Concours externe, interne et spécial docteur

Julien Rouyer
Valentin Massicot

Agrégation de mathématiques

10 ans d'annales avec corrigés détaillés de questions fondamentales

ellipses

Première partie

Concours interne

Chapitre 1

Mathématiques générales (épreuve 1)

1.1 2015, extraits des parties 1 et 2

Thèmes

algèbre linéaire (espace et sous-espace vectoriel, droite, base, matrice inversible, dimension, polynôme annulateur, polynôme caractéristique, vecteur propre, valeur propre, symétrie, vecteur directeur, trace, déterminant,)
anneaux et corps (sous-anneau, anneau commutatif, morphisme, isomorphisme, carré d'un élément, éléments inversibles, caractéristique, corps finis, corps des complexes, extension de corps)
groupes (ordre d'un élément, groupe linéaire)

Résultat majeur

théorème de Cayley-Hamilton

Remarques

Dans tout l'énoncé, il faut comprendre sous-anneau unitaire et morphisme d'anneaux unitaires. On démontre quelques résultats sur les matrices carrée de taille 2 *à coefficients dans un corps en prenant comme point de départ le théorème de* Cayley-Hamilton.

Énoncé

Pour tout corps k, on note $M_2(k)$ l'ensemble des matrices $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients $a, b, c, d \in k$, $\det(M)$ son déterminant et $\mathrm{tr}(M)$ sa trace. Ainsi, on a $\det(M) = ad - bc$ et $\mathrm{tr}(M) = a + d$. I_2 et 0_2 désignent respectivement la matrice identité et la matrice nulle de $M_2(k)$.

Soit $a \in k$. On pose $B = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$, $A = 2I_2 + B$, et

$$\mathscr{A}_a = \{M \in M_2(k) \mid \exists\, x, y \in k, M = xI_2 + yB\}.$$

Si R est un anneau unitaire, on note $\mathscr{U}(R)$ le groupe multiplicatif des éléments inversibles de R. $x \in R$ est un carré dans R s'il existe $y \in R$ tel que $x = y^2$.

3. Soit k un corps.
   (a) Montrer que pour tout $M \in M_2(k)$ on a $M^2 = \mathrm{tr}(M)M - \det(M)I_2$.
   (b) Exprimer, pour tout $M \in M_2(k)$, $\mathrm{tr}\left(M^2\right)$ en fonction de $(\mathrm{tr}(M))^2$ et $\det(M)$.
   (c) Soit $M \in \mathrm{GL}_2(k)$, telle que $\det M = 1$.
      i. Montrer que $M + M^{-1} = \mathrm{tr}(M)I_2$.
      ii. Montrer que $M^2 - M^{-2} = 0$ ssi $\mathrm{tr}(M) = 0$ ou $M^2 = I_2$.
      iii. On suppose que k est de caractéristique $\neq 2$. Montrer que M est d'ordre 4 ssi $\mathrm{tr}(M) = 0$.
4. Montrer que $\mathscr{A}_a$ est sous-anneau commutatif de $M_2(k)$ et en est un sous-k-espace vectoriel dont on donnera une base.
5. Si p est nombre premier et $k = \mathbb{F}_p$, en déduire que $\mathrm{Card}\mathscr{A}_a = p^2$.
6. Soit $\varphi : \mathscr{A}_a \mapsto \mathscr{A}_a$ la symétrie par rapport à la droite de vecteur directeur I parallèlement à la droite de vecteur directeur B. Montrer que φ est un morphisme d'anneaux.
7. Soit $M = xI_2 + yB$ un élément de $\mathscr{A}_a$.
   (a) Calculer $M\varphi(M)$ en fonction de x et y.
   (b) Montrer que $\det(M) = x^2 - ay^2$.
   (c) Montrer qu'une matrice M de $\mathscr{A}_a$ est dans $\mathscr{U}(\mathscr{A}_a)$ ssi $\det(M) \neq 0$.
8. Montrer que $\mathscr{A}_a$ est un corps ssi a n'est pas un carré dans k.
9. On suppose que $k = \mathbb{R}$. Montrer que si $a < 0$, $\mathscr{A}_a$ est isomorphe au corps $\mathbb{C}$ des nombres complexes.

Corrigé

3. (a) On peut obtenir cette égalité par un calcul direct (en remplaçant M, $\mathrm{tr}(M)$ et $\det(M)$ par leurs expressions en fonction de a, b, c et d) mais on préférera remarquer que si

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(k),$$

on a

$$\begin{aligned} \chi_M(X) = \begin{vmatrix} X-a & -b \\ -c & X-d \end{vmatrix} &= (X-a)(X-d) - bc \\ &= X^2 - (a+d)X + ad - bc \\ &= X^2 - \mathrm{tr}(M)X + \det(M). \end{aligned}$$

Faisons appel au théorème suivant :

Théorème (de Cayley-Hamilton)**.** *Soit k un corps, $n \geqslant 1$ et une matrice $M \in M_n(k)$. Le polynôme caractéristique de M, défini par $\chi_M(X) = \det(XI_n - M)$ est un polynôme annulateur de M, c'est-à-dire $\chi_M(M) = 0$.*

En l'appliquant ici, on obtient $M^2 - \mathrm{tr}(M)M + \det(M)I_2 = 0$ d'où $M^2 = \mathrm{tr}(M)M - \det(M)I_2$.

Remarque. De manière générale, il est utile de savoir que si $M \in M_n(k)$, le terme constant de χ_M est $\chi_M(0) = \det(-M) = (-1)^n \det(M)$ (car le déterminant est multilinéaire) et que le coefficient du monôme de degré $n-1$ de χ_M vaut $-\mathrm{tr}(M)$ (les autres coefficient sont plus difficiles à exprimer) :

$$\chi_M(X) = X^n - \mathrm{tr}(M)X^{n-1} + \cdots + (-1)^n \det(M).$$

(b) L'application trace est linéaire, $\mathrm{tr}(M) \in k$ et $\det(M) \in k$. La question précédente implique alors que pour tout $M \in M_2(k)$, on a

$$\begin{aligned} \mathrm{tr}(M^2) &= \mathrm{tr}\Big(\mathrm{tr}(M)M - \det(M)I_2\Big) \\ &= \mathrm{tr}(M)\,\mathrm{tr}(M) - \det(M)\,\mathrm{tr}(I_2) \\ &= \mathrm{tr}(M)^2 - 2\det(M). \end{aligned}$$

(c) i. Repartons de l'égalité $M^2 = \mathrm{tr}(M)M - \det(M)I_2$ démontrée à la question 3.(a). Comme $\det(M) = 1$, on a

$$M^2 = \mathrm{tr}(M)M - I_2.$$

En multipliant par M^{-1} chaque membre de l'égalité (ce qui est possible puisque M est supposée inversible), on obtient

$$M = \mathrm{tr}(M)MM^{-1} - I_2M^{-1} = \mathrm{tr}(M)I_2 - M^{-1},$$

d'où

$$M + M^{-1} = \mathrm{tr}(M)I_2.$$

ii. Il faut remarquer la présence d'une identité remarquable (valable car M et M^{-1} commutent : $MM^{-1} = M^{-1}M = I_2$) :

$$M^2 - M^{-2} = 0 \Leftrightarrow (M + M^{-1})(M - M^{-1}) = 0.$$

Or, d'après la question précédente, $M + M^{-1} = \mathrm{tr}(M)I_2$ donc

$$(M + M^{-1})(M - M^{-1}) = 0 \Leftrightarrow \mathrm{tr}(M)(M - M^{-1}) = 0.$$

Il serait très maladroit de faire appel à l'intégrité de l'anneau $M_2(k)$ (en interprétant l'égalité comme $(\mathrm{tr}(M)I_2)(M - M^{-1}) = 0$) puisque ce dernier n'est pas intègre : on a par exemple

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

On peut tout de même affirmer que

$$\mathrm{tr}(M)(M - M^{-1}) = 0 \Leftrightarrow \mathrm{tr}(M) = 0 \text{ ou } M - M^{-1} = 0$$

en remarquant que, k étant un corps, si $\mathrm{tr}(M) \neq 0$, $\mathrm{tr}(M)$ est inversible dans k et on peut multiplier par $\mathrm{tr}(M)^{-1}$ pour obtenir $M - M^{-1} = 0$. De plus, M étant inversible, la multiplication par M est réversible et on a $M - M^{-1} = 0 \Leftrightarrow M^2 - I_2 = 0$.
Finalement, on a bien

$$M^2 - M^{-2} = 0 \Leftrightarrow \mathrm{tr}(M) = 0 \text{ ou } M^2 = I_2.$$

iii. Il ne faut pas commettre l'erreur de penser que

$$M \text{ est d'ordre } 4 \Leftrightarrow M^4 = I_2.$$

En effet, l'ordre de M est défini par

$$\mathrm{ord}(M) = \min\{n \in \mathbb{N}^* \mid M^n = I_2\},$$

et on a en fait l'équivalence

$$M \text{ est d'ordre } 4 \Leftrightarrow M^4 = I_2 \text{ et } M \neq I_2, M^2 \neq I_2, M^3 \neq I_2.$$

Nous allons procéder par double implication car raisonner par équivalence lorsqu'une des propositions comporte un « et » ou un « ou » logique peut s'avérer périlleux.
Supposons que M est d'ordre 4. Par définition, on a $M^4 = I_2$ et donc $M^2 = M^{-2}$. D'après le résultat de la question précédente, on a $\mathrm{tr}(M) = 0$ ou $M^2 = I_2$. Cependant, l'ordre de M est 4 donc $M^2 \neq I_2$ et donc $\mathrm{tr}(M) = 0$.
Réciproquement, si $\mathrm{tr}(M) = 0$, le résultat de la question précédente implique que $M^2 = M^{-2}$ et donc $M^4 = I_2$. Il reste à montrer que $M \neq I_2, M^2 \neq I_2$ et $M^3 \neq I_2$. Pour cela, nous allons raisonner sur la trace des puissances de M. Le corps k est de caractéristique différente de 2 (on a $2 \neq 0$ dans k) et donc

$$\mathrm{tr}(I_2) = 2 \neq 0 = \mathrm{tr}(M),$$

ce qui implique que $M \neq I_2$. De plus, d'après 3.(b), on a

$$\mathrm{tr}\left(M^2\right) = \mathrm{tr}(M)^2 - 2\det(M) = -2$$

car $\mathrm{tr}(M) = 0$ et $\det(M) = 1$. Pour pouvoir affirmer que cela implique que $M^2 \neq I_2$, il faut nous assurer que $-2 \neq 2$ dans k, c'est-à-dire $4 \neq 0$ dans k. Or, la caractéristique p d'un corps $\mathbb{K}$ est un nombre premier vérifiant

$$\forall n \in \mathbb{Z}, \quad [\ n = 0 \text{ dans } \mathbb{K} \Leftrightarrow p \mid n\ ].$$

Puisque la caractéristique p de k est un nombre premier différent de 2, p ne divise pas 4 et donc $4 \neq 0$ dans k. Ainsi, on a également $M^2 \neq I_2$. Finalement, on a $M^3 = M^{-1} \neq I_2$ car $M \neq I_2$ donc l'ordre de M est bien exactement 4.

Remarque. On pouvait aussi évoquer le fait que $M^4 = I_2$ entraîne que l'ordre de M est un diviseur de 4, ce qui élimine de facto la possibilité que $M^3 = I_2$.

