élements de A (on peut prendre le même n puisque a_k et b_k sont nuls pour k assez grand). Leur produit vaut

$$ab = \sum_{p \leq n} a_p X^p \sum_{p \leq n} b_q X^q = \sum_{p,q \leq n} a_p X^p b_q X^q = \sum_{p,q \leq n} a_p b_q X^{p+q}.$$

Les coordonnées se lisant devant chaque puissance de X, il faut regrouper les termes ayant même puissance, ce qui se fait en séparant la somme en sommes à $p + q$ constant. Cela revient à partitionner le domaine de sommation en droites de pentes -1, ce qui n'est guère pratique avec le carré $[0, n]^2$. Puisque les a_k et b_k sont nuls pour $k > n$, on peut sans changer (la valeur de) la somme remplacer le carré par n'importe triangle le contenant, par exemple celui de sommets $\binom{0}{0}$, $\binom{0}{2n}$, $\binom{2n}{0}$. On peut ainsi écrire

$$\sum_{p,q \leq n} a_p b_q X^{p+q} = \sum_{p+q \leq 2n}^{p,q} a_p b_q X^{p+q} = \sum_{s \leq 2n} \left(\sum_{p+q=s} a_b b_q \right) X^s,$$

d'où, en notant $[c]_k$ la k-ième coordonnée d'un élément $c \in A$), la formule

$$[ab]_k = \sum_{i+j=k}^{i,j \geq 0} [a]_i [b]_j.$$

3. Partons d'une relation de liaison $\sum_{p+q=n} \lambda_p (\alpha + t)^p \alpha^q = 0$ et montrons que tous les λ_p sont nuls. On va tout développer puis regrouper les termes selon les puissances de α, lesquels seront nuls d'après l'unicité de la décomposition (le membre de droite est nul) :

$$\sum_{p+q=n} \lambda_p (\alpha + t)^p \alpha^q = \sum_{p+q=n} \lambda_p \sum_{i+j=p} \binom{p}{i} \alpha^i t^j \alpha^q = \sum_{p+q=n}^{i+j=p} \lambda_p \binom{p}{i} t^j \alpha^{i+q}.$$

Vu l'exposant de α dans la sommande, il faut sommer à $i + q$ constant ; or cette somme vaut $i + q = (p - j) + q = (p + q) - j = n - j$, donc il revient au même de sommer à j constant :

$$0 = \sum_{p+q=n}^{i+j=p} \lambda_p \binom{p}{i} t^j \alpha^{i+j} = \sum_{j \leq n} \sum_{p+q=n}^{0 \leq i = p-j} \lambda_p \binom{p}{p-j} t^j \alpha^{n-j} = \sum_{j \leq n} t^j \left[\sum_{p+q=n}^{p \geq j} \lambda_p \binom{p}{j} \right] \alpha^{n-j}.$$

[7] on note $|E| = \operatorname{Card} E$ le cardinal d'un ensemble E

Par unicité de la décomposition, tous les coefficients devant les α^{n-j} sont nuls. En simplifiant[8] par t^j, on tombe sur un système triangulaire en les λ_p :

$$\begin{aligned}
\binom{n}{n}\lambda_n &= 0 \qquad (j=n)\\
\binom{n-1}{n-1}\lambda_{n-1}+\binom{n}{n-1}\lambda_n &= 0 \qquad (j=n-1)\\
\binom{n-2}{n-2}\lambda_{n-2}+\binom{n-1}{n-2}\lambda_{n-1}+\binom{n}{n-2}\lambda_n &= 0 \qquad (j=n-2)\\
&\dots.
\end{aligned}$$

Les coefficients diagonaux étant tous non nuls (ils valent tous $\binom{k}{k}=1$), on trouve de proche en proche $\lambda_n=0$, $\lambda_{n-1}=0$, $\lambda_{n-2}=0$..., ce qui conclut.

4. La somme définissant e^a est bien finie : si $a^k=0$, alors $e^a=\sum_{n<k}\frac{a^n}{n!}$.

La formule $e^ae^b=e^{a+b}$ fera sens si $a+b$ est nilpotent ; or ses puissances se développent aisément puisque a et b commutent :

$$(a+b)^n=\sum_{p+q=n}\binom{n}{p}a^pb^q.$$

Vu la condition $p+q=n$, l'un des exposants p ou q est $\geq\frac{n}{2}$, donc l'un des éléments a^p ou b^q sera nul en choissant $\frac{n}{2}$ plus grand que des entiers (k,l) tels que $a^k=0=b^l$ (et il en existe d'après la nilpotence de a et b), par exemple $n=k+l$.

On peut donc écrire $e^{a+b}=\sum_{n\leq k+l}\frac{(a+b)^n}{n!}$ et développer

$$e^{a+b}=\sum_{n\leq k+l}\frac{1}{n!}\sum_{p+q=n}\binom{n}{p}a^pb^q=\sum_{n\leq k+l}\frac{a^pb^q}{p!q!}.$$

Par ailleurs, le produit e^ae^b se développe

$$e^ae^b=\sum_{p\leq k}\frac{a^p}{p!}\sum_{q\leq l}\frac{b^q}{q!}=\sum_{p\leq k}^{q\leq l}\frac{a^pb^q}{p!q!}.$$

Oberver que la sommande est la même : d'un côté, on somme sur le triangle de sommets $\binom{0}{0}$, $\binom{k+l}{0}$, $\binom{0}{k+l}$, de l'autre on somme sur le rectangle de sommets $\binom{0}{0}$, $\binom{k}{0}$, $\binom{0}{l}$, $\binom{k}{l}$. Or le triangle contient le rectangle et la sommande est nulle en-dehors du rectangle (un des facteurs a^p ou b^q doit s'annuler), ce qui montre que les deux sommes coïncident, *CQFD*.

5. Intuivement, la formule est claire : pour faire un produit de $k+1$ facteurs parmi a_0 et $\overrightarrow{a}$, ou bien l'on choisit d'une part a_0 et d'autre part k facteurs dans $\overrightarrow{a}$, ou bien l'on ne choisit pas a_0 et l'on choisit $k+1$ facteurs parmi $\overrightarrow{a}$.

Formellement, la distinction ci-dessus revient à séparer le domaine de sommation de $e_{k+1}(a_0,\overrightarrow{a})=\sum_{I\subset\{0,\dots,n\}}^{|I|=k+1}\prod_{i\in I}a_i$ selon que l'indice 0 appartienne ou non à la partie I. On obtient ainsi d'une part les parties $I\subset\{1,\dots,n\}$, d'autre part les parties I qui s'écrivent sous la forme $I=\{a_0\}\sqcup J$ où $J\subset\{1,\dots,n\}$ (ce qui amènera à reparamétrer par les parties $J\subset\{1,\dots,n\}$ de cardinal $|I|-1=k$). Il vient par conséquent

$$\begin{aligned}
e_{k+1}(a_0,\overrightarrow{a}) &= \sum_{I\subset\{0,\dots,n\}}^{|I|=k+1}\prod_{i\in I}a_i=\sum_{I\subset\{1,\dots,n\}}^{|I|=k+1}\prod_{i\in I}a_i+\sum_{J\subset\{1,\dots,n\}}^{|J|=k}\prod_{i\in\{a_0\}\sqcup J}a_i\\
&= e_{k+1}(\overrightarrow{a})+a_0\sum_{J\subset\{1,\dots,n\}}^{|J|=k}\prod_{j\in J}a_j)=e_{k+1}(\overrightarrow{a})+a_0e_k(\overrightarrow{a}).
\end{aligned}$$

La formule demandée, qui est claire pour $n\in\{0,1\}$, s'obtient alors par récurrence :

$$\prod_{i=0}^{n}(1+a_i)=(1+a_0)\prod_{i=1}^{n}(1+a_i)=(1+a_0)\sum_{k=0}^{n}e_k(\overrightarrow{a})=\sum_{k=0}^{n}e_k(\overrightarrow{a})+a_0\sum_{k=0}^{n}e_k(\overrightarrow{a}).$$

[8] on peut car λ est non nul par hypothèse ; d'ailleurs, s'il l'était, la famille considérée serait constante et ne serait pas libre du tout (sauf si $n=0$)

Pour utiliser la formule précédente, on crée un décalage d'indice. Afin d'éviter les effets de bord, on peut avant cela étendre la première somme à $k = n+1$ (il n'y pas de produit à $n+1$ facteurs dans la famille $\overrightarrow{a}$) et la seconde à $k = -1$ (un produit ne peut avoir -1 facteurs) :

$$\begin{aligned}\prod_{i=0}^{n}(1+a_i) &= \sum_{k=0}^{n+1} e_k\left(\overrightarrow{a}\right) + a_0 \sum_{k=-1}^{n} e_k\left(\overrightarrow{a}\right) \overset{\text{décalage dans le second } \Sigma}{=} \sum_{k=0}^{n+1} e_k\left(\overrightarrow{a}\right) + a_0 \sum_{k=0}^{n+1} e_{k-1}\left(\overrightarrow{a}\right) \\ &= \sum_{k=0}^{n+1} \left(e_k\left(\overrightarrow{a}\right) + a_0 e_{k-1}\left(\overrightarrow{a}\right)\right) = \sum_{k=0}^{n+1} e_k\left(a_0, \overrightarrow{a}\right), \ CQFD.\end{aligned}$$

Remarques.

Les anneaux des questions 1 et 2 ne sont autres que les anneaux $M_n(\mathbb{R})$ des matrices réelles et $\mathbb{R}[X]$ des polynômes à coefficients réels dont l'on a fait (re)découvrir la définition du produit. La question 3 est un exercice sur les polynômes que l'on peut traiter sans calculs (*cf.* feuilles sur les polynômes).

Le calcul sur les exponentielles dans la question 4 est le même utilisé pour l'exponentielle complexe – aux problèmes de convergence près, liés à la non-finitude des sommes considérées.

Le développement obtenu à la question 5 n'est qu'un cas particulier de la formule générale de distributivité (où les a_i et les b_j commutent tous entre eux)

$$\prod_{i=1}^{n}(a_i + b_i) = \sum_{I,J\subset\{1,..,n\}}^{I\sqcup J=\{1,..,n\}} \prod_{i\in I} a_i \prod_{j\in J} b_j$$

qui se généralise aisément en (avec tous les a_i^j commutant entre eux)

$$\prod_{i=1}^{n}\left(a_i^1 + a_i^2 + \cdots + a_i^p\right) = \sum_{\substack{I_1,\ldots,I_p\subset\{1,\ldots,n\} \\ I_1\sqcup\cdots\sqcup I_p=\{1,\ldots,n\}}} \prod_{i\in I_1} a_i^1 \prod_{i\in I_2} a_i^2 \ \cdots \prod_{i\in I_p} a_i^p.$$

5 Pour apprendre à sommer sur n'importe quoi

Calculer pour tout ensemble E fini la somme $\sum_{A\subset E}(-1)^{\operatorname{card} A}$.
En déduire la somme $\sum_{I\subset\{1,\ldots,n\}}(-1)^{|I|}\left(\sum_{i\in I}\lambda_i\right)^n$ pour tous scalaires $\lambda_1, ..., \lambda_n$ d'un même anneau.

Solution proposée.