4. Commençons par montrer que $\mathscr{A}_a$ est un sous-espace vectoriel de $M_2(k)$. Démontrer laborieusement que $\mathscr{A}_a$ est non vide et stable par combinaisons linéaires est inutile : par définition, $\mathscr{A}_a = \text{Vect}(I_2, B)$ donc $\mathscr{A}_a$ est le sous-k-espace vectoriel de $M_2(k)$ dont (I_2, B) est une famille génératrice. (I_2, B) est de plus libre puisque I_2 et B ne sont pas proportionnelles donc (I_2, B) est une base de $\mathscr{A}_a$. $\mathscr{A}_a$ est alors de dimension 2.
   Montrons maintenant que $\mathscr{A}_a$ est un sous-anneau commutatif unitaire de $M_2(k)$. Comme $\mathscr{A}_a$ est un sous-espace vectoriel de $M_2(k)$, c'est un sous-groupe de $M_2(k)$. Il nous suffit donc de montrer que $\mathscr{A}_a$ est stable par produit, que $I_2 = 1_{M_2(k)} \in \mathscr{A}_a$ (ce qui est évident par définition des éléments de $\mathscr{A}_a$) et que la multiplication est commutative dans $\mathscr{A}_a$ (le produit matriciel n'étant pas commutatif dans $M_2(k)$, on ne peut pas affirmer que la commutativité dans $\mathscr{A}_a$ est héritée de celle dans $M_2(k)$). Considérons $X, Y \in \mathscr{A}_a$. Il existe $x, y, z, t \in k$ tels que

$$X = xI_2 + yB \quad \text{et } Y = zI_2 + tB.$$

   On a

$$\begin{aligned} XY &= (xI_2 + yB)(zI_2 + tB) \\ &= xzI_2 + (xt + yz)B + ytB^2 \end{aligned}$$

   et comme

$$B^2 = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = aI_2,$$

   on a

$$\begin{aligned} XY &= xzI_2 + (xt + yz)B + ytB^2 \\ &= xzI_2 + (xt + yz)B + ytaI_2 \\ &= (xz + yta)I_2 + (xt + yz)B \in \text{Vect}(I_2, B) = \mathscr{A}_a \end{aligned}$$

   donc $\mathscr{A}_a$ est stable par produit. La matrice I_2 commute avec toute matrice de $M_2(k)$ et la matrice B commute évidemment avec elle-même. Il est alors clair que les matrices du type $xI_2 + yB$ commutent entre elles. La multiplication est donc commutative dans $\mathscr{A}_a$.
   $\mathscr{A}_a$ est donc bien un sous-anneau commutatif de $M_2(k)$.
5. D'après la question précédente, $\mathscr{A}_a$ est un $\mathbb{F}_p$-espace vectoriel de dimension 2 donc, en tant qu'espace vectoriel, on a $\mathscr{A}_a \simeq \mathbb{F}_p^2$ (l'application $(x, y) \mapsto xI_2 + yB$ est un isomorphisme d'espaces vectoriels entre $\mathbb{F}_p^2$ et $\mathscr{A}_a$). En particulier, $\mathscr{A}_a$ et $\mathbb{F}_p^2$ sont en bijection, et leurs cardinaux sont égaux :

$$\text{Card}(\mathscr{A}_a) = \text{Card}\left(\mathbb{F}_p^2\right) = (\text{Card}(\mathbb{F}_p))^2 = p^2.$$

6. La symétrie φ est l'endomorphisme de $\mathscr{A}_a$ défini par

$$\varphi(xI_2 + yB) = xI_2 - yB, \quad \forall x, y \in k.$$

$\varphi(I_2) = I_2$ et $\varphi(B) = -B$ donc la matrice de φ, dans la base (I_2, B) de $\mathscr{A}_a$ (base constituée de vecteurs propres) est $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. L'application φ étant linéaire, elle est additive et il reste seulement à montrer qu'elle est multiplicative et que $\varphi(1_{\mathscr{A}_a}) = 1_{\mathscr{A}_a}$.
Soit $X, Y \in \mathscr{A}_a$. Il existe $x, y, z, t \in k$ tels que

$$X = xI_2 + yB \quad \text{et } Y = zI_2 + tB$$

et d'après les calculs effectués à la question 4., on a

$$XY = (xz + yta)I_2 + (xt + yz)B.$$

Ainsi, on a d'une part

$$\begin{aligned} \varphi(XY) &= \varphi\Big((xz + yta)I_2 + (xt + yz)B\Big) \\ &= (xz + yta)I_2 - (xt + yz)B \end{aligned}$$

et d'autre part,

$$\begin{aligned} \varphi(X)\varphi(Y) &= (xI_2 - yB)(zI_2 - tB) \\ &= xzI_2 - xtB - yzB + ytB^2 \\ &= xzI_2 - (xt + yz)B + ytaI_2 \\ &= (xz + yta)I_2 - (xt + yz)B \end{aligned}$$

d'où

$$\varphi(XY) = \varphi(X)\varphi(Y).$$

De plus, on a $1_{\mathscr{A}_a} = 1_k I_2 + 0_k B$ donc

$$\varphi(1_{\mathscr{A}_a}) = 1_k I_2 = I_2 = 1_{\mathscr{A}_a}.$$

Ainsi, φ est un morphisme d'anneaux.

7. (a) Par définition de φ et d'après la formule établie à la question 4. pour le produit de deux éléments de $\mathscr{A}_a$, on a

$$\begin{aligned} M\varphi(M) &= (xI_2 + yB)(xI_2 - yB) \\ &= (xx + y(-y)a)I_2 + (x(-y) + yx)B \\ &= (x^2 - ay^2)I_2. \end{aligned}$$

Remarque. On aurait également pu faire appel à l'identité remarquable $(xI_2 + yB)(xI_2 - yB) = x^2 I_2 - y^2 B^2$, valable car I_2 et B commutent, et utiliser l'égalité $B^2 = aI_2$ obtenue plus haut.

(b) Un calcul direct de déterminant donne

$$\det(M) = \begin{vmatrix} x & ya \\ y & x \end{vmatrix} = x^2 - ay^2.$$

(c) Procédons par double implication. Supposons que M soit inversible dans $\mathscr{A}_a$. Comme $\mathscr{A}_a$ est un sous-anneau unitaire de $M_2(k)$ (les anneaux $\mathscr{A}_a$ et $M_2(k)$ ont le même élément neutre multiplicatif), M est aussi inversible dans $M_2(k)$ et donc $\det(M) \neq 0$.
Réciproquement, supposons que $\det(M) \neq 0$. D'après les questions 7.(a) et 7.(b), on a

$$M\left(\frac{1}{\det(M)}\varphi(M)\right) = I_2.$$

Or, $\mathscr{A}_a$ est un anneau commutatif, donc

$$M\left(\frac{1}{\det(M)}\varphi(M)\right) = \left(\frac{1}{\det(M)}\varphi(M)\right) M = I_2 = 1_{\mathscr{A}_a}.$$

M est donc inversible d'inverse $M^{-1} = \dfrac{1}{\det(M)}\varphi(M) \in \mathscr{A}_a$, car $\dfrac{1}{\det(M)}$ est dans k et car $\varphi(M) \in \mathscr{A}_a$ (φ est un endomorphisme de $\mathscr{A}_a$ et $M \in \mathscr{A}_a$) et car $\mathscr{A}_a$ est un espace vectoriel.

Remarque. Le fait que $\mathscr{A}_a$ soit un sous-anneau **unitaire** de $M_2(k)$, c'est-à-dire qu'ils ont en particulier le même élément neutre pour la multiplication, est crucial. Considérons l'ensemble

$$\mathbb{A} = \left\{ \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix} \mid x \in k \right\} = \mathrm{Vect}(P)$$

dans lequel la matrice $P = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ vérifie $P^2 = P$. L'ensemble $\mathbb{A}$ est à la fois un sous-anneau et un sous-espace vectoriel de $M_2(k)$ mais n'est pas un sous-anneau unitaire de $M_2(k)$, bien que ce soit un anneau unitaire (d'élément neutre multiplicatif P). On ne peut donc pas affirmer sans justification que l'inversibilité d'un élément X de $\mathbb{A}$ implique son inversibilité dans $M_2(k)$ et donc que $\det(X) \neq 0$ (ce qui est manifestement faux puisque les matrices de $\mathbb{A}$ sont toutes de déterminant nul).

8. L'idée à exploiter est la suivante : par définition, $\mathscr{A}_a$ est un corps si et seulement si tout élément non nul de $\mathscr{A}_a$ est inversible (dans $\mathscr{A}_a$). Or, d'après la question 7., un élément $M = xI_2 + yB$ de $\mathscr{A}_a$ est inversible dans $\mathscr{A}_a$ si et seulement si $x^2 - ay^2 \neq 0$, c'est-à-dire, lorsque $y \neq 0$, si et seulement si $a \neq \left(\frac{x}{y}\right)^2$. On voit ainsi que l'existence ou non d'une racine carrée de a dans k est directement reliée aux inversibles de $\mathscr{A}_a$.

   Nous allons procéder par double contraposée, c'est-à-dire montrer l'équivalence

   $$\mathscr{A}_a \text{ n'est pas un corps} \Leftrightarrow a \text{ est un carré dans } k$$

   par double implication. Il n'est pas nécessaire de procéder ainsi mais cela nous permet d'éviter une démonstration par l'absurde.

   Supposons tout d'abord que $\mathscr{A}_a$ n'est pas un corps. Il existe alors un élément $M = xI_2 + yB \in \mathscr{A}_a$ non nul et non inversible. Supposons que $y = 0$. L'élément M n'étant pas inversible dans $\mathscr{A}_a$, la question 7. implique que $0 = \det(M) = x^2$ et donc $x = 0$. On en déduit que $M = xI_2 + yB = 0$, ce qui contredit l'hypothèse $M \neq 0$. On a donc $y \neq 0$, mais comme

   $$0 = \det(M) = x^2 - ay^2,$$

   on a alors

   $$a = \left(\frac{x}{y}\right)^2.$$

   Ainsi, a est un carré dans k.

   Réciproquement, supposons que a est un carré dans k et fixons $b \in k$ tel que $b^2 = a$. La matrice $M = bI_2 + 1_k B$ est alors de déterminant

   $$\det(M) = b^2 - a = 0$$

   mais elle n'est pas nulle puisque $(b, 1_k) \neq (0_k, 0_k)$ et puisque (I_2, B) est une base de $\mathscr{A}_a$ (d'après la question 4.). Ainsi, $\mathscr{A}_a$ admet un élément non nul et non inversible. $\mathscr{A}_a$ n'est donc pas un corps.

9. Supposons que $a < 0$. Remarquons que d'après la question précédente, a n'étant pas un carré dans $\mathbb{R}$, $\mathscr{A}_a$ est bien un corps. Nous proposons deux méthodes : la première, très élémentaire, consiste à déterminer un isomorphisme explicite entre $\mathscr{A}_a$ et $\mathbb{C}$ tandis que la deuxième, plus théorique, nécessite des connaissances sur les extensions de corps (cette méthode est à destination des candidats de l'agrégation externe).

   En explicitant un isomorphisme : nous cherchons un isomorphisme de corps entre $\mathscr{A}_a$ et $\mathbb{C}$, c'est-à-dire une bijection entre ces ensembles

qui respecte leur structure d'anneaux unitaires. Pour avoir une idée de ce à quoi va ressembler cet isomorphisme, il faut d'abord avoir en tête comment est définie la structure de corps de $\mathbb{C}$. Cette dernière est assez simple à résumer : $\mathbb{C}$ est composé des expressions de la forme $a1 + ib$ avec $a, b \in \mathbb{R}$ et où i est sujet à la relation $i^2 = -1$. Il nous faut donc trouver les éléments de $\mathscr{A}_a$ qui vont jouer le rôle de 1 et de i. Le candidat pour 1 est assez clair : 1 est l'élément neutre multiplicatif de $\mathbb{C}$ donc son image doit être l'élément neutre multiplicatif de $\mathscr{A}_a$, c'est-à-dire I_2. Pour l'image de i, on peut avoir comme première idée de choisir la matrice B (puisque c'est avec elle qu'on a travaillé jusqu'ici) mais un calcul direct montre que $B^2 = aI_2$ alors qu'il nous faut un élément J de $\mathscr{A}_a$ vérifiant $J^2 = -I_2$. On peut poser $J = \dfrac{1}{\sqrt{-a}}B$ (la racine carrée et le quotient existent bien puisque $a < 0$) et on a alors

$$J^2 = \left(\frac{1}{\sqrt{-a}}B\right)^2 = \frac{1}{-a}B^2 = \frac{1}{-a}aI_2 = -I_2.$$

On pose alors l'application $\mathbb{R}$-linéaire

$$\begin{array}{rccc} f : & \mathbb{C} & \to & \mathscr{A}_a \\ & a + ib & \mapsto & aI_2 + bJ. \end{array}$$

On a $I_2 = f(1)$ et $J = f(i)$. De plus, (I_2, J) est une base de $\mathscr{A}_a$ puisque (I_2, B) en est une et puisque J est un multiple non nul de B. On en déduit que f envoie la base $(1, i)$ de $\mathbb{C}$ sur la base (I_2, J) de $\mathscr{A}_a$ et donc que f est bijective. La linéarité de f impliquant son additivité et la formule définissant f impliquant directement que $f(1) = I_2 = 1_{\mathscr{A}_a}$, il nous reste à montrer que f est multiplicative.
Considérons $z_1, z_2 \in \mathbb{C}$ et fixons $a, b, c, d \in \mathbb{R}$ tels que $z_1 = a + ib$ et $z_2 = c + id$. D'une part, on a

$$\begin{aligned} f(z_1 z_2) &= f\Big((a + ib)(c + id)\Big) \\ &= f\Big((ac - bd) + i(ad + bc)\Big) \\ &= (ac - bd)I_2 + (ad + bc)J \end{aligned}$$

et d'autre part, on a

$$\begin{aligned} f(z_1)f(z_2) &= f(a + ib)f(c + id) \\ &= (aI_2 + bJ)(cI_2 + dJ) \\ &= acI_2 + (ad + bc)J + bdJ^2 \\ &= acI_2 + (ad + bc)J - bdI_2 \\ &= (ac - bd)I_2 + (ad + bc)J \end{aligned}$$

donc $f(z_1 z_2) = f(z_1)f(z_2)$ et f est multiplicative.
Finalement, f est un isomorphisme de corps (et même de $\mathbb{R}$-algèbres puisqu'elle est également $\mathbb{R}$-linéaire) et $\mathscr{A}_a$ est isomorphe au corps $\mathbb{C}$ des complexes.

Remarque. Il y a un deuxième isomorphisme g possible :

$$\begin{array}{rccc} g : & \mathbb{C} & \to & \mathscr{A}_a \\ & a+ib & \mapsto & aI_2 - bJ, \end{array}$$

ce qui revient à composer f et la conjugaison complexe, qui sont tous les deux des isomorphismes de corps, et donc g en est un aussi.

Via la théorie des corps : nous allons utiliser le fait que la clôture algébrique d'un corps est unique à isomorphisme de corps près.
En effet, si $\mathbb{R} \subset \mathbb{L}$ est une extension de dimension finie de $\mathbb{R}$, elle est algébrique et donc toute clôture algébrique de $\mathbb{L}$ est également une clôture algébrique de $\mathbb{R}$. Considérons $\overline{\mathscr{A}_a}$ une clôture algébrique de $\mathscr{A}_a$ (elle est unique à isomorphisme de corps près). D'après la question 4., on a $\dim_{\mathbb{R}}(\mathscr{A}_a) = 2$ donc $\overline{\mathscr{A}_a}$ est une clôture algébrique de $\mathbb{R}$ et est donc isomorphe (en tant que corps) à $\mathbb{C}$. Par multiplicativité du degré, on a de plus

$$\begin{aligned} 2 &= [\mathbb{C} : \mathbb{R}] \\ &= [\overline{A_a} : \mathbb{R}] \\ &= [\overline{\mathscr{A}_a} : \mathscr{A}_a][\mathscr{A}_a : \mathbb{R}] \\ &= 2[\overline{\mathscr{A}_a} : \mathscr{A}_a] \end{aligned}$$

donc

$$[\overline{\mathscr{A}_a} : \mathscr{A}_a] = 1$$

et donc $\mathscr{A}_a = \overline{\mathscr{A}_a}$, ce qui démontre que $\mathscr{A}_a$ est isomorphe au corps des nombres complexes.

Remarque. Ce raisonnement implique presque directement que les seules extensions de dimension finie (ou même algébriques) de $\mathbb{R}$ sont $\mathbb{R}$ et $\mathbb{C}$ (noter que le corps $\mathbb{H}$ des quaternions, qui contient $\mathbb{R}$, n'est pas une extension de $\mathbb{R}$ car c'est un corps non-commutatif).

1.2 2016, extrait de la partie 2

Thèmes

topologie (ouvert, fermé, boule, fonction continue)
espace euclidien (produit scalaire, norme euclidienne)
calcul différentiel (dérivées partielles, laplacien)

Résultats majeurs

règle de la chaîne
formule de Leibniz

Remarques

Nous traitons les questions 6. à 10. uniquement.

Énoncé

Soit n un entier $\geqslant 1$. Pour tout couple d'éléments

$$x = (x_1, \ldots, x_n) \in \mathbb{R}^n, y = (y_1, \ldots, y_n) \in \mathbb{R}^n,$$

on note respectivement

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \quad \text{et} \quad \|x\| = \sqrt{x \cdot x}$$

le produit scalaire usuel sur $\mathbb{R}^n$ et la norme de x.
La sphère de rayon 1 centrée en 0 est notée

$$S_{n-1} = \{x \in \mathbb{R}^n \mid \|x\| = 1\},$$

et G désigne le groupe orthogonal $O_n(\mathbb{R})$ des endomorphismes orthogonaux de $\mathbb{R}^n$. Pour $a \in \mathbb{R}^n$ et r réel > 0, on note $B(a, r)$ la boule **fermée** de centre a et de rayon r.
On note C_n l'ensemble des fonctions de classe C^2 de $B(0, 1)$ dans $\mathbb{R}$ (c'est-à-dire les fonctions admettant un prolongement de classe C^2 sur un ouvert contenant $B(0, 1)$).

On note $\langle f|g\rangle$ le produit scalaire sur C_n défini par

$$\langle f|g\rangle = \left(\int_{B(0,1)} \mathrm{d}x_1 \dots \mathrm{d}x_n\right)^{-1} \int_{B(0,1)} f(x)g(x)\mathrm{d}x_1 \dots \mathrm{d}x_n.$$

Soit $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$.
On note $x^\alpha : B(0,1) \to \mathbb{R}$ l'élément de C_n qui à $(x_1, \dots, x_n)$ associe $x_1^{\alpha_1} \dots x_n^{\alpha_n}$.
Pour tout $k \in \mathbb{N}$, on note M_k le sous-espace vectoriel de C_n formé des combinaisons linéaires des x^α, pour les α tels que $\alpha_1 + \dots + \alpha_n = k$.
Pour toute $f \in C_n$, on note

$$\Delta(f) = \sum_{i=1}^{n} \frac{\partial^2 f}{\partial x_i^2},$$

et H_k le sous-espace vectoriel de M_k égal à $\{f \in M_k \mid \Delta(f) = 0\}$.

6. Soit $x \in B(0,1)$, et $\sigma \in G$. Démontrer que $\sigma(x)$ est un élément de $B(0,1)$. On note $t_\sigma : B(0,1) \to B(0,1)$ l'application définie par $t_\sigma(x) = \sigma(x)$.
7. Soit $f \in C_n$. Démontrer que, pour tout $\sigma \in G$, $f \circ t_\sigma \in C_n$ puis que $\Delta(f \circ t_\sigma) = \Delta(f) \circ t_\sigma$.

Soit $k \in \mathbb{N}$.

8. Soit $\sigma \in G$; démontrer que si $f \in M_k$, $f \circ t_\sigma \in M_k$, et que, si $f \in H_k$, $f \circ t_\sigma \in H_k$.
9. Démontrer que, pour $f, g \in C_n$ et $\sigma \in G$, on a $\langle f \circ t_\sigma | g \circ t_\sigma\rangle = \langle f|g\rangle$.
10. Soit $f \in M_k$ telle que, pour tout $\sigma \in G$, on a $f \circ t_\sigma = f$.
    (a) Démontrer que, si x et $y \in B(0,1)$ sont tels que $\|x\| = \|y\|$, on a $f(x) = f(y)$.
    (b) Soit $g : [0,1] \to \mathbb{R}$ la fonction définie par $g(t) = f(0, \dots, 0, t)$. Démontrer que, pour tout $t \in [-1,1]$, on a $f(0, \dots, 0, t) = g(|t|)$, et que pour tout $x \in B(0,1)$, on a $f(x) = g(\|x\|)$.
    (c) On suppose que f n'est pas l'application nulle. Démontrer que k est pair, et qu'il existe $\lambda \in \mathbb{R}^*$ tel que, pour tout $x \in B(0,1)$, on a $f(x) = \lambda \|x\|^k$.

Corrigé

Cette partie faisant intervenir le groupe $O_n(\mathbb{R})$ des endomorphismes orthogonaux de $\mathbb{R}^n$, il peut être utile (pour avoir une intuition géométrique de la situation) de garder en tête qu'il s'agit de l'ensemble des rotations et symétries vectorielles (qui fixent l'origine) de $\mathbb{R}^n$.

6. Il s'agit presque d'une question de cours puisque G est l'ensemble des endomorphismes orthogonaux de $\mathbb{R}^n$, ce qui coïncide avec l'ensemble des isométries linéaires de $\mathbb{R}^n$. En effet, si σ est un endomorphisme de $\mathbb{R}^n$ et si σ^* désigne l'adjoint de σ par rapport au produit scalaire usuel de $\mathbb{R}^n$, on a la suite d'équivalences

$$\begin{aligned}\sigma \in G &\Leftrightarrow \sigma^* \circ \sigma = \mathrm{id}_{\mathbb{R}^n} \\ &\Leftrightarrow \forall x, y \in \mathbb{R}^n,\ \langle \sigma^* \circ \sigma(x) | y \rangle = \langle x | y \rangle \\ &\Leftrightarrow \forall x, y \in \mathbb{R}^n,\ \langle \sigma(x) | \sigma(y) \rangle = \langle x | y \rangle \\ &\underset{(1)}{\Leftrightarrow} \forall x \in \mathbb{R}^n,\ \|\sigma(x)\| = \|x\|\end{aligned}$$

où (1) provient de l'identité de polarisation

$$\langle x, y \rangle = \frac{1}{2}\left(\|x+y\|^2 - \|x\|^2 - \|y\|^2\right).$$

Ainsi, tout élément σ de G est une isométrie de $\mathbb{R}^n$ et on a

$$\|\sigma(x)\| = \|x\| \leqslant 1,$$

ce qui démontre que $\sigma(x) \in B(0,1)$.

7. Fixons $\sigma \in G$. Par définition de C_n, il existe une fonction $g : U \to \mathbb{R}$ de classe C^2 qui prolonge f sur un ouvert U de $\mathbb{R}^n$ contenant $B(0,1)$. L'application σ étant linéaire sur un espace vectoriel normé ($\mathbb{R}^n$ est bien sûr muni de la norme euclidienne usuelle) de dimension finie, elle est automatiquement de classe C^∞. Plus précisément, la dimension finie de $\mathbb{R}^n$ implique que tous ses endomorphismes sont continus et de plus, pour un endomorphisme d'un espace vectoriel normé quelconque (peu importe sa dimension), être continu est équivalent à être de classe C^∞.

Pour pouvoir affirmer que $f \circ t_\sigma \in C_n$, il nous faut lui trouver un prolongement C^2 à un ouvert contenant $B(0,1)$. On veut bien sûr poser $h = g \circ \sigma$ mais il faut prendre quelque précautions sur l'ensemble de définition de h : l'application g n'est définie que sur l'ouvert U donc il nous faut restreindre l'ensemble de définition de σ à $V = \sigma^{-1}(U)$ de sorte que pour tout $x \in V$, $\sigma(x)$ soit dans l'ensemble de définition de g. On pose donc finalement l'application

$$\begin{array}{rccc} h : & \sigma^{-1}(U) & \to & \mathbb{R} \\ & x & \mapsto & g(\sigma(x)). \end{array}$$

Puisque σ est continue et puisque U est un ouvert de $\mathbb{R}^n$, $\sigma^{-1}(U)$ est un ouvert de $\mathbb{R}^n$ et comme h est définie sur cet ensemble comme la composée

de g et σ qui sont toutes deux de classe C^2 (σ est même de classe C^∞), h est bien de classe C^2. Il reste à vérifier que $\sigma^{-1}(U)$ contient $B(0,1)$ et que $h_{|B(0,1)} = f \circ t_\sigma$. Pour cela, considérons $x \in B(0,1)$. D'après la question précédente, $\sigma(x) \in B(0,1)$ et par définition de U, $B(0,1) \subset U$, ce qui prouve que $\sigma^{-1}(U)$ contient $B(0,1)$. Finalement, pour tout $x \in B(0,1)$, on a

$$h(x) = g(\sigma(x)) = f(\sigma(x)) = f \circ t_\sigma(x)$$

puisque $\sigma(x) \in B(0,1)$ et puisque $g_{|B(0,1)} = f$. h prolonge donc bien $f \circ t_\sigma$ et nous avons donc démontré que $f \circ t_\sigma \in C_n$.