Vu la sommande, il est naturel de partionner le domaine de sommation $\mathfrak{P}(E) = \bigsqcup_{k=0}^{|E|}\{A\subset E\}_{|A|=k}$ selon le cardinal de la partie considérée. Il vient alors

$$\begin{aligned}\sum_{A\subset E}(-1)^{|A|} &= \sum_{k=0}^{|E|}(-1)^k \sum_{|A|=k}^{A\subset E} 1 = \sum_{k=0}^{|E|}(-1)^k \operatorname{Card}\{A\subset E \ ; \ |A| = k\} \\ &= \sum_{k=0}^{|E|}(-1)^k \binom{n}{k} = (1-1)^n = \delta_0^n = \delta_E^{\emptyset}.\end{aligned}$$

On attaque à présent la grosse somme en développant la puissance n-ième :

$$\sum_{I\subset\{1,\ldots,n\}}(-1)^{|I|}\left(\sum_{i\in I}\lambda_i\right)^n = \sum_{I\subset[1,n]}(-1)^{|I|}\sum_{i_1,\ldots,i_n\in I}\lambda_{i_1}\cdots\lambda_{i_n} = \sum_{i_1,\ldots,i_n\in I}^{I\subset[1,n]}\lambda_{i_1}\cdots\lambda_{i_n}(-1)^{|I|}.$$

En choisissant d'abord les indices $i_1, ..., i_n$ dans $[1, n]$, le choix de $I \supset \{i_1, ..., i_n\}$ revient à choisir[9] une partie $J \subset [1, n]\setminus\{i_1, ..., i_n\}$ (écrire $I = \{i_1, ..., i_n\}\sqcup J$) :

$$\sum_{i_1,\ldots,i_n\in I}^{I\subset[1,n]}\lambda_{i_1}\cdots\lambda_{i_n}(-1)^{|I|} = \sum_{\overrightarrow{i}\in[1,n]}\lambda_{i_1}\cdots\lambda_{i_n}\sum_{I\supset\{i_1,\ldots,i_n\}}(-1)^{|I|}.$$

[9] De manière très formelle, on partitionne le domaine de sommation

$$\{(i_1, ..., i_n, I)\in[1,n]^n\times\mathsf{P}\,[1,n] \ ; \ \{i_1, ..., i_n\}\subset I\}$$

La seconde somme se calcule aisément grâce à la première question (on note $\#\overrightarrow{i}$ le cardinal de $\{i_1,...,i_n\}$) :

$$\sum_{I\supset\{i_1,...,i_n\}}(-1)^{|I|}=\sum_{J\subset\{1,...,n\}\setminus\{i_1,...,i_n\}}(-1)^{|J|+\#\overrightarrow{i}}=(-1)^{\#\overrightarrow{i}}\,\delta_{\emptyset}^{\{1,...,n\}\setminus\{i_1,...,i_n\}}=(-1)^n\,\delta_{\{i_1,...,i_n\}}^{\{1,...,n\}}.$$

La première somme $\sum_{\overrightarrow{i}\in[1,n]^n}$ est par conséquent restreinte aux familles $\overrightarrow{i}$ surjectives, c'est-à-dire aux bijections[10] $\overrightarrow{i}$ de $[1,n]$:

$$\sum_{I\subset\{1,...,n\}}(-1)^{|I|}\left(\sum_{i\in I}\lambda_i\right)^n=\sum_{\overrightarrow{i}\in[1,n]^n}\lambda_{i_1}\cdots\lambda_{i_n}\,(-1)^n\,\delta_{\{i_1,...,i_n\}}^{\{1,...,n\}}=(-1)^n\sum_{\overrightarrow{i}\in\mathfrak{S}_n}\lambda_{i_1}\cdots\lambda_{i_n}.$$

La sommande est alors constante égale à $\prod_{x\in\{i_1,...,i_n\}}\lambda_x=\prod_{x\in[1,n]}\lambda_x$. Puisque le groupe symétrique contient $n!$ éléments, on peut conclure :

$$\sum_{I\subset\{1,...,n\}}(-1)^{|I|}\left(\sum_{i\in I}\lambda_i\right)^n=n!\,(-1)^n\,\lambda_1\lambda_2\cdots\lambda_n.$$

On s'intéresse dans les trois prochains exercices à des questions typiquement non commutatives autour de l'inversibilité.

6 De l'intuition pour inverser $1+a$

1. *Soient dans un anneau une unité u et un nilpotent n qui commutent. Montrer que $u+n$ est aussi une unité. Contre-exemple sans la commutativité ?*
2. *Soient a et b deux éléments d'un anneau A tel que $1-ab$ soit inversible. Montrer que $1-ba$ est aussi inversible.*

Solution proposée.

1. Vu que[11] $u+n=u\left(1+\frac{n}{u}\right)$ et que $\frac{n}{u}$ est nilpotent (si $n^k=0$, alors on a $\left(\frac{n}{u}\right)^k=\frac{n^k}{u^k}=\frac{0}{u^k}=0$), il suffit de traiter le cas $u=1$.

   On intuite alors l'inverse à l'aide de la formule « physicienne »

   $$\frac{1}{1-x}=1+x+x^2+x^3+\cdots$$

   dont le membre de droite a le bon goût d'être bien défini pour x nilpotent. On vérifie alors que $1-n+n^2-n^3+...+(-1)^k\,n^k$ est bien l'inverse de $1+n$:

   $$(1+n)\sum_{i=0}^{k}(-1)^i\,n^i=\sum_{i=0}^{k}(-1)^i\,n^i+\sum_{i=0}^{k}(-1)^i\,n^{i+1}.$$

   En décalant l'indice de la seconde somme (on a mis le premier terme de côté) $\sum_{i=0}^{k}(-1)^i\,n^{i+1}\overset{j:=i+1}{=}1+\sum_{j=0}^{k-1}(-1)^{j-1}\,n^j$, on trouve 1 moins l'opposé de la première somme (le facteur d'indice k ne contribue pas à la somme), ce qui conclut.

---

en la réunion disjointe pour $(i_1,...,i_n)$ parcourant $[1,n]^n$ des ensembles des $(n+1)$-uplets $(i_1,...,i_n,I)$ tels que $I\supset\{i_1,...,i_n\}$. Ensuite, le reparmétrage des sommes à $(i_1,...,i_n)$ fixé vient de la bijection de la part $\{(i_1,...,i_n,I)\ ;\ I\supset\{i_1,...,i_n\}\}$ avec l'ensemble des parties de $[1,n]\setminus\{i_1,...,i_n\}$.donnée par

$$\left\{\begin{array}{ccc}\left(\overrightarrow{i},I\right)&\longmapsto&I\setminus\{i_1,...,i_n\}\\ \left(\overrightarrow{i},J\sqcup\{i_1,...,i_n\}\right)&\longleftarrow&J\end{array}\right.$$

[10] on note S_n leur ensemble, appelé **groupe symétrique** à n éléments

[11] la commutativité de u et n légitime la notation $\frac{n}{u}$ pouvant signifier nu^{-1} ou $u^{-1}n$

(Attention, nous n'avons montré l'inversibilité que d'un seul côté : pour nous dispenser de l'autre côté, on peut dire que, notre inverse étant un polynôme en n, il commute trivialement avec $1+n$.)

Pour un contre-exemple, en cherchant dans les matrices 2×2, on trouve que l'inversible $\begin{pmatrix} 1 & 1 \\ \cdot & 1 \end{pmatrix}$ plus le nilpotent $\begin{pmatrix} \cdot & \cdot \\ 1 & \cdot \end{pmatrix}$ n'est pas inversible (sanity check : ils ne commutent pas).

2. On va intuiter l'inverse toujours à l'aide de la formule

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots.$$

On l'applique de façon complètement non rigoureuse à $x = ba$ et on fait apparaître l'inverse i de $1-ab$:

$$\begin{aligned} \frac{1}{1-ba} &= 1 + ba + baba + bababa + ... \\ &= 1 + b\left(1 + ab + abab + ababab + ...\right)a \\ &= 1 + b\frac{1}{1-ab}a \\ &= 1 + bia. \end{aligned}$$

On pose donc $j := 1 + bia$ et on vérifie à la main que ça marche :

$$\begin{aligned} (1-ba)\,j &= (1-ba)\,(1+bia) = 1 + bia - ba - babia = 1 - ba + b1ia - babia \\ &= 1 - ba + b\underbrace{(1-ab)\,i}_{=1}a = 1 - ba + ba = 1 \end{aligned}$$

et pareil de l'autre côté :

$$j\,(1-ba) = (1+bia)\,(1-ba) = 1 - ba + bia - biaba = 1 - ba + b\left[i\,(1-ab)\right]a = 1.$$

Remarque. L'erreur est classique de ne vérifier qu'un sens pour les inverses car l'on raisonne trop souvent sur l'anneau $M_n(K)$ où cela est suffisant. On pourra méditer sur les tapis roulants[12] de $\mathbb{R}^{\mathbb{N}}$

$$\begin{cases} \gamma : (a_0, a_1, ...) \mapsto (a_1, a_2, ...) \\ \delta : (a_0, a_1, ...) \mapsto (0, a_0, a_1, ...) \end{cases},$$

lesquels vérifient $\gamma\delta = 1 \neq \delta\gamma$.

Remarque. Le même énoncé tient en remplaçant inversible par inversible à droite/gauche.

7 Inversibilité bilatère automatique

On se donne un anneau dans lequel toute suite croissante d'idéaux stationne.

Montrer que l'inversibilité est automatiquement bilatère. (On pourra s'intéresser à l'injectivité d'une homothétie et à ses noyaux itérés.)

Solution proposée.

Donnons-nous deux éléments a et b tels que $ab = 1$ et montrons $ba = 1$.

Quatre homothéties nous tendent les bras : deux choix pour le rapport (a ou b) et deux choix pour le côté. Essayons $a\cdot$, qui a le bon goût (comme $\cdot b$) d'envoyer 1 et ba sur la même image : on aura donc terminé si $a\cdot$ est injective.

Par ailleurs, les noyaux itérés $I_n := \mathrm{Ker}\,(a^n\cdot)$ suggérés par l'énoncé forment une suite croissante d'idéaux. On peut même préciser la croissance : elle est ou bien constante ou bien stricte (en effet, si l'on peut piocher un élément i dans un $I_n \setminus I_{n-1}$, alors l'élément bi tombe dans $I_{n+1} \setminus I_n$, ce qui montre par récurrence la stricte croissance à partir du rang n).

[12] pas trop longtemps quand même, sinon on créé des accidents dans les couloirs du RER

L'hypothèse impose donc $I_1 = I_0$, ce qui signifie l'injectivité de $a\cdot$, d'où la conclusion.

Remarque. Un tel anneau est dit ***noethérien***[13]. Lorsque l'on se restreint aux idéaux *principaux*, la ***noethérianité*** dit que toute suite (d'éléments de l'anneau) décroissante pour la divisibilité stationne : c'est cet argument qui permet dans $\mathbb{Z}$ de décomposer tout entier comme produit de premiers. Et c'est cet argument qui équivaut dans un anneau général à la décomposabilité de tout élément en produit d'irréductibles (modulo les inversibles). On renvoit à la feuille *Arithmétique des anneaux* pour plus de précisions.

8 Impossible d'avoir exactement 18 inverses à gauche

Soit a élément d'un anneau.

Montrer que l'ensemble des inverses à gauche de A est, s'il est non vide, en bijection avec le noyau de l'homothétie $\cdot a$. (Interpréter en termes linéaires.)

En déduire que, si a a au moins deux inverses à gauche, alors il en a une infinité.

Solution proposée.