Le calcul de $\Delta(f \circ t_\sigma)$ s'effectue alors avec la généralisation multidimensionnelle de la règle de la chaîne, dont nous rappelons l'énoncé.

Théorème (de dérivation des fonctions composées)**.** *Soit $m, n, p > 0$, U un ouvert de $\mathbb{R}^m$, V un ouvert de $\mathbb{R}^n$ et $g : U \to V$, $f : V \to \mathbb{R}^p$ deux fonctions de classe C^1. L'application $f \circ g : U \to \mathbb{R}^p$ est de classe C^1 et pour tout couple $(i,j) \in [\![1,m]\!] \times [\![1,p]\!]$, on a*

$$\frac{\partial (f \circ g)_j}{\partial x_i} = \sum_{k=1}^{n} \left(\frac{\partial f_j}{\partial x_k} \circ g \right) \frac{\partial g_k}{\partial x_i}.$$

Dans notre cas, pour tout $i \in [\![1,n]\!]$, on a

$$\frac{\partial (f \circ t_\sigma)}{\partial x_i} = \sum_{k=1}^{n} \left(\frac{\partial f}{\partial x_k} \circ t_\sigma \right) \frac{\partial (t_\sigma)_k}{\partial x_i}$$

et donc par la formule de Leibniz

$$\frac{\partial^2 (f \circ t_\sigma)}{\partial x_i^2} = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \left(\left(\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma \right) \frac{\partial (t_\sigma)_j}{\partial x_i} \right) \frac{\partial (t_\sigma)_k}{\partial x_i} + \left(\frac{\partial f}{\partial x_k} \circ t_\sigma \right) \frac{\partial^2 (t_\sigma)_k}{\partial x_i^2} \right).$$

Cette formule est assez lourde mais il y a bien heureusement des simplifications à faire. Tout d'abord, si $(e_1, \ldots, e_n)$ désigne la base canonique

de $\mathbb{R}^n$ et si $i \in [\![1, n]\!]$, on a, pour tout $a \in B(0,1)$:

$$\begin{aligned}\frac{\partial t_\sigma}{\partial x_i}(a) &= \lim_{t\to 0} \frac{1}{t}\left(t_\sigma(a+te_i) - t_\sigma(a)\right)\\ &= \lim_{t\to 0} \frac{1}{t}\left(\sigma(a+te_i) - \sigma(a)\right)\\ &= \lim_{t\to 0} \frac{1}{t}\sigma(te_i)\\ &= \lim_{t\to 0} \sigma(e_i)\\ &= \sigma(e_i).\end{aligned}$$

Ainsi, pour tous $i, j \in [\![1, n]\!]$, $\dfrac{\partial (t_\sigma)_i}{\partial x_j}$ est exactement le coefficient a_{ij} de la matrice de σ dans la base canonique de $\mathbb{R}^n$. En particulier, pour tous $i, j \in [\![1, n]\!]$, $\dfrac{\partial (t_\sigma)_i}{\partial x_j}$ est une fonction constante et donc $\dfrac{\partial^2 (t_\sigma)_k}{\partial x_i^2} = 0$. On peut donc réécrire la formule obtenue précédemment sous la forme plus agréable

$$\frac{\partial^2 (f \circ t_\sigma)}{\partial x_i^2} = \sum_{k=1}^{n}\sum_{j=1}^{n}\left(a_{ji}a_{ki}\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma\right)$$

où $(a_{ij})_{1\leqslant i,j\leqslant n}$ désigne la matrice de σ dans la base canonique de $\mathbb{R}^n$. Ainsi, le laplacien de $f \circ t_\sigma$ est donné par

$$\begin{aligned}\Delta(f \circ t_\sigma) &= \sum_{i=1}^{n} \frac{\partial^2 (f \circ t_\sigma)}{\partial x_i^2}\\ &= \sum_{i=1}^{n}\sum_{k=1}^{n}\sum_{j=1}^{n}\left(a_{ji}a_{ki}\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma\right)\\ &= \sum_{k=1}^{n}\sum_{j=1}^{n}\sum_{i=1}^{n}\left(a_{ji}a_{ki}\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma\right)\\ &= \sum_{k=1}^{n}\sum_{j=1}^{n}\left(\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma \sum_{i=1}^{n} a_{ji}a_{ki}\right).\end{aligned}$$

On voit apparaître les produits scalaires des lignes de la matrice A à travers l'expression $\displaystyle\sum_{i=1}^{n} a_{ji}a_{ki}$. Il faut se rappeler de la caractérisation matricielle des endomorphismes orthogonaux : un endomorphisme d'un espace euclidien est orthogonal ssi sa matrice A dans toute base orthonormale (il suffit en fait que ce soit vrai pour une base orthonormale)

vérifie $AA^T = A^TA = I_n$. En particulier, les lignes (resp. les colonnes) d'une matrice dans une base orthonormale d'un endomorphisme orthogonal forment une base orthonormale de l'espace des vecteurs lignes (resp. vecteurs colonnes). La base canonique de $\mathbb{R}^n$ étant bien sûr orthonormale pour le produit scalaire scalaire usuel et σ étant un endomorphisme orthogonal, on a donc $\sum_{i=1}^{n} a_{ji}a_{ki} = \delta_{jk}$ pour tous $j, k \in [\![1, n]\!]$ et donc notre formule pour le laplacien de $f \circ t_\sigma$ devient

$$\begin{aligned}\Delta(f \circ t_\sigma) &= \sum_{k=1}^{n}\sum_{j=1}^{n}\left(\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma\right)\sum_{i=1}^{n} a_{ji}a_{ki} \\ &= \sum_{k=1}^{n}\sum_{j=1}^{n}\left(\frac{\partial^2 f}{\partial x_j \partial x_k} \circ t_\sigma\right)\delta_{jk} \\ &= \sum_{k=1}^{n}\frac{\partial^2 f}{\partial x_k^2} \circ t_\sigma \\ &= \Delta(f) \circ t_\sigma.\end{aligned}$$

8. Soit $f \in M_k$. f est une combinaison linéaire de termes du type x^α avec $\alpha_1 + \cdots + \alpha_n = k$. Puisque la composition à droite par t_σ est linéaire, il suffit de montrer que si f est du type x^α alors $f \circ t_\sigma \in M_k$. Considérons $\alpha \in \mathbb{N}^n$ tel que $\alpha_1 + \cdots + \alpha_n = k$ et posons $A = (a_{ij})$ la matrice de σ dans la base canonique de $\mathbb{R}^n$. Pour tout $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ et tout $i \in [\![1, n]\!]$, la i-ième coordonnée de Ax est $(Ax)_i = \sum_{k=1}^{n} a_{ik}x_k$ et donc

$$x^\alpha \circ t_\sigma(x) = \prod_{i=1}^{n}\left(\sum_{k=1}^{n} a_{ik}x_k\right)^{\alpha_i}.$$

Nous allons utiliser une propriété importante des polynômes homogènes : si $r, s \geqslant 0$ et si $f \in M_r$, $g \in M_s$ alors $fg \in M_{r+s}$ [1].
En effet, avec de telles fonctions f et g, on peut écrire

$$f = \sum_{\alpha_1+\cdots+\alpha_n=r} a_\alpha x^\alpha \quad \text{et} \quad g = \sum_{\beta_1+\cdots+\beta_n=s} b_\beta x^\beta$$

et on a

$$fg = \sum_{\alpha_1+\cdots+\alpha_n=r}\ \sum_{\beta_1+\cdots+\beta_n=s} a_\alpha b_\beta x^{\alpha+\beta}$$

1. Si M est l'ensemble des polynômes réels à n variables, M est une $\mathbb{R}$-algèbre et admet la décomposition en somme directe $M = \bigoplus_{k\in\mathbb{N}} M_k$. On dit que M est une $\mathbb{R}$-algèbre graduée car cette décomposition en somme directe vérifie $M_iM_j \subset M_{i+j}$ pour tous $i, j \in \mathbb{N}$.

qui est bien un élément de M_{r+s} car pour tous $\alpha, \beta \in \mathbb{N}^n$ vérifiant respectivement $\alpha_1 + \cdots + \alpha_n = r$ et $\beta_1 + \cdots + \beta_n = s$, on a

$$(\alpha+\beta)_1 + \cdots + (\alpha+\beta)_n = \alpha_1 + \beta_1 + \cdots + \alpha_n + \beta_n = r + s$$

et car M_{r+s} est stable par combinaison linéaire (c'est un sous-espace vectoriel de C_n).

Revenons en à $x^\alpha \circ t_\sigma$. Pour tout $i \in [\![1, n]\!]$, la fonction polynomiale $\sum_{k=1}^{n} a_{ik}x_k$ est un élément de M_1 et donc par la propriété mentionnée précédemment, on a

$$\left(\sum_{k=1}^{n} a_{ik}x_k\right)^{\alpha_i} = \prod_{j=1}^{\alpha_i}\left(\sum_{k=1}^{n} a_{ik}x_k\right) \in M_{\underbrace{1+\cdots+1}_{\alpha_i \text{ fois}}} = M_{\alpha_i}.$$

En utilisant une fois de plus cette propriété, on peut affirmer que

$$x^\alpha \circ t_\sigma = \prod_{i=1}^{n}\left(\sum_{k=1}^{n} a_{ik}x_k\right)^{\alpha_i} \in M_{\alpha_1+\cdots+\alpha_n} = M_k.$$

Il reste finalement à montrer que si de plus $\Delta(f) = 0$ alors $\Delta(f \circ t_\sigma) = 0$. Or, la question précédente nous assure que $\Delta(f \circ t_\sigma) = \Delta(f) \circ t_\sigma$ donc si $\Delta(f) = 0$, on a $\Delta(f \circ t_\sigma) = 0 \circ t_\sigma = 0$ et $f \circ t_\sigma \in H_k$.

9. Il faut montrer que pour tous $f, g \in C_n$ et $\sigma \in G$, on a

$$\int_{B(0,1)} f \circ t_\sigma(x) g \circ t_\sigma(x) \mathrm{d}x_1 \ldots \mathrm{d}x_n = \int_{B(0,1)} f(x)g(x)\mathrm{d}x_1 \ldots \mathrm{d}x_n.$$

Si on garde en tête ce que représente t_σ, l'égalité se comprend très bien géométriquement : σ est une rotation ou une symétrie laissant fixe l'origine et ces transformations isométriques de l'espace (qui préservent donc les hypervolumes) envoient $B(0,1)$ sur lui-même donc l'intégration sur $B(0,1)$ doit être invariante par composition avec σ. La démonstration, elle, se fera grâce au théorème de changement de variable. Ce dernier nécessitant qu'on intègre sur un ouvert de $\mathbb{R}^n$, nous allons réduire le domaine d'intégration de $B(0,1)$ à la boule unité ouverte B. La sphère S_{n-1} étant un « ensemble de dimension $n-1$ » [2], retirer cet ensemble du domaine d'intégration (qui est un objet de dimension n) ne changera rien à notre intégrale, de la même manière que changer la valeur d'une fonction $f : [a, b] \to \mathbb{R}$ en un nombre fini de points ne change pas la valeur de son intégrale sur $[a, b]$.