Étant donné un inverse à gauche g_0, on a les équivalences suivantes pour tout $g \in A$:

$$g \text{ inverse à gauche} \iff ga = 1 \iff ga = g_0 a \iff (g - g_0)\, a = 0 \iff g - g_0 \in \operatorname{Ker}(\cdot a) \iff g \in g_0 + \operatorname{Ker}(\cdot a)\,.$$

Ainsi, les inverses à gauche s'obtiennent en translatant le noyau de $\cdot a$ selon un inverse à gauche fixé. (En termes linéaires, on pourrait, en considérant l'équation $ax = 1$ en l'inconnue x, vérifier l'adage « solution affine = solution particulière + solution linéaire ».)

Il suffit de montrer que $\operatorname{Ker}(\cdot a)$ est infini. Nous proposons deux chemins.

1. Montrons que $\operatorname{Ker}(\cdot a)$ admet une partie stricte équipotente à lui-même, ce qui revient à trouver une injection de $\operatorname{Ker}(\cdot a)$ dans lui-même non sujective. Or d'une part trouver des applications stabilisant $\operatorname{Ker}(\cdot a)$ est aisé (n'importe quelle homothétie $\lambda\cdot$ convient – attention au côté !), d'autre part tout élément régulier d'un côté fournit une injection de l'anneau dans lui-même (prendre l'homothétie associéé du bon côté) : à notre grande satisfaction, ces deux conditions sont simultanément réalisées par l'homothétie $a\cdot$. Montrons pour conclure que cette dernière ne saurait être surjective : si elle l'était, elle atteindrait a en un élément k du noyau de $\cdot a$, ce qui s'écrit $a = ak$ (avec $ka = 0$), d'où (en multipliant à droite par a) $a^2 = aka = a0 = 0$ puis (en multipliant deux fois par un inverse à gauche) $1 = 0$, ce qui force tous les éléments de l'anneau à coïncider et contredit l'existence de deux inverses à gauche.
2. Supposons par l'absurde $\operatorname{Ker}(\cdot a)$ fini et prenons un élément k dedans. Alors n'importe quel λk reste dedans, en particulier la suite $(a^n k)_n$ ne saurait être injective, d'où deux entiers $p > q \geq 0$ tels que $a^p k = a^q k$. Multiplier à gauche p fois par un inverse à gauche g donne $k = g^{p-q} k$, d'où une contradiction si l'on trouvait un $k \in \operatorname{Ker}(\cdot a)$ non nul annulé par $g\cdot$; or l'élément $1 - ag$ tombe toujours dans $\operatorname{Ker}(\cdot a) \cap \operatorname{Ker}(g\cdot)$ et sa nullité contredirait l'hypothèse (on aurait sinon un inverse à gauche *et* à droite, d'où un *unique* inverse, empêchant la multiplicité des inverses à gauche).

Remarque. On peut se passer de $\operatorname{Ker}(\cdot a)$ en traduisant l'injection non surjective ci-dessus directement dans l'ensemble G des inverses à gauche : on conjugue pour cela par une bijection entre ces deux ensembles, *e. g.* par la translation selon un inverse à gauche g_0 fixé, ce qui donne

$$\begin{array}{ccccccc} G & \xrightarrow[-g_0]{\sim} & \operatorname{Ker}(\cdot a) & \xrightarrow[a\cdot]{} & \operatorname{Ker}(\cdot a) & \xrightarrow[+g_0]{\sim} & G \\ g & \longmapsto & g - g_0 & \longmapsto & ag - ag_0 & \longmapsto & ag - ag_0 + g_0 \end{array}\,.$$

On peut même remplacer ag_0 par 1, ce qui donne une injection « plus simple »

$$\left\{ \begin{array}{ccc} G & \hookrightarrow & G \\ g & \longmapsto & ag - 1 + g_0 \end{array} \right.\,.$$

Le second chemin peut aussi être directement pris en remarquant que $g + a^n (ag - 1)$ est dans G pour tout $g \in G$ et pour tout entier $n \geq 0$. Mais le remarquer en passant à côté de l'aspect linéaire évoqué à la première question nous semble être un défaut de compréhension (tout comme sortir de son chapeau l'application $g \mapsto ag - 1 + g_0$).

Rappelons qu'un ***pseudo-anneau*** est une structure vérifiant les axiomes d'un anneau à l'exception (possible) de l'exitence d'une unité. Les quatre prochains exercices leur sont consacrés.

[13] Claude Chevalley proposa en 1943 de baptiser ces anneaux en l'honneur de Mlle Emmy Noether.

9 Pseudo-anneaux finis

Soient dans un pseudo-anneau fini deux éléments γet δ réguliers respectivement à gauche et à droite. Montrer que A est unifère.

Que se passe-t-il sans l'hypothèse de finitude ?

Solution proposée.

Lorsque l'on cherche un certain élément – question pouvant souvent se traduire en terme de surjectivité –, la finitude doit susciter le réflexe suivant : les injections sont surjectives. Et dans notre cas les hypothèses de régularité nous donnent des injections : les homothéties $\gamma\cdot$ et $\cdot\delta$. Il ne reste plus qu'à travailler.

La composée $\gamma\cdot\delta$ reste injective, donc surjective, donc atteint $\gamma\delta$, mettons $\gamma e\delta = \gamma\delta$ (l'élément e va être notre 1), d'où en simplifiant respectivement par γ et δ les égalités $e\delta = \delta$ et $\gamma e = \gamma$. Ensuite, multiplier à gauche par un élément a donne $ae\delta = a\delta$, d'où en simplifiant par δ l'égalité $ae = a$; on montrerait de même l'égalité $ea = e$, ce qui conclut.

Le résultat tombe en défaut sans la finitude : le pseudo-anneau $2\mathbb{Z}$ est régulier mais n'a pas d'unité.

Remarque. Le lecteur pourra généraliser sans peine : *un pseudo-anneau est unifère ssi il y a deux éléments a et b tels que les homothéies $a\cdot$ et $\cdot b$ sont bijectives.* (Dans notre cas, les régularités impliquent des injectivités et la finitude transforme ces dernières en bijectivités).

10 Pseudo-anneaux commutatifs (ou pas)

1. *Rappeler pourquoi, dans un groupe, l'union de deux sous-groupes en est un ssi l'un des sous-groupes est inclus dans l'autre.*
2. *Soit A un pseudo-anneau où deux éléments quelconques commutent ou anti-commutent*[14]*. Montrer que A est commutatif ou anti-commutatif.*

Solution proposée.

1. Soit G et H deux sous-groupes dont la réunion est un sous-groupe. Supposons par exemple $G \not\subset H$ et montrons $H \subset G$. Puisque $G \not\subset H$, il y a un $g \in G \setminus H$. Alors, à $h \in H$ fixé, le produit gh doit rester dans le sous-groupe $G \cup H$: il ne peut appartenir à H (sinon $g \in Hh^{-1} \subset H$ puisque H est un sous-groupe), donc il doit rester dans G, d'où $h \in g^{-1}G \subset G$ puisque G est un sous-groupe, *CQFD.*
2. On veut montrer que le pseudo-anneau A coïncide avec son centre Z ou son « anti-centre[15] » Z'. En remarquant que Z et Z' sont des sous-groupes additifs de A, il suffit de montrer que leur réunion fait tout A : en effet, la réunion $Z \cup Z'$ serait alors un sous-groupe, donc $A = Z \cup Z'$ vaudrait l'un ou l'autre des sous-groupes Z ou Z', ce qu'il faut démontrer.

   Considérons par l'absurde un élément a hors de Z et Z' : il y a donc deux éléments b, c tels que $ba \neq ab$ et $ca \neq -ac$, ce qui force par hypothèse $\binom{ba}{ca} = \binom{-ab}{ac}$. En mélangeant les deux égalités obtenues séparément (on les additionne), on tombe sur $(b+c)\,a = a\,(c-b)$; or ce dernier vaut aussi par hypothèse $\pm\,(c-b)\,a$. Si le signe est un $+$, on obtient $ba + ca = ba - ca$, d'où $ca = -ca$; mais alors d'une part le membre de droite vaut $-ac$ car a et c commutent, d'autre part le membre de gauche diffère de $-ac$ car a et c n'anti-commutent pas, d'où la contradiction recherchée. (De la même manière, si le signe est un $-$, on obtiendrait $ab \neq ba = -ba = ab$.)

11 Pseudo-anneaux à division

On veut montrer qu'un pseudo-anneau où tout élément est divisible par tout autre élément non nul est ***à division***[16].

[14] $ba \in \{-ab, ab\}$ pour tous $a, b \in A$

[15] partie formée des éléments qui anti-commutent avec tous le monde

[16] tout élément non nul est inversible

1. *Soit A un pseudo-anneau non nul tel que $\forall a \neq 0$, $A = aA + Aa$.*
   Quels sont les idéaux bilatères de A ? Commenter.
   Montrer que le carré d'un élément non nul est non nul.
   Montrer que A est intègre[17].
2. *Soit A un pseudo-anneau intègre dont tous les éléments sont divisibles par un même élément $d \in A$ (peu importe le côté). Montrer que A est unifère.*
3. *Soit A un pseudo-anneau non nul où $\forall a \neq 0$, $A = aA \cup Aa$. Conclure $A^\times = A \setminus \{0\}$.*

Solution proposée.

1. Soit I un tel idéal. S'il contient un élément non nul i, on a $A = iA + Ai \subset I$, d'où $I = A$. Ainsi, les idéaux bilatères sont triviaux, comme dans un corps[18].

   Soit par l'absurde un élément a non nul de carré nul. Multiplier l'hypothèse (appliquée pour a) à gauche par a donne $aA = a^2A + aAa = aAa$, d'où en multipliant par a à droite la nullité de $aAa = aAa^2 = \{0\}$, de sorte que la première égalité devient $aA = \{0\}$. On montrerait de manière symétrique que $Aa = 0$, d'où la nullité de l'anneau $A = aA + Aa = \{0\}$, ce qui est contraire aux hypothèses.

   Supposons $ab = 0$ avec a ou b non nul ; puisque $(ba)^2 = b(ab)a = 0$, on a $ba = 0$, de sorte que a et b sont interchangeables. On peut donc supposer $a \neq 0$. Alors, en multipliant l'hypothèse (appliquée pour a) à gauche et à droite par b donne la nullité de $bAb = baAb + bAab = 0$. En particulier, le carré $bb^2b = \left(b^2\right)^2$ est nul, donc b^2 aussi, d'où $b = 0$, *CQFD.*

2. Observer que le « pgcd » d est non nul, sinon A serait nul (tous ses éléments sont mutiples de d) et donc non intègre.

   Écrivons d comme multiple de lui-même, mettons $d = de$ (l'élément e va être notre 1). En multipliant à droite par un élément $a \in A$ fixé, on trouve $da = dea$, d'où en simplifiant par $d \neq 0$ l'égalité $a = ea$; multiplier à gauche par a donne $aa = aea$, d'où en simplifiant à droite (pour $a \neq 0$) l'égalité $a = ae$. Comme annoncé[19], notre e est bien un 1.

3. La question 1 montre que A est intègre. Alors, considérant un élément d non nul (il en existe), la question 2 montre que A est unifère. Enfin, divisons 1 par un élément non nul a, mettons $1 = ab$: multiplier par b à gauche donne $b = bab$, d'où en simplifiant à droite l'égalté $1 = ba$. Nous avons montré que tout élément non nul est inversible, *CQFD.*

12 Comment transformer un pseudo-anneau en un anneau

Soit A un pseudo-anneau. On veut construire un anneau *unifère* contenant A (comme sous-anneau) et qui soit le *plus petit* possible (ce afin d'espérer une unicité).