2. Le terme topologique exact serait « sous-variété de dimension $n-1$ ».

N'oublions pas de dire que t_σ envoie bien B dans B car si $x \in B$, on a

$$\|t_\sigma(x)\| = \|\sigma(x)\| = \|x\| < 1.$$

De plus, t_σ est de classe C^∞ sur B car c'est la restriction d'une application linéaire (donc de classe C^∞ car $\mathbb{R}^n$ est de dimension finie) et que c'est même un C^∞-difféomorphisme de B dans B car $t_{\sigma^{-1}}$ (qui existe bien car G est un groupe) est sa réciproque.

Calculons maintenant le déterminant jacobien de t_σ. Pour cela, on peut remarquer que, puisque t_σ est une restriction de σ et puisque σ est une application linéaire, la différentielle de t_σ est constante et vaut toujours σ. En effet, pour tous $a \in B$ et $h \in B - a$, on a

$$\begin{aligned} t_\sigma(a+h) &= \sigma(a+h) \\ &= \sigma(a) + \sigma(h) \\ &= t_\sigma(a) + \sigma(h) \\ &= t_\sigma(a) + \sigma(h) + \|h\|\varepsilon(h) \end{aligned}$$

avec $\varepsilon(h) = 0 \xrightarrow[h\to 0]{} 0$. Or, σ est linéaire sur un espace vectoriel normé de dimension finie donc σ est bien continue et par définition de la différentiabilité, on a

$$\mathrm{d}_a t_\sigma = \sigma$$

pour tout $a \in B$. Ainsi, pour tout $a \in B$, on a

$$|\det(\mathrm{Jac}_{t_\sigma}(a))| = |\det(\mathrm{d}_a t_\sigma)| = |\det(\sigma)| = 1$$

car σ est un endomorphisme orthogonal donc de déterminant 1 ou -1.

Finalement, en posant

$$C = \left(\int_{B(0,1)} \mathrm{d}x_1 \dots \mathrm{d}x_n \right)^{-1}$$

pour simplifier les notations, le théorème de changement de variable

donne, pour tous $f, g \in C_n$, les égalités

$$\begin{aligned}
\langle f \circ t_\sigma \mid g \circ t_\sigma \rangle &= C \int_{B(0,1)} f \circ t_\sigma(x) g \circ t_\sigma(x) \mathrm{d}x_1 \dots \mathrm{d}x_n \\
&= C \int_B f \circ t_\sigma(x) g \circ t_\sigma(x) \mathrm{d}x_1 \dots \mathrm{d}x_n \\
&= C \int_B f \circ t_\sigma(x) g \circ t_\sigma(x) |\det(\mathrm{Jac}_{t_\sigma}(a))| \mathrm{d}x_1 \dots \mathrm{d}x_n \\
&= C \int_B f(x) g(x) \mathrm{d}x_1 \dots \mathrm{d}x_n \\
&= C \int_{B(0,1)} f(x) g(x) \mathrm{d}x_1 \dots \mathrm{d}x_n \\
&= \langle f \mid g \rangle .
\end{aligned}$$

10. (a) L'argument clef est le fait que G agit transitivement sur la sphère S_{n-1}. En effet, si on admet ce résultat, pour tous $x, y \in B(0,1)$ vérifiant $\|x\| = \|y\|$, il existe $\sigma \in G$ tel que $x = \sigma(y)$ et on a donc

$$f(x) = f(\sigma(y)) = f \circ t_\sigma(y) = f(y).$$

Le jury attend que le candidat donne une justification de la transitivité de l'action. Ceci peut se faire en se ramenant au cas plus élémentaire $n = 2$. En effet, si $x, y \in B(0,1)$ ont la même norme, on peut considérer deux cas.

— Si (x, y) est liée alors comme les vecteurs x et y ont la même norme, on a $x = y$ ou $x = -y$. Dans le premier cas, l'élément $\sigma = \mathrm{id}_{\mathbb{R}^n} \in G$ vérifie bien $\sigma(x) = y$ et dans le deuxième cas, l'élément $\sigma = -\mathrm{id}_{\mathbb{R}^n} \in G$ vérifie bien $\sigma(x) = y$.

— Si (x, y) est libre, on peut considérer $F = \mathrm{Vect}(x, y)$ qui est un sous-espace vectoriel de dimension 2 de $\mathbb{R}^n$. Il existe donc un endomorphisme orthogonal σ de F (pour le produit scalaire induit par celui de $\mathbb{R}^n$) vérifiant $\sigma(x) = y$. On prolonge alors σ à $\mathbb{R}^n$ par l'identité sur $F^\perp$ en posant

$$\begin{array}{rccc}
 & \mathbb{R}^n = F \oplus F^\perp & \to & \mathbb{R}^n \\
\tilde{\sigma} : & x = x_1 + x_2 & \mapsto & \sigma(x_1) + x_2.
\end{array}$$

On a alors $\tilde{\sigma}(x) = y$ mais il reste à vérifier que $\tilde{\sigma} \in G$. Considérons $z \in \mathbb{R}^n$ et posons $z = z_1 + z_2$ sa décomposition dans la somme directe

$\mathbb{R}^n = F \oplus F^\perp$. On a

$$\begin{aligned}\|\tilde{\sigma}(z)\|^2 &= \|\tilde{\sigma}(z_1 + z_2)\|^2 \\ &= \|\sigma(z_1) + z_2\|^2 \\ &= \|\sigma(z_1)\|^2 + 2\langle \sigma(z_1) \mid z_2\rangle + \|z_2\|^2.\end{aligned}$$

Or, σ est orthogonal pour le produit scalaire induit donc

$$\|\sigma(z_1)\|^2 = \|z_1\|^2$$

et comme $\sigma(z_1) \in F$ et $z_2 \in F^\perp$, on a

$$\langle \sigma(z_1) \mid z_2\rangle = 0.$$

Finalement, on a

$$\begin{aligned}\|\tilde{\sigma}(z)\| &= \|\sigma(z_1)\|^2 + 2\langle \sigma(z_1) \mid z_2\rangle + \|z_2\|^2 \\ &= \|z_1\|^2 + \|z_2\|^2 \\ &= \|z_1 + z_2\|^2 \\ &= \|z\|^2\end{aligned}$$

car z_1 et z_2 sont orthogonaux. On a donc $\tilde{\sigma} \in G$.

(b) Soit $t \in [-1, 1]$. Les deux vecteurs $(0, \dots, 0, t)$ et $(0, \dots, 0, -t)$ ayant la même norme, la question précédente nous donne l'égalité

$$f(0, \dots, 0, t) = f(0, \dots, 0, -t).$$

Or, $|t| \in \{t, -t\}$ donc on a bien $g(|t|) = f(0, \dots, 0, |t|) = f(0, \dots, 0, t)$. De même, si $x \in B(0, 1)$, les vecteurs x et $(0, \dots, 0, \|x\|)$ ayant la même norme, la question précédente nous donne l'égalité

$$g(\|x\|) = f(0, \dots, 0, \|x\|) = f(x).$$

(c) Le candidat attentif aura remarqué que nous n'avons toujours pas utilisé le fait que $f \in M_k$. Nous allons le faire ici. C'est en effet la seule chose nécessaire pour cette question : si $x \in B(0, 1)$ est non nul, on a

$$f(x) = f\left(\frac{\|x\|}{\|x\|}x\right) = \|x\|^k f\left(\frac{1}{\|x\|}x\right)$$

car f est homogène de degré k. De plus, la quantité

$$f\left(\frac{1}{\|x\|}x\right)$$

ne dépend pas de x car $\left\|\frac{1}{\|x\|}x\right\| = 1$ et d'après la question précédente, on a

$$f\left(\frac{1}{\|x\|}x\right) = g(1).$$

Ainsi, pour tout $x \in B(0,1)\backslash\{0\}$, on a

$$f(x) = g(1)\|x\|^k$$

et comme $f(0) = 0$ (car f est une fonction polynomiale homogène), l'égalité est vraie pour tout $x \in B(0,1)$. On a $g(1) \neq 0$ car sinon f serait nulle, ce qui est exclu par l'énoncé.

Il ne reste plus qu'à montrer que k est pair. Cela provient du fait que f est homogène de degré k et vérifie donc l'égalité $f(\lambda x) = \lambda^k f(x)$ pour tout $x \in \mathbb{R}^n$ et tout $\lambda \in \mathbb{R}$. En effet, cette propriété implique en particulier que si $\|x\| = 1$, on a alors aussi $\|-x\| = 1$ et on a donc

$$g(1) = f(x) = f(-(-x)) = (-1)^k f(-x) = (-1)^k g(1).$$

Comme $g(1) \neq 0$, on a alors $1 = (-1)^k$ et donc k est pair.

1.3 2022, vrai-faux et exercice préliminaire

Thèmes

matrices (trace, déterminant, polynôme annulateur, polynôme caractéristique, endomorphisme associé, matrices semblables et invariants de similitude)
espaces vectoriels (famille libre, famille liée, base)
anneaux (morphisme d'anneaux, élément inversible d'un anneau)

Résultats majeurs

théorème spectral
théorème de Cayley-Hamilton
théorème de la base incomplète
propriétés de la matrice compagnon d'un polynôme unitaire

Remarques

1(a) Trouver un contre-exemple pour $n \geqslant 2$ et pas seulement pour $n = 2$. 1(b) Il faut démontrer que $\chi_M(X) = X^2 - \mathrm{Tr}(M)X + \det(M)$. 1(c) Le théorème spectral pour les matrices symétriques n'est pas valable sur $\mathbb{C}$. χ_M scindé n'entraîne pas que M est diagonalisable. 3(b) Le but est de démontrer le théorème de Cayley-Hamilton *à l'aide des résultats qui précèdent.*

Énoncé

Vrai ou faux ?

Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera soigneusement les réponses.

1. (a) Soit n un entier strictement positif. Il existe des matrices M et N de $\mathscr{M}_n(\mathbb{C})$ telles que $\mathrm{Tr}(MN) \neq \mathrm{Tr}(NM)$.

(b) Deux matrices de $\mathscr{M}_2(\mathbb{C})$ ont le même polynôme caractéristique si et seulement si elles ont la même trace et le même déterminant.

(c) Les matrices carrées et symétriques à coefficients dans $\mathbb{C}$ sont diagonalisables.

(d) Soit $\varphi : A \to B$ un morphisme d'anneaux [3].
Si $\varphi(a)$ est inversible dans B alors a est inversible dans A.

Exercice préliminaire [4]

2. Soit d un entier strictement positif. Soit

$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0$$

un polynôme de $\mathbb{C}[X]$ à coefficients complexes [5]. On appelle *matrice compagnon* du polynôme P la matrice C_P de $\mathscr{M}_d(\mathbb{C})$ suivante :

$$C_P = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -a_{d-2} \\ 0 & \dots & 0 & 1 & -a_{d-1} \end{pmatrix}.$$

En développant le déterminant $\chi_{C_P}(X) = \det(XI_d - C_P)$ par rapport à sa première ligne et à l'aide d'une récurrence, montrer que

$$\chi_{C_P}(X) = P(X).$$

3. Soit p un entier strictement positif et soit M une matrice de $\mathscr{M}_p(\mathbb{C})$.

3. Sous-entendu *unitaires*. La notion d'élément inversible n'aurait sinon pas de sens.

4. L'exercice 2 de l'épreuve spéciale docteurs de 2023 (voir page 370 du présent volume) traite également des matrices compagnons mais avec une approche différente. Sur le même thème, on trouvera les corrigés des questions relatives aux matrices compagnons de l'épreuve de mathématiques générales du concours externe de 2019 (I. exercice préliminaire 4.) et de 2020 (exercice 2) dans notre précédent ouvrage [Rou22].