Pour préciser ce « plus petit possible », on identifie les anneaux X contenant de A aux morphismes injectifs $A \overset{i_X}{\hookrightarrow} X$, que l'on pensera volontiers comme des inclusions, et l'on pré-ordonne ces « sur-anneaux » par

$$\text{« } i_X \leq i_Y \text{ si } \quad \begin{array}{c}\text{il y a un morphisme } X \xrightarrow{f} Y \\ \text{faisant commuter le diagramme}^{20}\end{array} \quad \begin{array}{ccccc} X & \longrightarrow & \xrightarrow{f} & \longrightarrow & Y \\ & \nwarrow^{i_X} & \circlearrowright & \nearrow_{i_Y} & \\ & & A & & \end{array} \text{ ».}$$

1. **Analyse.** *Montrer qu'un tel anneau est (isomorphe à) un quotient de $\mathbb{Z} \times A$.*
2. **Construction.** *Munir le groupe additif $\mathbb{Z} \times A$ d'un produit qui en fait un anneau contenant $\mathbb{Z}$ et A (pour les deux inclusions canoniques $\mathbb{Z}, A \hookrightarrow \mathbb{Z} \times A$).*
   On note $A_\bigstar$ l'anneau ainsi défini et i_A l'inclusion canonique $A \hookrightarrow A_\bigstar$.

[17] On n'ergotera pas pour savoir si la commutativité ou l'unitarité font ou non partie de la définition de l'intégrité. Pour nous, **intègre** signifie *non nul* et *sans diviseurs de zéro.*
[18] c'était le commentaire
[19] le cas $a = 0$ est trivial
[20] la flèche $\circlearrowright$ centrale indique la commutativité du diagramme

3. **Unicité faible.** *Montrer que $A_\bigstar$ est un*[21] *plus petit sur-anneau contenant A pour le pré-ordre défini ci-dessus.*

   On aimerait bien montrer l'unicité de $A_\bigstar$ à isomorphisme près. On vient de montrer que deux plus petits sur-anneaux sont chacun plus petit et plus grand que l'autre. *Montrer que cette condition ne suffit pas en général pour conclure qu'ils sont isomorphes.* (On pourra multipler $A_\bigstar$ par un anneau assez gros.)

   Nous allons par conséquent travailler un peu plus.

4. **Unitarisation des flèches.** *Montrer que tout morphisme $f : A \longrightarrow B$ de pseudo-anneaux induit un unique morphisme $f_\bigstar : A_\bigstar \longrightarrow B_\bigstar$ d'anneaux faisant commuter le diagramme*

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow i_A & & \downarrow i_B \\ A_\bigstar & \xrightarrow{f_\bigstar} & B_\bigstar \end{array} . \qquad \textit{Que vaut } \left(\underset{A}{\mathrm{Id}}\right)_\bigstar \ ?$$

5. **Fonctorialité.** *Vérifier que*[22] $(g \circ f)_\bigstar = g_\bigstar \circ f_\bigstar$ *pour tous morphismes $A \xrightarrow{f} B \xrightarrow{g} C$ de pseudo-anneaux.*

6. **Unicité forte.** *En déduire que, si A_* est un autre plus petit sur-anneau de A, alors il y a un* unique *isomorphisme $A_* \cong A_\bigstar$ commutant aux deux inclusions $A \hookrightarrow A_*, A_\bigstar$.*

7. *Que devient notre problème si l'on retire l'injectivité dans le pré-ordre défini en introduction ?*

Solution proposée.

1. Un anneau unifère contenant A contient aussi l'anneau $\mathbb{Z}1$ engendré par son unité, donc contient la somme $A + \mathbb{Z}1$, laquelle est bien un anneau répondant au problème. Ainsi, si $A_\bigstar$ répond au problème ; on a une surjection évidente $\left\{ \begin{array}{ccc} \mathbb{Z} \times A & \twoheadrightarrow & A_\bigstar \\ (k, a) & \longmapsto & k + a \end{array} \right.$ qui est un morphisme de pseudo-anneaux, donc son image $A_\bigstar$ est isomorphe à son espace de départ quotienté par son noyau, ce qui conclut.

2. Pour intuiter le produit, plaçons-nous dans le cas agréable où la surjection ci-dessus est une bijection. Puisque le produit dans $A_\bigstar$ est donné par $(k + a)(l + b) = \underline{kl} + \underline{kb + la + ab}$ (avec k, l entiers et $a, b \in A$), on doit avoir $\binom{k}{a}\binom{l}{b} = \binom{kl}{ab+kb+la}$.

   Essayons de montrer que le produit ainsi défini munit bien le groupe additif $\mathbb{Z} \times A$ d'une structure d'anneau contenant $\mathbb{Z}$ et A. Les inclusions sont claires vu les identités $\binom{k}{0}\binom{l}{0} = \binom{kl}{0}$ et $\binom{0}{a}\binom{0}{b} = \binom{0}{ab}$. Il reste à montrer l'associativité du produit ainsi que sa distributivité sur l'addition (dans les deux sens), ce qui est pédestre et laissé au soin du lecteur[23], ainsi bien sûr que le caractère neutre de $\binom{1}{0}$.

3. Soit $i : A \hookrightarrow A_*$ un sur-anneau contenant A. Cherchons un morphisme $\varphi : A_\bigstar \longrightarrow A_*$ qui commute aux inclusions i_A et i. Puisque φ préserve l'unité, on doit avoir pour tout k entier $\varphi\binom{k}{0_A} = k$. De plus, puisque φ commute à i_A et i, on doit avoir pour tout $a \in A$

$$\varphi\binom{0}{a} = [\varphi \circ i_A](a) = i(a) .$$

   Finalement, φ étant additif, il est entièrement décrit par

$$\varphi\binom{k}{a} = \varphi\binom{k}{0} + \varphi\binom{0}{a} = k + i(a) .$$

   On vérifie facilement que le φ ainsi défini est un morphisme d'anneaux :

$$\begin{aligned} \varphi\left(\binom{k}{a}\binom{l}{b}\right) &= \varphi\binom{kl}{ab + kb + la} = kl + i(ab + kb + la) \\ &= kl + i(a)\, i(b) + ki(b) + li(a) \\ &= (k + i(a))(l + i(b)) = \varphi\binom{k}{a}\varphi\binom{l}{b}. \end{aligned}$$

[21] Par un « plus petit » on entend quelqu'un de « plus petit que tout le monde ». (On dit « un » et pas « le » car on n'a unicité d'un minimum que dans un *vrai* ordre : dans un *pré*ordre, on obtient unicité modulo la relation « être plus petit et plus grand que ».)

[22] On dit que la correspondance $A \mapsto A_\bigstar$ est un ***foncteur*** de la ***catégorie*** des pseudo-anneaux vers celle des anneaux. Vu la formule demandée, on peut voir un foncteur comme un morphisme de morphismes.

[23] Il doit obtenir ce qu'il aurait obtenu en développant un produit de la forme $(k + a)(l + b)(m + c)$ (pour l'associativité) ou $(k + a)[(l + b) + (m + c)]$ (pour la distributivité à droite).

Il est par ailleurs immédiat qu'il commute avec i et i_A (calcul déjà fait lors de l'analyse).

Considérons comme indiqué le sur-anneau produit $A_\bigstar \times B$ (où B est un anneau à choisir judicieusement) dans lequel A se plonge via les injections canoniques $A \overset{i_A}{\hookrightarrow} A_\bigstar \hookrightarrow A_\bigstar \times B$. Si ce sur-anneau était isomorphe à $A_\bigstar$, on pourrait surjecter l'ensemble $A_\bigstar$ sur B, ce qui est impossible pour $B = \mathfrak{P}(A_\bigstar)$ d'après un résultat connu de Cantor[24]. Pourtant, on a deux morphismes évidents $\left\{ \begin{array}{ccc} A_\bigstar \times B & \longrightarrow & A_\bigstar \\ (x,b) & \longmapsto & x \end{array} \right.$ et $\left\{ \begin{array}{ccc} A_\bigstar & \longrightarrow & A_\bigstar \times B \\ x & \longmapsto & (x,0) \end{array} \right.$ qui commutent aux deux injections.

4. Soit $f_\bigstar$ convenant. Comme à la question précédente, on doit avoir pour tout k entier $f_\bigstar \binom{k}{0_A} = \binom{k}{0_B}$ et pour tout $a \in A$

$$f_\bigstar \binom{0}{a} = [f_\bigstar \circ i_A](a) = [i_B \circ f](a) = \binom{0}{f(a)},$$

de sorte que $f_\bigstar$ envoie[25] $\binom{k}{a}$ sur $\binom{k}{f(a)}$.

On vérifie aisément que $f_\bigstar := \mathrm{Id}_\mathbb{Z} \times f$ répond au problème : c'est un morphisme d'anneaux comme produit de morphismes d'anneaux et les calculs ci-dessus montrent qu'il commute bien avec i_A et i_B.

5. Étant donnés deux morphismes $A \overset{f}{\longrightarrow} B \overset{g}{\longrightarrow} C$ de pseudo-anneaux, il suffit pour montrer la formule demandée de vérifier (d'après l'unicité) que la composée $g_\bigstar \circ f_\bigstar$ est un morphisme d'anneaux (c'est clair) commutant aux inclusions i_A et i_C, ce qui peut se voir en suivant les flèches dans le diagramme « élargi » avec i_B :

$$\begin{array}{ccccc} A & \overset{f}{\longrightarrow} & B & \overset{g}{\longrightarrow} & C \\ \downarrow i_A & \circlearrowleft & \downarrow i_B & \circlearrowleft & \downarrow i_C \\ A_\bigstar & \overset{f_\bigstar}{\longrightarrow} & B_\bigstar & \overset{g_\bigstar}{\longrightarrow} & C_\bigstar \end{array}$$. On y lit $\begin{array}{l} (g_\bigstar \circ f_\bigstar) \circ i_A = g_\bigstar \circ (f_\bigstar \circ i_A) \\ = g_\bigstar \circ (i_B \circ f) = (g_\bigstar \circ i_B) \circ f \\ = (i_C \circ g) \circ f = i_C \circ (g \circ f) \end{array}$, *CQFD.*

6. Notons pour abréger i et j les inclusions $A \hookrightarrow A_\bigstar$ et $A \hookrightarrow A_*$ et donnons-nous deux isomorphismes $A_\bigstar \overset{\varphi,\ \psi}{\longrightarrow} A_*$ commutant à i et j. En dédoublant le A grâce à l'identité $A \overset{\mathrm{Id}}{\longrightarrow} A$, la commutativité se lit sur les carrés

$$\begin{array}{ccc} A & \overset{\mathrm{Id}}{\longrightarrow} & A \\ \downarrow i & \circlearrowleft & \downarrow j \\ A_\bigstar & \overset{\varphi}{\longrightarrow} & A_* \end{array} \quad \text{et} \quad \begin{array}{ccc} A & \overset{\mathrm{Id}}{\longrightarrow} & A \\ \downarrow j & \circlearrowleft & \downarrow i \\ A_* & \overset{\psi^{-1}}{\longrightarrow} & A_\bigstar \end{array} , \quad \text{lesquels peuvent se concaténer en} \quad \begin{array}{ccccc} A & \overset{\mathrm{Id}}{\longrightarrow} & A & \overset{\mathrm{Id}}{\longrightarrow} & A \\ \downarrow i & \circlearrowleft & \downarrow j & & \downarrow i \\ A_\bigstar & \overset{\varphi}{\longrightarrow} & A_* & \overset{\psi^{-1}}{\longrightarrow} & A_\bigstar \end{array} .$$

Ce dernier diagramme rectangulaire est commutatif (même calcul qu'à la question précédente), donc la composée $\psi^{-1} \circ \varphi$ vaut (par unicité de $f_\bigstar$) l'étoile-en-bas de $\mathrm{Id} \circ \mathrm{Id} = \mathrm{Id}$, ce qui s'écrit $\psi^{-1} \circ \varphi = [\mathrm{Id}]_\bigstar = \mathrm{Id}$, d'où $\varphi = \psi$ en composant à gauche par ψ.