5. C'est un pléonasme. Les éléments de $\mathbb{C}[X]$ sont précisément les polynômes à coefficients complexes.

(a) Étant donné un élément x quelconque non nul de $\mathbb{C}^p$ on pose [6]

$$\mu = \min\{r \geqslant 1 \mid \text{ la famille } (x, MX, \dots, M^r x) \text{ est liée dans } \mathbb{C}^p\}.$$

i. Montrer qu'il existe un élément $(\alpha_0, \dots, \alpha_{\mu-1})$ de $\mathbb{C}^\mu$ et une matrice N de $\mathscr{M}_{p-\mu}(\mathbb{C})$ tels que la matrice M soit semblable à une matrice M' de la forme suivante :

$$M' = \begin{pmatrix} 0 & \dots & \dots & 0 & -\alpha_0 & \star \\ 1 & \ddots & & \vdots & -\alpha_1 & \star \\ 0 & 1 & \ddots & \vdots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & -\alpha_{\mu-3} & \star \\ \vdots & & \ddots & 1 & -\alpha_{\mu-2} & \star \\ 0 & \dots & \dots & 0 & -\alpha_{\mu-1} & \star \\ O & \dots & \dots & O & O & N \end{pmatrix}$$

où les $\star$ représentent des lignes d'éléments de $\mathbb{C}$ et les O représentent des colonnes nulles.

ii. Montrer que $\chi_M(M)x = 0$.

(b) Montrer que χ_M est un polynôme annulateur de M.

Corrigé

Vrai-Faux

1. (a) C'est faux. Si on note $M = (m_{ij})_{1\leqslant i,j\leqslant n}$ et $N = (n_{ij})_{1\leqslant i,j\leqslant n}$ deux matrices de $\mathscr{M}_n(\mathbb{C})$ alors

$$MN = \left(\sum_{k=1}^{n} m_{ik}n_{kj}\right)_{1\leqslant i,j\leqslant n} \quad \text{et} \quad NM = \left(\sum_{k=1}^{n} n_{ik}m_{kj}\right)_{1\leqslant i,j\leqslant n}.$$

6. Nous corrigeons ici une erreur manifeste dans l'énoncé original, qui indiquait malheureusement $\mu = \min\{r \geqslant 1 \mid \text{ la famille } \{x, MX, \dots, M^r x\} \text{ est liée dans } \mathbb{C}^p\}$. Le diable se niche dans les détails : $\{x, MX, \dots, M^r x\}$ désigne non pas une *famille* mais un *ensemble*. La nuance est de taille. Si par exemple, $Mx = x$ pour un certain $x \neq 0$, alors l'ensemble $\{x, Mx\}$ est égal au singleton $\{x\}$ et on ne peut pas considérer qu'on est en présence d'une partie de $\mathbb{C}^p$ composée de vecteurs linéairement dépendants. En revanche, la famille (x, Mx) est bien liée par la relation de dépendance linéaire $x - Mx = 0$.

Leurs traces sont donc bien égales car d'une part

$$\mathrm{Tr}(MN) = \sum_{i=1}^{n}\sum_{k=1}^{n} m_{ik}n_{ki}$$

et d'autre part, par associativité et commutativité de la somme (on permute les deux symboles $\sum$) et par commutativité du produit (on permute n_{ik} et m_{ki})

$$\begin{aligned}\mathrm{Tr}(NM) &= \sum_{i=1}^{n}\sum_{k=1}^{n} n_{ik}m_{ki}\\ &= \sum_{k=1}^{n}\sum_{i=1}^{n} m_{ki}n_{ik}\\ &= \sum_{i=1}^{n}\sum_{k=1}^{n} m_{ik}n_{ki}.\end{aligned}$$

La dernière égalité est un simple changement de notation des paramètres : les variables i et k étant muettes, on peut changer tous les i par des k et vice versa.

(b) C'est vrai et il suffit de savoir montrer que le polynôme caractéristique d'une matrice $M \in \mathscr{M}_2(\mathbb{C})$ est $X^2 - \mathrm{Tr}(M)X + \det(M)$. En notant $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ pour quatre nombres complexes a, b, c, d, on a en effet $\mathrm{Tr}(M) = a + d$ et $\det(M) = ad - bc$. Comme

$$XI_2 - M = \begin{pmatrix} X - a & -b \\ -c & X - d \end{pmatrix},$$

on a alors

$$\begin{aligned}\chi_M(X) &= \det(XI_2 - M)\\ &= (X - a)(X - d) - (-b)(-c)\\ &= X^2 - (a + d)X + ad - bc\\ &= X^2 - \mathrm{Tr}(M)X + \det(M).\end{aligned}$$

On voit donc que le polynôme caractéristique d'une matrice est entièrement déterminé par sa trace et son déterminant : deux matrices de $\mathscr{M}_2(\mathbb{C})$ ont donc même polynôme caractéristique ssi elles ont même trace et même déterminant.

Remarque. On ne peut pas généraliser cette propriété à $\mathscr{M}_n(\mathbb{C})$ pour $n \geqslant 3$. Un contre-exemple minimal est fourni par la matrice nulle et la matrice diagonale $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ qui sont toutes deux de trace nulle et de déterminant nul mais dont les polynômes caractéristiques sont respectivement X^3 et $X^3 - X$.

(c) C'est faux et le contre-exemple minimal classique à connaître est donné par

$$M = \begin{pmatrix} i & 1 \\ 1 & -i \end{pmatrix}.$$

Il répond aux critères suivants :

— M est carrée et symétrique,

— M est à coefficients dans $\mathbb{C}$,

— le polynôme caractéristique de M est

$$\det(XI_2 - M) = (X - i)(X + i) - (-1)^2 = X^2,$$

et son unique valeur propre est $\lambda = 0$.

Or, la seule matrice diagonalisable n'ayant qu'une valeur propre λ est la matrice λI_2 (c'est-à-dire ici la matrice nulle). M n'étant pas nulle, elle n'est donc pas diagonalisable.

Remarque. le piège de cette question réside dans le fait que les affirmations suivantes (il s'agit du théorème spectral dans les cas réel et complexe) sont vraies :

— les matrices carrées symétriques réelles (c'est-à-dire égales à leur transposée) sont diagonalisables dans $\mathbb{R}$,

— les matrices carrées complexes et dont la transposée est égale au conjugué (c'est-à-dire vérifiant $M^T = \overline{M}$ ou encore égales à leur transconjugué $\overline{M}^T$) sont diagonalisables dans $\mathbb{C}$ et de plus leurs valeurs propres sont toutes réelles.

(d) C'est évidemment faux et il ne faut pas chercher loin, en considérant par exemple le plongement d'un anneau commutatif unitaire intègre quelconque A qui n'est pas un corps dans son corps des fractions B. Le plus simple est ainsi de considérer le morphisme d'anneaux $\varphi : \mathbb{Z} \to \mathbb{Q}$ défini par

$$\forall\, n \in \mathbb{Z}, \quad \varphi(n) = n.$$

Ainsi, pour tout $n \in \mathbb{Z}^*$, $\varphi(n) = n \neq 0$ est bien inversible dans $\mathbb{Q}$, d'inverse $\dfrac{1}{n} \in \mathbb{Q}$, alors que, si on prend rien que $n = 2$, on est bien en présence d'un élément qui n'est pas inversible dans $\mathbb{Z}$ (au même titre que tout autre n différent de ± 1).

Exercice préliminaire

2. Pour un entier $d \geqslant 1$ donné, on a

$$XI_d - C_P = \begin{pmatrix} X & 0 & \dots & \dots & 0 & a_0 \\ -1 & X & \ddots & & \vdots & a_1 \\ 0 & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & -1 & X & a_{d-2} \\ 0 & \dots & \dots & 0 & -1 & X + a_{d-1} \end{pmatrix}.$$

Remarque. Si on peine à se convaincre de ce qu'il faut écrire pour le cas $d = 1$ (voir l'initialisation donnée un peu plus bas), on peut dans un premier temps écrire le cas $d = 3$ puis le cas $d = 2$, ce qui permet de mieux comprendre la dynamique d'épuisement de l'expression de C_P quand d est de plus en plus petit. Il n'est en effet pas évident de saisir du premier coup que pour $d = 1$, il n'y a ni 0 ni -1 à écrire dans la matrice C_P.

Si $d = 3$ et $P = X^3 + a_2X^2 + a_1X + a_0 \in \mathbb{C}[X]$, on a $C_P = \begin{pmatrix} 0 & 0 & -a_0 \\ 1 & 0 & -a_1 \\ 0 & 1 & -a_2 \end{pmatrix}$ et

$$\begin{aligned} \chi_{C_P} &= \begin{vmatrix} X & 0 & a_0 \\ -1 & X & a_1 \\ 0 & -1 & X + a_2 \end{vmatrix} \\ &= X\Big((X(X + a_2) - (-1)a_1\Big) + a_0(-1)^2 \\ &= X^3 + a_2X^2 + a_1X + a_0 \\ &= P(X). \end{aligned}$$

La proposition P_3 est donc vraie.

Si $d = 2$ et $P = X^2 + a_1X + a_0 \in \mathbb{C}[X]$, on a $C_P = \begin{pmatrix} 0 & -a_0 \\ 1 & -a_1 \end{pmatrix}$ et

$$\begin{aligned} \chi_{C_P} &= \begin{vmatrix} X & a_0 \\ -1 & X + a_1 \end{vmatrix} \\ &= X(X + a_1) - (-1)a_0 \\ &= X^2 + a_1X + a_0 \\ &= P(X). \end{aligned}$$

La proposition P_2 est donc vraie.

En considérant $d \geqslant 2$ (car pour $d = 1$ il n'y a rien à faire) et en développant par rapport à la première ligne, on obtient une somme de deux déterminants de taille $d - 1$ (tous les autres termes du développement sont nuls). Le premier est similaire au déterminant initial et le second est triangulaire supérieur donc d'un calcul immédiat (il est égal au produit de ses termes diagonaux) :

$$\det(XI_d - C_P) = (-1)^{1+1}X \begin{vmatrix} X & 0 & \dots & \dots & 0 & a_1 \\ -1 & X & \ddots & & \vdots & a_2 \\ 0 & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & \vdots \\ \vdots & & \ddots & -1 & X & a_{d-2} \\ 0 & \dots & \dots & 0 & -1 & X + a_{d-1} \end{vmatrix}$$

$$+ (-1)^{1+d}a_0 \underbrace{\begin{vmatrix} -1 & X & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & X \\ 0 & \dots & \dots & 0 & -1 \end{vmatrix}}_{=(-1)^{d-1}}.$$

On a donc

$$\det(XI_d - C_P) = X \det(XI_d - C_Q) + a_0$$

où Q est le polynôme complexe de degré $d - 1$ défini par

$$Q(X) = X^{d-1} + a_{d-1}X^{d-2} + \cdots + a_2X + a_1.$$

On peut alors montrer par récurrence le prédicat P_d, dépendant du paramètre $d \in \mathbb{N}^*$ et défini par :
P_d : *tout polynôme du type*

$$P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0 \in \mathbb{C}[X]$$

est le polynôme caractéristique de sa matrice compagnon $C_{_P}$.

Initialisation : si $d = 1$ et $P(X) = X + a_0 \in \mathbb{C}[X]$, alors $C_{_P} = \Big(-a_0\Big)$ et $\chi_{C_{_P}} = \Big|X + a_0\Big| = X + a_0 = P(X)$. La proposition P_1 est donc vraie.

Hypothèse de récurrence : supposons que P_{d-1} est vraie pour un certain entier $d \geqslant 2$ (c'est-à-dire $d - 1 \geqslant 1$).

Hérédité : soit $P(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_0 \in \mathbb{C}[X]$. On a vu plus haut que

$$\det(XI_d - C_{_P}) = X\det(XI_d - C_{_Q}) + a_0$$

où Q est le polynôme défini par

$$Q(X) = X^{d-1} + a_{d-1}X^{d-2} + \cdots + a_2X + a_1 \in \mathbb{C}[X].$$

L'hypothèse de récurrence appliquée à $Q(X)$ nous permet d'affirmer que

$$\det(XI_d - C_{_Q}) = Q(X).$$

On a alors

$$\begin{aligned}\det(XI_d - C_{_P}) &= XQ(X) + a_0\\ &= X\Big(X^{d-1} + a_{d-1}X^{d-2} + \cdots + a_2X + a_1\Big) + a_0\\ &= X^d + a_{d-1}X^{d-1} + \cdots + a_2X^2 + a_1X + a_0\\ &= P(X).\end{aligned}$$

Nous venons de montrer le caractère héréditaire du prédicat P_d, c'est-à-dire que pour tout entier $d \geqslant 2$, on a l'implication

$$P_{d-1} \Rightarrow P_d.$$

Conclusion : la proposition P_1 est vraie et le prédicat P_d est héréditaire, donc P_d est vraie pour tout $d \in \mathbb{N}^*$.