Nous avons donc prouvé l'unicité d'un isomorphisme entre $A_\bigstar$ et A_* qui commute à i et j. Montrons à présent l'existence.

Puisque $A_\bigstar$ est un plus petit anneau contenant A et que A_* en est un, on a une inclusion $A_\bigstar \overset{I}{\hookrightarrow} A_*$ qui commute avec i et j ; par un agument symétrique, on dispose également d'une inclusion $A_* \overset{J}{\hookrightarrow} A_\bigstar$ commutant à i et j. Montrons que I et J sont inverses l'une de l'autre. Il suffit pour cela de montrer comme ci-dessus que $J \circ I$ est l'étoile-en-bas de Id, ce qui se lit (comme ci-dessus) sur le diagramme commutatif

$$\begin{array}{ccccc} A & \overset{\mathrm{Id}}{\longrightarrow} & A & \overset{\mathrm{Id}}{\longrightarrow} & A \\ \downarrow i & \circlearrowleft & \downarrow j & & \downarrow i \\ A_\bigstar & \overset{I}{\longrightarrow} & A_* & \overset{J}{\longrightarrow} & A_\bigstar \end{array} \qquad \begin{array}{c} \text{(idem pour } I \circ J \\ \text{en échangeant} \\ \text{les rôles de } i \text{ et } j\text{).} \end{array}$$

7. Sans l'injectivité, il est facile d'envoyer n'importe quel pseudo-anneau vers un anneau unitaire : prendre le morphisme nul vers l'anneau nul, lequel est clairement unique à unique isomorphisme près.

Remarque caractéristique. Si l'on souhaite prendre en compte la « caractéristique » du pseudo-anneau A, au sens où l'on aurait la nullité de $cA = 0$ pour un entier $c \geq 0$, on peut remplacer l'anneau $\mathbb{Z}$ par $\mathbb{Z}/c$ et reprendre les questions une par une. On obtiendra l'unicité (à unique isomorphisme près faisant

[24] aucun ensemble ne se surjecte sur l'ensemble de ses parties – *cf.* feuille *Ensembles et applications*

[25] en d'autre termes, $f_\bigstar = \mathrm{Id}_\mathbb{Z} \times f$

commuter le diagramme adéquat) d'un anneau $A_\bigstar := {}^{\mathbb{Z}}\!/_{c} \times A$ contenant A et de caractéristique c imposée. (Il faut juste faire un peu plus attention pour vérifier que $A_\bigstar$ est un anneau et pour définir des morphismes entre les ${}^{\mathbb{Z}}\!/_{c}$.)

Remarque catégorielle. Le lecteur pourrait se sentir perdu au milieu de tous ces diagrammes de flèches. Peut-être plus tard, lorsqu'il reverra ce genre de problème de complétion et d'autres plus généraux[26], verra-t-il se dessiner la même trame de raisonnement et se répéter les mêmes arguments. Peut-être alors appréciera-t-il d'avoir été initié sur le terrain familier des anneaux.

Nous parlons à présent des ***idempotents*** (éléments dont toutes les puissances ≥ 1 sont égales) et de leur lien avec les « briques de base » d'un anneau.

13 Idempotents et factorisations d'anneaux

Le cadre est celui d'un anneau commutatif appelé A.

1. *Montrer qu'un idéal est un anneau pour les lois induites ssi il est engendré par un idempotent.*
2. *Montrer que l'application « complémenter à 1 » est une involution sans point fixe des idempotents de A (modulo un cas pathologique à préciser).*
3. *Soient i et j deux idempotents de somme 1. Montrer que A est isomorphe à l'anneau produit $iA \times jA$.*
   On dit qu'une famille (a_i) d'éléments de A est ***orthogonale*** si les produits $a_x a_y$ pour $x \neq y$ sont tous nuls.
4. *Soient i_x des idempotents orthogonaux en nombre fini. Montrer que la somme des i_x est idempotente. En déduire un idempotent orthogonal à tous les i_x.*
5. *Soient $i_1, ..., i_n$ des idempotents orthogonaux en nombre maximal. Montrer que A est isomorphe au produit $\prod_{x=1}^{n} i_x A$.*

Solution proposée.

1. Soit i un idempotent. L'idéal (i) est un sous-groupe additif (c'est immédiat) stable par produit (grâce à l'idempotence de i) et possède i pour neutre (pour la même raison). Attention à dire que ce n'est pas un sous-anneau de l'anneau de départ car ils n'ont pas la même unité[27].

   Soit réciproquement I un idéal qui soit un anneau. Notons i son unité et montrons (comme suggéré par ce qui précède) que $I = (i)$. D'une part l'idéal $(i) = iA$ est inclus dans I (car I est stable par $i\cdot$), d'autre part tout élément $x \in I$ vaut son produit par l'unité i, d'où l'inclusion réciproque $I \subset iA$.
2. Soit i idempotent. L'idempotence de $1 - i$ est immédiate :
$$(1-i)^2 = 1^2 - 2i + i^2 = 1 - 2i + i = 1 - i.$$
   Si i et $1 - i$ devaient coïncider, multiplier par i donnerait $i^2 = i(1-i) = 0$, donc $i = i^2$ serait nul et l'on aurait $1 - i = 1 \overset{?}{\neq} 0 = i$, ce qui est une contradiction dans un anneau non nul[28].
3. Comment envoyer A sur $iA \times jA$? Il est facile d'envoyer A sur iA (prendre l'homothétie de rapport i), donc il est naturel d'essayer le produit $\pi : a \mapsto (ia, ja)$ des homothéties de rapport i et j. C'est clairement un morphisme d'anneaux (grâce aux idempotences de i et j). Montrons qu'il est bijectif : si a est un antécédent d'un $(ix, iy) \in iA \times jA$, alors sommer les coordonnées de $(ia, ja) = \pi(a) = (ix, jy)$ donne $a = ix + jy$, ce qui d'une part montre l'injectivité de π et d'autre part donne l'antécédent de tout élément de $iA \times jA$ (c'est immédiat à vérifier une fois observée la nullité du produit $ij = i(1-i) = i - i^2$).

[26] Le terme consacré est celui de ***problème universel***. On renvoit le lecteur très motivé (*i. e.* dont les catégories suscitent la curiosité) à l'ouvrage de Régine et Adrien Douady *Algèbre et théories galoisiennes*.

[27] à moins bien sûr que $i = 1$

[28] Dans l'anneau nul $\{0\}$, l'unique élément est idempotent et fixe par toute les applications de $\{0\}$ dans $\{0\}$.

4. Le calcul est immédiat (dans le carré de la somme, les termes croisés disparaissent par orthogonalité) :

$$\left(\sum_x i_x\right)^2 = \sum_x i_x^2 + \sum_{x\neq y} i_x i_y = \sum_x i_x + 0.$$

Étant donné un seul idempotent i, la question 2 nous suggère $1-i$. Avec plusieurs idempotents i_x orthogonaux, l'analogue serait $1-\sum i_x$. C'est bien un idempotent en tant que complément à 1 de l'idempotent $\sum i_x$. Montrons qu'il est orthogonal à tous les i_x : cela résulte de l'égalité $i_\xi \sum_x i_x = \sum_x \delta_x^\xi i_x = i_\xi$ pour tout ξ.

5. Tentons le même raisonnement qu'à la question 3. Il est déjà clair que le produit des homothéties de rapport i_x est un morphisme d'anneaux surjectif (grâce à l'orthogonalités des i_x). Son injectivité viendrait de ce que la somme des i_x fasse 1 (même argument : un élément $a \in A$ vaut la somme des coordonnées de son image). Il s'agit donc de montrer que la différence $\delta := 1 - \sum i_x$ est nulle. D'après la question précédente, δ est un idempotent orthogonal à tous les i_x, donc par maximalté doit valoir l'un d'eux, disons $\delta = i_\xi$; mais alors δi_ξ est nul par orthogonalité et vaut i_ξ par idempotence, d'où $0 = \delta = i_\xi$, *CQFD.*

14 Autour de l'indécomposabilité

Le cadre est toujours celui d'un anneau commutatif A.

On dit qu'un anneau est ***décomposable*** s'il est isomorphe au produit de deux anneaux non nuls, ***indécomposable***[29] sinon.

1. *Montrer que A est indécomposable ssi ses seuls idempotents sont trivaux (0 et 1). Exemples ?*
2. *On suppose A indécomposable et on se donne un entier $n \geq 1$. Montrer que les seuls morphismes de l'anneau produit A^n vers A sont les projections canoniques « coordonnées ». Contre-exemple sans l'indécompsabilité ?*
3. *On suppose que A est un produit $\prod_i A_i$ d'indécomposables. Montrer qu'un morphisme $A^n \to A$ est un produit (indexé par i) de projections canoniques $A_i^n \longrightarrow A_i$.*
4. *On suppose que A est* ***artinien***[30], i. e. *que toute famille d'idéaux admet un élément minimal. Montrer que A est produit fini d'indécomposables.*
5. *L'anneau A est-il toujours un produit d'indécomposables ?* (On pourra dénombrer les idempotents.)

Solution proposée.

1. Si on peut « casser » $A \simeq B \times C$ avec B et C non nuls (*i. e.* $1 \neq 0$ dans chacun), alors les éléments $(1,0)$ et $(0,1)$ sont des idempotents non trivaux. Observer alors les isomorphismes $B \simeq (1,0)\,A$ et $C \simeq (0,1)\,A$.

   Réciproquement, si i est un idempotent non trivial, alors la synthèse suggère de considérer l'idempotent $j := 1-i$ (il est non trivial sinon i serait trivial) ainsi qu'un éventuel isomorphisme $A \overset{?}{\simeq} iA \times jA$ (les deux facteurs sont non nuls car contiennent chacun d'une part 0 et d'autre part i ou j) ; or la question 3 de l'exercice précédent nous donne une telle factorisation, ce qui conclut.

   Vu qu'un idempotent i est caractérisé par la relation $i^2 = i$, tout anneau *intègre* est indécomposable, par exemple $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}[X]$. Par ailleurs, tout produit $A \times B$ admet deux idéaux maximaux distincts $\mathfrak{m}_A \times B$ et $A \times \mathfrak{m}_B$ (où $\mathfrak{m}_R$ est un idéal maximal de l'anneau non nul R), donc ne peut être local[31] : par contraposée, tout anneau *local* est indécomposable.
2. Notons f_i les images des « vecteurs » e_i de la base canonique de A^n. L'idempotence étant conservée par les morphismes, les f_i sont des idempotentss. Puisque leur somme est l'image de $\sum e_i = 1$, on a un isomorphisme $A \cong \prod f_i A$, donc pour tout i l'un des anneaux $f_i A$ ou $\prod_{j\neq i} f_j A$ est nul, ce qui montre qu'il n'y au plus qu'un f_j non nul, l'égalité $\sum f_j = 1$ assurant qu'il y en a exactement 1, mettons $f_k = 1$ (idempotent non nul). Alors f est la projection sur la k-ième coordonnée.