3. (a) i.

Remarque. Tout d'abord, et bien que cela ne soit pas demandé, on peut noter que l'entier μ est bien défini. En effet, l'ensemble

$$\{r \geqslant 1 \,|\, \text{ la famille } (x, MX, \dots, M^r x) \text{ est liée dans } \mathbb{C}^p\}$$

est une partie non vide de $\mathbb{N}^*$ car la famille $(x, Mx, \dots, M^p x)$, constituée de $p+1$ vecteurs, est nécessairement liée dans le $\mathbb{C}$-espace vectoriel $\mathbb{C}^p$ de dimension p. On sait ainsi que p est un élément de cet ensemble. Toute partie non vide de $\mathbb{N}$ admettant un minimum, l'existence de μ est assurée. On a de plus $1 \leqslant \mu \leqslant p$.

La lecture préalable des questions ii. et (b) permet de comprendre qu'il ne faut pas chercher à utiliser le théorème de Cayley-Hamilton pour répondre à la question i. (la question (b) consiste précisément à conclure que ce théorème est alors démontré).

Par définition, dans $\mathbb{C}^p$, la famille de vecteurs $(x, Mx, \dots, M^{\mu-1}x)$ est libre alors que la famille de vecteurs $(x, Mx, \dots, M^{\mu}x)$ est liée. En conséquence, on peut affirmer que $M^\mu x$ s'exprime comme une combinaison linéaire de $x, Mx, \dots, M^{\mu-1}x$. Il faut cependant le démontrer [7] : il existe des complexes $\beta_0, \dots, \beta_{\mu-1}, \beta_\mu$ non tous nuls tels que

$$\beta_0 x + \beta_1 Mx + \cdots + \beta_{\mu-1} M^{\mu-1}x + \beta_\mu M^\mu x = 0.$$

Il est impossible que $\beta_\mu = 0$ car dans ce cas les complexes $\beta_0, \dots, \beta_{\mu-1}$ seraient non tous nuls et la famille $(x, Mx, \dots, M^{\mu-1}x)$ serait liée, ce qui est faux par hypothèse. On peut donc diviser par β_μ, isoler $M^\mu x$ et affirmer qu'il existe des complexes $\alpha_0 = \dfrac{\beta_0}{\beta_\mu}, \dots, \alpha_{\mu-1} = \dfrac{\beta_{\mu-1}}{\beta_\mu}$ non tous nuls tels que

$$M^\mu x = -\alpha_0 x - \alpha_1 Mx - \cdots - \alpha_{\mu-1} M^{\mu-1}x.$$

Le théorème de la base incomplète nous permet de compléter la famille libre $(x, Mx, \dots, M^{\mu-1}x)$ en une base $\mathbf{b}$ du $\mathbb{C}$-espace vectoriel $\mathbb{C}^p$ (dans un espace vectoriel de dimension finie, toute famille libre peut-être complétée en une base de cet espace). Il est alors immédiat que l'endomorphisme canoniquement associé à la matrice M (c'est-à-dire l'application inéaire qui à tout $y \in \mathbb{C}^p$ associe $My \in \mathbb{C}^p$) admet, vis-à-vis de la base $\mathbf{b}$, une matrice de la forme M'. En effet, l'image du premier vecteur de

7. La question 2. de l'exercice 1 de l'épreuve interne de 2023 traite de maière plus générale cette question, voir page 39 du présent ouvrage.

b, x, est Mx, l'image du second, Mx, est M^2x et ainsi de suite, l'image de $M^{\mu-2}x$ est $M^{\mu-1}x$. Enfin, l'image de $M^{\mu-1}x$ est

$$M^\mu x = -\alpha_0 x - \alpha_1 Mx - \cdots - \alpha_{\mu-1} xM^{\mu-1}.$$

Les images des vecteurs suivants de la base **b** s'expriment de manière quelconque dans cette base : leurs coordonnées dans **b** sont cachées dans les $\star$ et dans la matrice N.
M et M' sont donc les matrices d'un même endomorphisme, exprimées respectivement dans la base canonique et dans la base **b** de $\mathbb{C}^p$. M et M' sont donc semblables.

ii. En considéront le polynôme

$$P(X) = X^\mu + \alpha_{\mu-1}X^{\mu-1} + \cdots + \alpha_1 X + \alpha_0.$$

La matrice M' étant triangulaire supérieure par blocs et les deux blocs qui composent sa diagonale étant les matrices carrées $C_{_P}$ et N , on a $\chi_{_{M'}} = \chi_{_{C_P}}\chi_{_N}$ ce que l'on peut aussi écrire sous la forme

$$\chi_{_{C_P}} \,\Big|\, \chi_{_{M'}}.$$

De plus,

$$\chi_{_{M'}} = \chi_{_M}$$

car le polynôme caractéristique d'un endomorphisme est un invariant de similitude : deux matrices semblables M et M' ont même polynôme caractéristique. Ainsi, en utilisant le résultat de la question 2. , on a

$$\chi_{_M} = \chi_{_{M'}} = \chi_{_{C_P}}\chi_{_N} = \chi_{_N} P.$$

Enfin, on a

$$\begin{aligned} P(M)x &= \Big(M^\mu + \sum_{k=0}^{\mu-1} \alpha_k M^k\Big)x \\ &= M^\mu x + \alpha_{\mu-1}M^{\mu-1}x + \cdots + \alpha_1 Mx + \alpha_0 x \\ &= 0 \end{aligned}$$

d'après la définition des scalaires $\alpha_0, \ldots, \alpha_{\mu-1}$. On peut donc écrire

$$\chi_{_M}(M)x = (\chi_{_N}P)(M)x = (\chi_{_N}(M)\cdot P(M))\,x = (\chi_{_N}(M)\cdot 0)\,x = 0.$$

(b) Le résultat obtenu à l'instant est valable pour tout élément non nul x de $\mathbb{C}^p$ (il est également vrai quand x est le vecteur nul de $\mathbb{C}^p$). L'endomorphisme canoniquement associé à la matrice $\chi_{_M}(M)$ est donc l'endomorphisme nul et en conséquence, $\chi_{_M}(M)$ est la matrice nulle, ce qui signifie que $\chi_{_M}$ est un polynôme annulateur de M. Nous venons ainsi, dans cet exercice, de démontrer le théorème de Cayley-Hamilton.

1.4 2023, vrai-faux et exercices préliminaires

Vrai-Faux

Thèmes

structures algébriques (groupe, groupe quotient, anneau, anneau quotient, corps, groupe multiplicatif d'un corps, groupe des éléments inversibles d'un anneau, morphisme d'anneaux)
arithmétique (nombres premiers, premiers entre eux, congruence)
matrices (inversibles)

Résultat majeur

$\mathbb{Z}/n\mathbb{Z}$ **est un corps ssi** n **est premier**

Remarques

Des propriétés usuelles des anneaux $\mathbb{Z}/n\mathbb{Z}$*, plusieurs questions ne nécessitent que les cas où* $n = 4$*,* 5 *ou* 9*. On a 1.(b)* $\Rightarrow$ *1.(c). 1.(e) Ne pas chercher un contre-exemple avec* $\mathbb{Z}$ *ou* $\mathrm{GL}_2(\mathbb{Z})$ *qui ne sont pas des corps, ou avec une application de* $\mathbb{Z}/2\mathbb{Z}$ *dans* $\mathbb{Z}/3\mathbb{Z}$ *qui n'est pas un morphisme.*

Énoncé

1. Les affirmations suivantes sont-elles vraies ou fausses ? On justifiera soigneusement les réponses.

   (a) Affirmation : « Pour tout nombre premier p et pour tout entier naturel n non nul, l'anneau $(\mathbb{Z}/p^n\mathbb{Z}, +, \cdot)$ est un corps ».

   (b) Affirmation : « Si p est un nombre premier impair, alors la classe de 2 engendre le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/p^n\mathbb{Z}, +, \cdot)$ ».

   (c) Affirmation : « Le groupe multiplicatif des éléments inversibles de l'anneau $(\mathbb{Z}/9\mathbb{Z}, +, \cdot)$ est cyclique. »

(d) Si a est un entier relatif, alors on note $\overline{a}$ la classe de a dans $\mathbb{Z}/5\mathbb{Z}$. Étant donnés quatre entiers relatifs a, b, c et d, on note M la matrice de $\mathscr{M}_2(\mathbb{Z})$ définie par $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et on note $\overline{M}$ la matrice de $\mathscr{M}_2(\mathbb{Z}/5\mathbb{Z})$ définie par $\overline{M} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$.

Affirmation : « Si $M \in \mathrm{GL}_2(\mathbb{R})$, alors $\overline{M} \in \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$. »

(e) Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps commutatifs.

Affirmation : « Un morphisme d'anneaux $\mu : \mathbb{K} \to \mathbb{L}$ est toujours injectif. »

Corrigé

1. (a) C'est évidemment faux et ce ne sont pas les contre-exemples qui manquent : on peut se contenter de poser $p = n = 2$ (et donc $p^n = 4$) et constater, si besoin en dressant la Table 1.1 de multiplication de l'anneau $(\mathbb{Z}/4\mathbb{Z}, +, \cdot)$, que l'élément $\overline{2} \neq \overline{0}$ ne possède pas d'inverse. $\mathbb{Z}/4\mathbb{Z}$ n'est donc pas un corps (pire que ça : ce n'est même pas un anneau intègre). Plus généralement, pour tout nombre premier p et tout $n \geqslant 2$, l'anneau $(\mathbb{Z}/p^n\mathbb{Z}, +, \cdot)$ n'est pas intègre. Il possède en effet des diviseurs de zéro. On a par exemple $\overline{p} \neq \overline{0}$ et $\overline{p^{n-1}} \neq \overline{0}$ mais $\overline{p} \times \overline{p^{n-1}} = \overline{p^n} = \overline{0}$. Rappelons qu'un corps est nécessairement un anneau intègre et qu'aucun diviseur de zéro n'est inversible.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Table 1.1 – Multiplication dans $\mathbb{Z}/4\mathbb{Z}$.

On peut aussi évoquer le fait que dans un anneau du type $\mathbb{Z}/m\mathbb{Z}$ pour un entier $m \geqslant 2$, les éléments inversibles sont les classes des entiers k premiers avec m. Dès que m n'est pas premier, on peut l'écrire sous la forme $m_1 m_2$ avec $1 < m_1 < m$ et $1 < m_2 < m$: les classes $\overline{m_1} \neq \overline{0}$ et $\overline{m_2} \neq \overline{0}$ sont des diviseurs de zéro (leur produit est nul) et en conséquence ne sont pas inversibles.

(b) Ce serait trop beau. Il ne faut pas chercher bien loin pour voir que la classe de 2 dans $\mathbb{Z}/7\mathbb{Z}$ n'engendre que les classes

$$\overline{2}^1 = \overline{2}, \quad \overline{2}^2 = \overline{4} \quad \text{et} \quad \overline{2}^3 = \overline{8} = \overline{7+1} = \overline{1}.$$

Les puissances suivantes $\overline{2}^k$ pour $k \geqslant 4$ donnent ces trois mêmes résultats cycliquement. $\overline{2}$ n'engendre pas les classes de 3, 5 et 6 qui sont pourtant inversibles :

$$\overline{3} \times \overline{5} = \overline{15} = \overline{7 \times 2 + 1} = \overline{1}$$

et

$$\overline{6}^2 = \overline{36} = \overline{7 \times 5 + 1} = \overline{1}.$$

On peut aussi, de manière un peu plus originale, constater que quand $\overline{2}$ est un carré de l'anneau $\mathbb{Z}/p\mathbb{Z}$, il n'engendre que des carrés. On peut alors évoquer le fait que quand $p \equiv 3[4]$, $\overline{-1}$ n'est jamais un carré (ce qui constitue un résultat associé à la loi de réciprocité quadratique) et ne sera donc pas engendré par $\overline{2}$. Pour $p = 7$, on a en effet $\overline{3}^2 = \overline{9} = \overline{7+2} = \overline{2}$. Là encore, si besoin, on peut dresser la Table 1.2 de multiplication dans $\mathbb{Z}/7\mathbb{Z}$.