[29] Cela revient à dire que toute factorisation (isomorphisme) $A \simeq A_1 \times \cdots \times A_n$ est triviale, au sens où les A_i sont alors tous nuls sauf un qui vaut A (à isomorphisme près).

[30] La définition équivaut à ce que toute suite décroissante d'idéaux stationne, à rapprocher de la définition des anneaux noethériens. Il est d'ailleurs remarquable qu'un anneau artinien soit toujours noethérien – *cf.* feuille *Algèbre commutative* pour une démonstration.

[31] Un anneau commutatif est dit ***local*** lorsqu'il admet un unique idéal maximal. Le quotient par cet idéal est alors appelé ***corps résiduel***.

Pour trouver un contre-exemple, partons d'un anneau $A = B \times C$ décomposable. Un morphisme $A^2 \longrightarrow A$ est donc un morphisme $B \times C \times B \times C \longrightarrow B \times C$. Pour éviter de tomber sur une projection canonique, on peut « mélanger » les coordonnées en considérant l'un ou l'autre des morphismes $\begin{cases} A^2 & \longrightarrow & A \\ (b,c,b',c') & \longmapsto & (b,c') \text{ ou } (b',c) \end{cases}$.

La question suivante montre que ce type de contre-exemple est le plus général possible (dans les anneaux produits d'indécomposables).

3. On raisonne de même. Un morphisme $A^n \longrightarrow A$ n'est autre qu'un produit de morphismes de A_i^n (identifié au sous-anneau $A_i^n \times \prod_{j \neq i} \{0\}$) vers A_i avec i variant, or l'on vient de voir que chacun de ces morphismes est une projection.

4. Une idée simple est la suivante : si A est indécomposable, on a terminé, sinon on peut écrire $A \simeq B \times C$ et on se pose la même question concernant les idéaux-anneaux B et C. Il nous faut une hypothèse de finitude pour garantir la terminaison de notre algorithme : c'est l'hypothèse de l'énoncé.

   Plus présisément, cette dernière permet d'effectuer une ***induction noethérienne***[32] : si une propriété portant sur les idéaux est vraie pour un idéal donné dès qu'elle est vérifiée pour les idéaux strictement plus petits, alors on obtient une contradiction en considérant par l'absurde un idéal minimal ne vérifiant pas cette propriété.

   Montrons par induction noethérienne que tout idéal-anneau est produit fini de décomposables (alors l'anneau-idéal $A = (1)$ le sera, ce qu'il faut démontrer). Soit eA un idéal-anneau dont tous les sous-idéaux-anneaux iA stricts soient produits finis d'indécomposables. Alors ou bien l'anneau eA est indécomposable, ou bien il se décompose en $eA \simeq iA \times jA$: alors les idéaux-anneaux iA et jA sont non nuls, donc forment des idéal-anneaux stricts de $iA \times jA \simeq eA$ et sont décomposables par induction en produits finis d'indécomposables, d'où la même conclusion pour leur produit eA, *CQFD*.

5. Regardons les idempotents d'un produit d'incomposables $\prod_{i \in I} A_i$: il s'agit des familles (a_i) telles que $\left(a_i^2\right) = (a_i)$, *i. e.* des familles d'idempotents, à savoir (par indécomposabilité des A_i) des familles de 0 ou de 1, lesquelles sont clairement en bijection avec $\mathfrak{P}(I)$ (à une famille d'idempotents associer la partie de I indexant les 1).

   Les idempotents de $\prod_{i \in I} A_i$ ne sauraient donc être dénombrables : si I est fini, alors $\mathfrak{P}(I)$ est trop petit ; si I est infini, alors I contient une partie dénombrable, donc $\mathfrak{P}(I)$ contient $\mathfrak{P}(\mathbb{N})$ qui est trop gros.

   On pourra donc répondre au problème par la négative si l'on exhibe un anneau ayant un nombre dénombrable d'idempotents. Or le même raisonnement que ci-dessus montre qu'une *somme directe* d'indécomposables $\bigoplus_{i \in I} A_i$ a autant d'idempotents que de parties *finies*[33] de I, à savoir autant que d'éléments de $\max(\mathbb{N}, I)$. Ainsi, le sous-anneau $\mathbb{Z}^{(\mathbb{N})}$ du produit $\mathbb{Z}^{\mathbb{N}}$ a un nombre dénombrable d'idempotents, donc ne saurait être produit d'indécomposables.

Les quatre derniers exercices sont consacrés au théorème de Jacobson. On commence par deux cas particuliers, (presque) englobés par le troisième exercice, lequel est à son tour généralisé dans le dernier exercice.

15 Les anneaux de Boole sont commutatifs

Un anneau ***booléen*** est un anneau dont tout élément est idempotent.
Montrer qu'un anneau booléen est commutatif.

Solution proposée.
Remarquons déjà que l'idempotence de 2 entraîne sa nullité (écrire $2 = 2^2 - 2$). Ensuite, étant donnés deux éléments a et b, on peut faire apparaître le défaut de commutativité $[a,b] := ab - ba \overset{2=0}{=} ab + ba$ dans le carré $(a+b)^2$, ce qui donne

$$[a,b] = (a+b)^2 - a^2 - b^2 = (a+b) - a - b = 0, \ CQFD.$$

[32] Un ordre est ***noethérien*** si toute partie non vide admet un élément minimal. Par exemple, $\mathbb{N}^*$ est noethérien pour la divisibilité, ce qui permet de montrer par induction que tout entier non nul est produit de premiers (par ± 1).

[33] Déjà, les parties finies de I contiennent celles de cardinal 1 qui sont équipotentes à I. Ensuite, celles de cardinal fixé $n \in \mathbb{N}$ s'injectent dans I^n qui est équipotent à I lorsque ce dernier est infini, donc les parties finies de I s'injectent dans la réunion dénombrable des I^n, laquelle s'injecte dans la réunion disjointe $\bigsqcup_{n \in \mathbb{N}} I = I \times \mathbb{N}$ et ce dernier produit est équipotent à I pour I infini.

Remarque. On renvoit au DM sur les anneaux de Boole pour plus de détails sur leur classification et leur liens avec les algèbres de Boole.

16 Les anneaux où $a^3 = a$ pour tout a sont commutatifs

Soit A un anneau où $a^3 = a$ pour tout $a \in A$. On veut montrer que A est commutatif.

Première démonstration.

1. *Montrer que l'homothétie de rapport* 6 *est nulle puis expliciter un isomophisme d'anneaux* $A \simeq 2A \times 3A$.
2. *Montrer que l'on supposer* A *de caractéristique* 2 *ou* 3.
3. *Conclure.* (On pourra utliser les nullités éventuelles des quantités $s^2 + s$ et $ab^2 + bab + b^2a$.)

Deuxième démonstration.

1. *Montrer que les idempotents de* A *sont centraux et en déduire que les carrés de* A *sont centraux.* (On pourra regarder les produits iaj pour i et j idempotents duaux et a élément quelconque.)
2. *Montrer que* $2a$ *et* $3a$ *sont centraux et conclure.*

Première solution proposée.

1. L'hypothèse appliquée à 2 donne $8 = 2^3 = 2$, d'où $6 = 0$, *CQFD.*

   En écrivant $a = 3a - 2a$, on voit que $A = 3A + 2A$. La décomposition est de plus unique vu l'implication $2a = 3b \overset{\times 3}{\Longrightarrow} 0 = 9b = 3b$. On peut donc écrire $A = 3A \oplus 2A$, ce qui induit une bijection $\begin{cases} A & \xrightarrow{\sim} & 3A \times 2A \\ a & \longmapsto & (3a, -2a) \\ 3x - 2y & \longleftarrow & (3x, 2y) \end{cases}$ qui a le bon goût d'être un isomorphisme d'anneaux (pour les lois induites, les neutres de $3A$ et $2A$ étant respectivement 3 et 2).

   Remarque. On aurait pu utiliser un exercice précédent : les éléments 2 et 3 étant des idempotents non triviaux, l'anneau A est décomposable selon $2A \times 3A$.
2. Les anneaux $2A$ et $3A$ vérifiant la même propriété que A. Si l'on montre qu'ils sont commutatifs, l'anneau produit $2A \times 3A \simeq A$ le sera. Il suffit donc de se restreindre à $3A$ (où $2 = 0$) et à $2A$ (où $3 = 0$).
3. Les deux identités vont s'obtenir en faisant apparaître des cubes (afin d'utiliser l'hypothèse) ainsi que des doubles/triples selon la caractéristique.

   Lorsque $2 = 0$, on écrit $0 = (s+1)^3 - (s+1) = 3s^2 + 3s = s^2 + s$, d'où en substituant une somme $a + b$ à s

   $$0 = (a+b) + (a+b)^2 = 0 + ab + ba + 0, \text{ ce qui conclut } ab = -ba \overset{2=0}{=} ba.$$
4. Lorsque $3 = 0$, on écrit

   $$2a = (a+b)^3 + (a-b)^3 = 2a + 2ab^2 + 2bab + 2b^2a,$$

   d'où la nullité de $ab^2 + bab + b^2a$ en simplifiant par 2 (qui est involutif donc inversible). En multipliant cette dernière par b d'une part à droite d'autre part à gauche, on obtient

   $$ab + \underline{bab^2 + b^2ab} = 0 = \underline{bab^2 + b^2ab} + ba, \text{ d'où le résultat après simplification.}$$

Seconde solution proposée.

1. Soit i idempotent et $a \in A$. On a donc $i(1-i) = 0 = (1-i)i$, d'où $[ia(1-i)]^2 = 0$. Par hypothèse, on a

   $$ia(1-i) = [ia(1-i)]^3 = 0,$$

   d'où $ia = iai$. On montrerait de même que le produit $(1-i)ai$ est nul, d'où $ai = iai = ia$, *CQFD.*

   Il suffit de montrer qu'un carré est idempotent, ce qui immédiat :

   $$\left(a^2\right)^2 = a^4 = a^3a = a^2.$$

2. Décomposer $a = 3a - 2a$ permettra de conclure.

Or, d'une part $2a = (a+1)^2 - a^2 - 1$ est central comme somme de carrés (centraux), d'autre part $a+1 = (a+1)^3 = a^3+3a^2+3a+1$ montre que $3a = -3a^2$ est central (comme multiple entier d'un carré).

Remarque. Contrairement à la première solution qui utilise vraiment les particularités de 2 et 3, la seconde solution se généralise (en partie) quand on remplaçe l'exposant 3 par un entier quelconque (*cf.* deux premières questions du dernier exercice – difficile).

17 Sur un théorème de Jacobson 1

Soit A un anneau de caractéristique $p > 0$ tel que $\forall a \in A,\ a^p = a$.
On veut montrer que A est commutatif.
(la solution proposée nécessite de connaître les systèmes linéaires.).

1. *On fixe deux éléments a et b dans A et on leur associe le polynôme $(a+\lambda b)^p - a^p - (\lambda b)^p$ en la variable λ (commutative). Montrer que son coeffcient de degré 1 en b est nul.* (On pourra chercher un système linéaire satisfait par ses coefficients.)
2. *En déduire que a^p est central et conclure.*

Solution proposée.

1. Puisque l'indéterminée λ commute avec tout le monde, on peut bien parler des coefficients $S(k)$ du polynôme
$$P(\lambda) := (a+\lambda b)^p - a^p - (\lambda b)^p = \lambda S(1) + \lambda^2 S(2) + ... + \lambda^{p-1} S(p-1)$$
(les termes constant et de degré p sont annulés). Faisant varier λ dans le sous-corps premier de notre anneau (qui est central puisqu'il est formés des itérés de l'unité), on obtient un système linéaire en les $p-1$ éléments $S(k)$. Or ce sous-corps est $\mathbb{F}_p$ puisque notre anneau est de caractéristique p, d'où en se restreignant à $\mathbb{F}_p^*$ un système de Vandermonde
$$\begin{pmatrix} 1 & 1^2 & 1^3 & \cdots & 1^{p-1} \\ 2 & 2^2 & 2^3 & \cdots & 2^{p-1} \\ 3 & 3^2 & 3^3 & \cdots & 3^{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p-1 & (p-1)^2 & (p-1)^3 & \vdots & (p-1)^{p-1} \end{pmatrix} \begin{pmatrix} S(1) \\ S(2) \\ S(3) \\ \vdots \\ S(p-1) \end{pmatrix} = \begin{pmatrix} P(1) \\ P(2) \\ P(3) \\ \vdots \\ P(p-1) \end{pmatrix}.$$
Le calcul son déterminant est classique :
$$\det\left(i^j\right)_{1\le i,j<p} \overset{\substack{\text{factoriser dans} \\ \text{chaque ligne}}}{=} \left(\prod_{1\le i<p} i\right) \det\left(i^{j-1}\right)_{1\le i,j<p} \overset{\substack{\text{déterminant de} \\ \text{Vandermonde}}}{=} (p-1)! \prod_{1\le i<j<p} (j-i).$$
Tous les entiers apparaissant étant non nuls dans le corps $\mathbb{F}_p$, leur produit est non nul, donc le système est inversible ; or tous les $P(k)$ sont nuls vu l'hypothèse, d'où l'on déduit en particulier la nullité de $S(1)$, *CQFD.*
2. On peut expliciter $S(1) = \sum_{u+v=p-1}^{u,v\ge 0} a^u b a^v$. Pour relier $S(1)$ à a^p, on peut observer que le crochet $[a, S(1)]$ vaut par télescopage celui $[a^p, b]$. Puisque $S(1)$ est nul et que $a^p = a$, on en déduit $[a,b] = 0$; ceci tenant pour tout $b \in A$, l'élément a est central, ce qui conclut.

18 Sur un théorème de Jacobson 2

Soit A un anneau tel que $\forall a \in A,\ \exists n \geq 2,\ a^n = a$. On souhaite montrer que A est commutatif (théorème attribué à **Jacobson**).

La résolution de cet exercice nécessite la connaissance des corps finis, du corps de décomposition d'un polynômes ainsi que des rudiments de réduction. On rappelle quelques définitions ci-après.

Un élément a d'une algèbre sur un corps K est dit ***algébrique*** s'il est racine d'un polynôme à coefficients dans K. L'idéal des polynômes annulateurs de a admet alors un unitaire générateur unitaire non constant de degré minimal, appelé ***polynôme minimal*** de a, qui est irréductible sur K.

Une K-algèbre est dite ***finie*** si sa dimension en tant que K-espace vectoriel est finie, ***algébrique*** si tous ses éléments sont algébriques (sur K).

Un élément a d'une K-algèbre algèbrique sera dit ***galoisien*** si son polyôme minimal a toutes ses racines simples dans une extension de décomposition et si l'ensemble $K[X]$ agit transitivement sur ses racines.

On peut alors formuler un énoncé préliminaire qui nous servira par la suite :

Dans une K-algèbre algébrique dont toutes les sous-algèbres finies sont commutatives, les éléments galoisiens sont tous centraux.

On rappelle au besoin que, *lorsqu'un polynôme irréductible sur $\mathbb{F}_p$ admet une racine dans une extension finie $\mathbb{F}_{p^d}$, alors il se scinde entièrement dans cette extension.*

On s'attaque maintenant au problème.

1. *Montrer que les idempotents de A sont nécessairement centraux.* (On pourra former le produit $ia(1-i)$.) *Rappeler brièvement pourquoi, si $a_1, ..., a_k$ sont des éléments centraux de somme 1 vérifiant $a_i a_j = a_i \delta^i_j$, alors l'anneau A est isomorphe au produit des anneaux $a_i A = A a_i$.*
2. *Montrer que la caractéristique de A est un produit de premiers distincts. En déduire que l'on peut se ramener au cas où $\operatorname{car} A$ est un premier p.*
3. *Soit $a \in A$ et $n := \min\{m \geq 2\ ;\ a^m = a\}$. Montrer que p ne saurait diviser $n-1$.* (question bonus[34] : montrer alors que l'on peut supposer n puissance de p)
4. *Montrer $X^n - X$ est scindé simple dans son corps de décomposition. En déduire des polynômes $Q_1, ..., Q_k$ tels que, en notant $a_i := Q_i(a)$, chaque $a_i a$ est galoisien dans l'anneau $a_i A$. Expliquer alors pourquoi on peut supposer a galoisien pour montrer qu'il est central.*
5. *Montrer que l'énoncé préliminaire permet de conclure.* (On considèra, dans une sous-algèbre finie de A, une famille maximale d'éléments $b_1, ..., b_k$ orthogonaux non nuls de somme 1 et on montrera que les $b_i B$ sont des corps.)

On chercher à présent à prouver l'énoncé préliminaire.

On note cette fois A une K-algèbre algébrique dont toutes les sous-algèbres finies sont commutatives.

Les matrices de $M_n(K)$ seront indexées de 0 à $n-1$ par commodité.

On fixe un élément $a \in A$ galoisien, on note μ_a son polynôme minimal, C la matrice compagnon de μ_a et on pose pour $X \in M_n(K)$

$$X(b) := \sum_{0 \leq i,j < n} x_{i,j} a^i b a^j.$$

1. *Que vaut $E_{0,0}(b)$? En déduire qu'il suffit de trouver une famille (B_r) génératrice de $M_n(K)$ telle que a commute avec $B_r(b)$ pour tout r.*

[34] Le premier p est donc étranger à $n-1$, d'où par le petit théorème de Fermat un entier $k > 0$ tel que $p^k = 1$ modulo $n-1$, mettons $p^k = 1 + K(n-1)$. On en déduit $a^{p^k} = a\underbrace{a^{n-1}a^{n-1}\cdots a^{n-1}}_{K \text{ fois}} = a$ en remplaçant successivement chaque aa^{n1} à gauche par a.

2. *Justifier l'existence d'une matrice Λ diagonale et d'une matrice inversible Q telles que $C = Q\Lambda Q^{-1}$, ainsi que d'une famille de polynômes $P_{i,j}$ tels que $\forall i,j,\ \lambda_i = P_{i,j}(\lambda_j)$. Dans quel corps tombent les coefficients de $\Lambda, Q, P_{i,j}$?*

   On pose
$$B_{i,j} := QE_{i,j}\ {}^tQ.$$

3. *Montrer que $E_{i,j}P_{i,j}(\Lambda) = \Lambda E_{i,j}$ et en déduire $B_{i,j}P_{i,j}({}^tC) = CB_{i,j}$.*
4. Soit (e_k) une K-base du corps de décomposition de μ_a dans laquelle on décompose
$$B_{i,j} = \sum_k e_k B_{i,j}^k \text{ avec } B_{i,j}^k \in M_n(K).$$
   Montrer que la famille $\left(B_{i,j}^k\right)$ engendre $M_n(K)$ lorsque i,j,k varient.
5. *En montrant* $\begin{cases} [CX](b) = aX(b) \\ [X^tC](b) = X(b)\,a \end{cases}$ *pour toute matrice X, conclure en considérant les algèbres $K\left[a, B_{i,j}^k(b)\right]$.*

Solution proposée (le théorème de Jacobson).

1. Soit i idempotent et $a \in A$. On a donc $i(1-i) = 0 = (1-i)i$, d'où $[ia(1-i)]^2 = 0$. L'hypothèse nous donne un $n \geq 2$ tel que $ia(1-i) = [ia(1-i)]^n$, mais ce dernier est nul puisque $n \geq 2$, d'où $ia = iai$. On montrerait de même que le produit $(1-i)ai$ est nul, d'où $ai = iai = ia$, *CQFD.*

   Chaque a_iA est bien un anneau car a_i est idempotent et central. Il suffit alors de considérer l'isomorphisme l'anneaux (vérifier que c'en est bien un)
$$\begin{cases} A & \xrightarrow{\sim} & a_1A \times \cdots \times a_kA \\ a & \longmapsto & (a_1a, ..., a_ka) \\ x_1 + \cdots + x_k & \longleftarrow & (x_1, ..., x_k) \end{cases}.$$

2. Soit p un premier divisant $c := \operatorname{car} A$. Par hypothèse, il y a un $n \geq 2$ tel que $p^n = p$. L'entier $p\left(p^{n-1} - 1\right)$ est donc nul dans A, donc multiple de c. Si p^2 divisait c, on obtiendrait $p \mid p^{n-1} - 1$, d'où modulo p la contradiction $1 = p^{n-1} = 0$ (car $n \geq 2$).

   Écrivons $c = p_1 \cdots p_r$ où les p_i sont des premiers distincts. Les nombres $\frac{c}{p_i}$ sont alors premiers entre eux, d'où par Bézout une écriture $1 = \sum u_i \frac{c}{p_i}$. En posant $a_i := u_i \frac{c}{p_i}$, on vérifie que $a_ia_j = u_iu_j \frac{c}{p_ip_j} c = 0$ pour $i \neq j$, puis que $a_i = 1a_i = \left(\sum_j a_j\right) a_i = a_i^2$. Le point précédent nous dit alors que $A \simeq \prod a_iA$ où chaque a_iA est de caractéristique p_i et vérifie l'hypothèse $\forall x,\ \exists n \geq 2,\ x^n = x$; il clair que la commutativité des a_iA implique celle de A.
3. On écrit $n - 1 = kp$. L'égalité $a^n = a$ devient alors $a\left(a^{kp} - 1\right) = 0$, ou encore $a\left(a^k - 1\right)^p = 0$ puisque l'anneau A est de caractéristique p. L'hypothèse appliquée à $a^k - 1$ nous donne un $m \geq 2$ tel que $\left(a^k - 1\right)^m = a^k - 1$, ce qui permet d'écrire (pour $m \geq p$)
$$a\left(a^k - 1\right) = a\left(a^k - 1\right)^m = a\left(a^k - 1\right)^p \left(a^k - 1\right)^{m-p} = 0,$$
   d'où $a^{k+1} = a$. Par minimalité de n, on doit avoir $n \leq k + 1$, mais l'égalité $n - 1 = kp$ force $p \leq 1$, d'où la contradiction.

   Il reste à voir pourquoi on peut effectivement choisir $m \geq p$. Or, si $b^m = b$, une récurrence immédaite montre $b^{m+r(m-1)} = b$ pour tout entier $r \geq 0$, ce qui permet de choisir m aussi grand que voulu.
4. Soit par l'absurde λ une racine multiple de $X^n - X$. Le scalaire λ est donc racine de $X^n - X$ et de sa dérivée $nX^{n-1} - 1$, ce qui s'écrit $\lambda^n = \lambda$ et $n\lambda^{n-1} = 1$, d'où
$$(n-1)\lambda = n\lambda^n - \left(n\lambda^{n-1}\right)\lambda = 0.$$
   Comme l'on est dans un corps, les condition $\lambda \neq 0$ (car $n\lambda^{n-1} = 1$) et $n - 1 \neq 0$ (car $p \nmid n - 1$) interdissent la nullité du produit ci-dessus, contradiction.

On peut donc décomposer $X^n - X = P_1 \cdots P_r$ dans $\mathbb{F}_p[X]$ en produit d'irréductible distincts. Comme pour le raisonnement sur la caractéristique, Bézout nous donne une relation $1 = \sum U_i \frac{X^n - X}{P_i}$; en posant $Q_i := U_i \frac{X^n - X}{P_i}$ et $a_i := Q_i(a)$, on obtient pour $i \neq j$ l'égalité

$$\begin{aligned} a_i a_j &= \left[U_i U_j \frac{X^n - X}{P_i P_j}(X^n - X)\right](a) = 0 \text{ puisque } a^n = a, \text{ d'où} \\ a_i &= a_i \cdot 1 = a_i \cdot \left[\sum_k Q_k\right](a) = a_i \sum_k a_k = a_i^2. \end{aligned}$$

Les idempotents de A étant automatiquement centraux, on peut donc factoriser $A \simeq \prod a_i A$.

Il reste à montrer que aa_i est galoisien dans $a_i A$. Il s'agit déjà de trouver un polynôme annulateur. Pour ne pas dire de bétises, bien noter que, l'anneau $a_i A$ étant une $\mathbb{F}_p$-algèbre unitaire, on peut y faire du calcul polynomial à coefficients dans $\mathbb{F}_p$ et que l'évaluation d'un terme λ constant vaudra λ fois l'unité de l'algèbre, à savoir λa_i. Ainsi, pour $P = \sum p_n X^n$ dans $\mathbb{F}_p[X]$, l'évaluation de P en l'élément $a_i x$ de l'anneau $a_i A$ est l'élément suivant de A :

$$P(a_i x) = \sum p_n (a_i x)^n = \sum p_n a_i x^n = a_i \sum p_n x^n = a_i P(x)$$

(bien noter la cohérence pour $n = 0$). Ces précautions étant prises, on peut calculer

$$P_i(a_i a) = a_i P_i(a) = [Q_i P_i](a) = [U_i (X^n - X)](a) = 0.$$

Comme P_i est irréductible, c'est bien le polynôme minimal de $a_i a$. Par ailleurs, toute racine de P_i est une racine de $X^n - X$ et ne saurait donc être multiple. Enfin, si λ et μ sont deux racines de P_i, ce dernier a une a racine dans l'extension $\mathbb{F}_p[\lambda]$, donc (*cf.* rappel) a toutes ses racines sont dans cette extension, en particulier μ, ce qui montre la transitivité de $\mathbb{F}_p[X]$ sur les racines de P_i et conclut ainsi au caractère galoisien de aa_i.

Par conséquent, si l'on montre que tout élément galoisien est central, on montrera que les composantes $a_i A$ de l'anneau $A \simeq \prod a_i A$ sont commutatives, donc que A est commutatif.

5. Admettons l'énoncé préliminaire. La $\mathbb{F}_p$-algèbre A est algébrique car chacun de ses éléments est annulé par un $X^n - X$. Si l'on montre que toute sous-algèbre finie de A est commutative, on pourra conclure que ses éléments galoisiens sont centraux, ce qui suffit à notre bonheur.

Soit donc B une sous-algèbre finie de A. Comme indiqué, on considère une famille maximale d'éléments $b_1, ..., b_k$ orthogonaux non nuls de somme 1, de sorte que l'anneau B est $\simeq \prod_{i=1}^k b_i B$. Pour justifier l'existence d'une telle famille, on remarque que, les espace-vectoriels $b_i B$ étant non nuls (car les b_i sont non nuls), on a nécessairement

$$\dim_{\mathbb{F}_p} B = \dim\left(\prod b_i B\right) = \sum \dim(b_i B) \geq \sum 1 = k.$$

Les familles (b_i) cherchées sont donc bornées en cardinal. Comme la famille à un élément (1) convient, on est sain et sauf.

Comme indiqué, montrons que les $b_i B$ sont des corps. Ceci montrera que l'anneau B est commutatif (comme produit d'anneau commutatif). D'après le théorème de Wedderburn, il suffit de montrer qu'un élément $x \in b_i B$ est ou bien nul ou bien inversible. Soit un tel x. On a un entier $n \geq 2$ tel que $x^n = x$, d'où un idempotent $y := x^{n-1}$ (vérifier !) qui commute nécessairement avec tout le monde. Puisque $y b_i = y$ (l'élément y est, comme x, de la forme $b_i b$), on en déduit que l'élément $b_i - y$ est encore idempotent :

$$(b_i - y)^2 = b_i^2 - 2 b_i y + y^2 = b_i - 2y + y = b_i - y.$$

Ainsi, en décomposant l'idempotent $b_i = (b_i - y) + y$ en somme de deux idempotents, la maximalité de notre famille de départ impose que l'un de ces idempotents soit nul : si c'est y, on trouve $x = x^n = xy = 0$, sinon on trouve $x^{n-1} = b_i$ et x est inversible dans $b_i B$, *CQFD*.

Solution proposée (énoncé préliminaire).

1. On voit que $E_{0,0}(b) = b$. Si on trouve une telle famille (B_r), alors b commutera (par linéairité) avec tous les $X(b)$ pour $X \in M_n(K)$, en particulier pour $X = E_{0,0}$, *CQFD*.

2. Le polynôme caractéristique de C est μ_a qui est scindé simple dans une extension de décomposition, donc C est diagonalisable dans cette extension, d'où l'existence de Λ et Q. Les polynômes $P_{i,j}$ sont donnés par la transitivité de l'action de $K[X]$ sur les racines de μ_a : ils sont donc à coefficients dans le corps K de base, eux.

3. Multiplier à droite par $P_{i,j}(\Lambda)$ multiplie la q-ième colonne par $P_{i,j}(\lambda_q)$ pour tout q, tandis que multiplier à gauche par Λ multiplie la p-ième ligne par λ_p pour tout p, d'où

$$E_{i,j}P_{i,j}(\Lambda) = P_{i,j}(\lambda_j)E_{i,j} = \lambda_i E_{i,j} = \Lambda E_{i,j}.$$

On en déduit

$$\begin{aligned} B_{i,j}P_{i,j}\left({}^tC\right) &= \left(Q\ E_{i,j}\ {}^tQ\right)\ \left({}^tQ^{-1}\ P_{i,j}(\Lambda)\ {}^tQ\right) \\ &= Q\ \left(E_{i,j}\ P_{i,j}(\Lambda)\right)\ {}^tQ \\ &= Q\ DE_{i,j}\ {}^tQ \\ &= Q\ \Lambda\ Q^{-1}\ Q\ E_{i,j}\ {}^tQ \\ &= CB_{i,j}. \end{aligned}$$

4. Les $B_{i,j}^k$ engendrent les $B_{i,j} = QE_{i,j}\ {}^tQ$ sur le gros corps $L := K(\lambda_1, ..., \lambda_n)$, donc par linéarité toute matrice de la forme $QM\ {}^tQ$ où $M \in M_n(L)$, donc (Q étant inversible) toutes les matrices de $M_n(L)$. Cela s'écrit aussi $\mathrm{rg}_L\left\{B_{i,j}^k\right\} = n^2$. Or, le rang est invariant par extension des scalaires, d'où $\mathrm{rg}_K\left\{B_{i,j}^k\right\} = n^2$ et $\mathrm{Vect}_K\left\{B_{i,j}^k\right\} = M_n(K)$, *CQFD.*

5. Admettons les deux égalités indiquées. De la seconde égalité $[X{}^tC](b) = X(b)\,a$ l'on déduit $\left[X\left({}^tC\right)^n\right](b) = X(b)\,a^n$ par une récurrence immédiate sur l'entier $n \geq 0$, d'où par linéarité $\left[XP\left({}^tC\right)\right](b) = X(b)\,P(a)$ pour tout polynôme P.

En remarquant que $C\sum_k e_k B_{i,j}^k = CB_{i,j} = B_{i,j}P_{i,j}\left({}^tC\right) = \sum_k e_k B_{i,j}^k P_{i,j}\left({}^tC\right)$, on déduit de la liberté des e_k les égalités $CB_{i,j}^k = B_{i,j}^k P_{i,j}\left({}^tC\right)$. On en tire

$$aB_{i,j}^k(b) = \left[CB_{i,j}^k\right](b) = \left[B_{i,j}^k P_{i,j}\left({}^tC\right)\right](b) = B_{i,j}^k(b)\,P_{i,j}(a).$$

Dans l'algèbre $K\left[a, B_{i,j}^k(b)\right]$, les deux générateurs sont tués par un polynôme d'après l'hypothèse "A algèbrique" et la relation ci-dessus montre que les éléments sont tous de la forme $\sum B_{i,j}^k(b)^r\,P^r(a)$ où P^r est un polynôme de degré $\deg\mu_a$ et où r varie de 0 à $\deg\mu_{B_{i,j}^k(b)}$. L'algèbre $K\left[a, B_{i,j}^k(b)\right]$ est donc finie, donc commutative, donc a commute avec $B_{i,j}^k(b)$. Comme les $B_{i,j}^k$ engendrent $M_n(K)$, on a terminé.

Montrons enfin l'indication : pour tout matrice $X \in M_n(K)$ on a d'une part (en abrégeant $n' := n-1$)

$$\begin{aligned} [CX](b) &= \sum_{i,j}\left(\sum_p c_{i,p}x_{p,j}\right)a^i b a^j \\ &= \sum_{p<n'}\sum_j x_{p,j}a^{p+1}ba^j + \sum_{i,j} c_{i,n'}x_{n',j}a^i b a^j \\ &= \left(a\sum_{j,p} x_{p,j}a^p b a^j - \sum_j x_{n',j}a^n b a^j\right) + \sum_j x_{n',j}\left(\sum_i c_{i,n'}a^i\right)ba^j \\ &= aX(b) - \sum_j x_{n',j}\underbrace{\left(a^n - \sum_i c_{i,n'}a^i\right)}_{=\mu(a)=0}ba^j \\ &= aX(b), \end{aligned}$$

d'autre part

$$\begin{aligned}
\left[X^t C\right](b) &= \sum_{i,j}\left(\sum_p x_{i,p}c_{j,p}\right)a^i b a^j \\
&= \sum_{p<n'}\sum_i x_{i,p}a^i b a^{p+1} + \sum_{i,j} x_{i,n'}c_{j,n'}a^i b a^j \\
&= \left(\left(\sum_{i,p} x_{i,p}a^i b a^p\right)a - \sum_i x_{i,n'}a^i b a^n\right) + \sum_i x_{i,n'}a^i b\left(\sum_j c_{j,n'}a^j\right) \\
&= X(b)\,a - \sum_i x_{i,n'}a^i b \underbrace{\left(a^n - \sum_j c_{j,n'}a^j\right)}_{=\mu(a)=0} \\
&= X(b)\,a, \text{ ce qui conclut.}
\end{aligned}$$

Remarque. On pourra comparer cette démonstration (tirée de la RMS) avec celle que nous proposons en DM (tirée d'un forum). Juste pour se convaincre que les mathématiciens aiment bien réécrire plusieurs fois la même chose :-).

Le lecteur curieux pourra chercher des anneaux vérifiant l'hypothèse de l'exercice. Il pourra montrer qu'ils sont nécessairement sous-anneaux d'un produit de corps (ou plus précisément que cette dernière condition équivaut à ce que tout nombre soit multiple de son carré) ; dans chacun de ces corps, tout élément est une racine de l'unité, donc chaque corps est de caractéristique positive. Réciproquement, convient tout sous-anneau d'un produit de corps dont chacun est la réunion de ses racines de l'unité : par exemple, une somme directe de corps finis.