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{1}$	$\overline{3}$	$\overline{5}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{2}$	$\overline{5}$	$\overline{1}$	$\overline{4}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{1}$	$\overline{5}$	$\overline{2}$	$\overline{6}$	$\overline{3}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{3}$	$\overline{1}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Table 1.2 – Multiplication dans $\mathbb{Z}/7\mathbb{Z}$.

(c) C'est vrai. Le groupe des éléments inversibles de $\mathbb{Z}/9\mathbb{Z}$ est

$$(\mathbb{Z}/9\mathbb{Z})^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}.$$

Il est engendré par $\overline{2}$. Seules les classes de 0, 3 et 6 ne sont pas inversibles car 0, 3 et 6 ne sont pas premiers avec 9. La Table 1.3 est convaincante : on y voit apparaître les six éléments inversibles de l'anneau $(\mathbb{Z}/9\mathbb{Z}, +, \cdot)$.

k	1	2	3	4	5	6
$\overline{2}^k$	$\overline{2}$	$\overline{4}$	$\overline{8}$	$\overline{7}$	$\overline{5}$	$\overline{1}$

TABLE 1.3 – Puissances de 2 dans $\mathbb{Z}/9\mathbb{Z}$.

(d) C'est faux. Il suffit de trouver une matrice M à coefficients entiers dont le déterminant est 5 (ou plus généralement un multiple de 5). La matrice $\overline{M}$ associée sera alors de déterminant $\overline{5} = \overline{0}$. Encore une fois, pas besoin de chercher bien loin. Il suffit de poser

$$M = \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$$

M est bien dans $\mathrm{GL}_2(\mathbb{R})$ et

$$M^{-1} = \begin{pmatrix} 1/5 & 0 \\ 0 & 1 \end{pmatrix}$$

mais

$$\overline{M} = \begin{pmatrix} \overline{0} & \overline{0} \\ \overline{0} & \overline{1} \end{pmatrix}$$

n'est pas dans $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$.

Remarque. Une matrice à coefficients dans un anneau est inversible ssi son déterminant est un élément inversible de cet anneau. En particulier, si l'anneau est un corps (c'est le cas de $\mathbb{Z}/5\mathbb{Z}$), une matrice est inversible si et seulement si son déterminant est non nul.

Remarque. Si l'énoncé avait indiqué $M \in \mathrm{GL}_2(\mathbb{Z})$ au lieu de $\mathrm{GL}_2(\mathbb{R})$, l'affirmation aurait alors été vraie. En effet, une matrice M de $\mathrm{GL}_2(\mathbb{Z})$ a un déterminant égal à ± 1 (ce sont les deux seuls éléments inversibles de l'anneau $\mathbb{Z}$) et la matrice $\overline{M}$ a alors un déterminant égal à $\pm\overline{1}$ et elle est bien également inversible.
Dans le cas particulier qui nous occupe, on a de manière générale

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

à condition bien sûr que $ad - bc \neq 0$. On a le résultat similaire avec $\overline{ad-bc} \neq \overline{0}$ dans $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$. En revanche, dans $\mathrm{GL}_2(\mathbb{Z})$, la condition serait $ad - bc = \pm 1$

(e) C'est vrai. Le noyau $\mathrm{Ker}(\mu) = \mu^{-1}(\{0_{\mathbb{L}}\})$ d'un tel morphisme μ est un idéal de l'anneau $\mathbb{K}$. $\mathbb{K}$ étant un corps, ses seuls idéaux sont $\{0_{\mathbb{K}}\}$ et $\mathbb{K}$ lui-même. Puisqu'un morphisme d'anneaux conserve l'élément unité (c'est-à-dire $\mu(1_{\mathbb{K}}) = 1_{\mathbb{L}}$), on a alors $1_{\mathbb{K}} \notin \mathrm{Ker}(\mu)$, donc $\mathrm{Ker}(\mu) \neq \mathbb{K}$ et finalement $\mathrm{Ker}(\mu) = \{0_{\mathbb{K}}\}$. μ est donc bien injectif.

Remarque. Un morphisme de groupes (ou d'anneaux, ou de corps ou encore d'algèbres) est injectif ssi son noyau est réduit à $\{0\}$.

Exercice 1

Thèmes

matrices (semblables, diagonales, diagonalisables, inversibles, nilpotentes, classes de similitude, valeurs propres, $\mathrm{GL}_n(\mathbb{K})$)
espaces vectoriels (famille libre, combinaison linéaire, nombre d'éléments dans le cas d'un corps de base fini)

Résultat majeur

cardinal de $\mathrm{GL}_n(\mathbb{K})$

Remarques

Pour une famille liée, il existe des coefficients non tous nuls tels que la combinaison linéaire soit nulle mais certains coefficients peuvent être nuls. C'est la liberté d'une famille de k vecteurs qui implique que le sous-espace qu'elle engendre est de cardinal p^k.

Énoncé

Soit p un nombre premier, on désigne par $\mathbb{K}$ le corps $\mathbb{Z}/p\mathbb{Z}$.

2. Soit E un $\mathbb{K}$-espace vectoriel et soit k un entier strictement positif. Notons $(x_1, \ldots, x_{k+1})$ une famille constituée de $k+1$ vecteurs de E telle que la famille $(x_1, \ldots, x_k)$ est libre.

Montrer que la famille de vecteurs $(x_1, \ldots, x_{k+1})$ est libre si et seulement si le vecteur x_{k+1} n'est pas combinaison linéaire des vecteurs $x_1, \ldots, x_k$.

3. Soit n et k deux entiers strictement positifs vérifiant la relation $k \leqslant n$. Montrer par récurrence que le nombre de familles libres constituées de k vecteurs de $\mathbb{K}^n$ vaut $(p^n - 1)(p^n - p) \ldots \left(p^n - p^{k-1}\right)$.
4. Soit n un entier strictement positif. Déterminer le cardinal de $\mathrm{GL}_n(\mathbb{K})$.

Corrigé

2. Cette première question n'est pas spécifique au corps $\mathbb{Z}/p\mathbb{Z}$ et peut être résolue en se plaçant dans un corps $\mathbb{K}$ quelconque. On peut traiter cette question en parlant 1) de fastidieuses combinaisons linéaires ou 2) de lourdes dimensions d'espaces vectoriels.

   Première méthode : nous allons raisonner par contraposée et démontrer l'équivalence

   x_{k+1} est combinaison linéaire de $x_1, \ldots, x_k \iff (x_1, \ldots, x_{k+1})$ est liée.

   — *Implication directe* ($\Rightarrow$). Supposons que x_{k+1} est combinaison linéaire des $x_1, \ldots, x_k$ alors

   $$\exists (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k, x_{k+1} = \sum_{i=1}^{k} \lambda_i x_i.$$

   En posant $\lambda_{k+1} = -1$, on a alors

   $$\sum_{i=1}^{k+1} \lambda_i x_i = 0 \quad \text{avec} \quad (\lambda_1, \ldots, \lambda_{k+1}) \neq (0, \ldots, 0),$$

   ce qui prouve que la famille $(x_1, \ldots, x_{k+1})$ est liée.

   — *Implication réciproque* ($\Leftarrow$). Supposons que la famille $(x_1, \ldots, x_{k+1})$ est liée. Il existe donc $(\lambda_1, \ldots, \lambda_{k+1}) \in \mathbb{K}^{k+1}$ tel que

   $$(\lambda_1, \ldots, \lambda_{k+1}) \neq (0, \ldots, 0) \quad \text{et} \quad \sum_{i=1}^{k+1} \lambda_i x_i = 0.$$

   Si $\lambda_{k+1} = 0$ alors

   $$\sum_{i=1}^{k} \lambda_i x_i = 0 \quad \text{avec} \quad (\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k, (\lambda_1, \ldots, \lambda_k) \neq (0, \ldots, 0),$$

ce qui contredit le fait que la famille $(x_1, \ldots, x_k)$ est libre. On a donc $\lambda_{k+1} \neq 0$ et on peut alors écrire

$$x_{k+1} = \sum_{i=1}^{k} -\frac{\lambda_i}{\lambda_{k+1}} x_i.$$

Le vecteur x_{k+1} est donc une combinaison linéaire des vecteurs $x_1, \ldots, x_k$.

Deuxième méthode : par hypothèse $(x_1, \ldots, x_k)$ est libre, donc

$$\dim\left(\text{Vect}(x_1, \ldots, x_k)\right) = k.$$

— *Implication directe* ($\Rightarrow$). Supposons que $(x_1, \ldots, x_{k+1})$ est libre.
On a alors $\dim\left(\text{Vect}(x_1, \ldots, x_{k+1})\right) = k + 1$
Si x_{k+1} est combinaison linéaire des vecteurs $x_1, \ldots, x_k$, alors x_{k+1} est dans $\text{Vect}(x_1, \ldots, x_k)$ et alors

$$\text{Vect}(x_1, \ldots, x_{k+1}) = \text{Vect}(x_1, \ldots, x_k),$$

ce qui est absurde : deux sous-espaces de dimensions respectives $k+1$ et k ne peuvent pas être égaux. x_{k+1} n'est donc pas combinaison linéaire des vecteurs $x_1, \ldots, x_k$.

— *Implication réciproque* ($\Leftarrow$). Supposons que x_{k+1} n'est pas combinaison linéaire des $x_1, \ldots, x_k$. En particulier, $x_{k+1} \neq 0$ (le vecteur nul est toujours combinaison linéaire de toute famille non vide de vecteurs, $0 = 0x_1 + \cdots + 0x_k$) : x_{k+1} engendre donc un sous-espace vectoriel de dimension 1 dont l'intersection avec le sous-espace engendré par $x_1, \ldots, x_k$ est réduite au vecteur nul et on a alors

$$\text{Vect}(x_1, \ldots, x_k) \oplus \text{Vect}(x_{k+1}) = \text{Vect}(x_1, \ldots, x_{k+1}).$$

On en déduit

$$\begin{aligned}\dim\left(\text{Vect}(x_1, \ldots, x_{k+1})\right) &= \dim\Big(\text{Vect}(x_1, \ldots, x_k) \oplus \text{Vect}(x_{k+1})\Big) \\ &= \dim\left(\text{Vect}(x_1, \ldots, x_k)\right) + \dim(\text{Vect}(x_{k+1})) \\ &= k + 1,\end{aligned}$$

ce qui permet de déduire que la famille $(x_1, \ldots, x_{k+1})$ est libre.

3. Fixons $n > 0$ et procédons par récurrence finie sur k dans $[\![1, n]\!]$.
On notera P_k le prédicat

P_k : le nombre de familles libres constituées de k vecteurs de $\mathbb{K}^n$ vaut $(p^n-1)(p^n-p)\dots(p^n-p^{k-1})$.

Initialisation : il est clair que P_1 est vraie : (x_1) est libre si et seulement si $x_1 \neq 0$. $\mathbb{K}^n\backslash\{(0,\dots,0)\}$ ayant p^n-1 éléments (tous les éléments de $\mathbb{K}^n$ sauf un), le nombre de familles libres constituées d'un seul vecteur est égal à p^n-1.

Hérédité : supposons que pour un entier k tel que $1 \leqslant k < n$, le nombre de familles libres de k vecteurs de $\mathbb{K}^n$ est $(p^n-1)(p^n-p)\dots(p^n-p^{k-1})$. La question 2. a permis de voir qu'une famille libre $(x_1,\dots,x_{k+1})$ de $k+1$ vecteurs de $\mathbb{K}^n$ peut être vue comme une famille libre $(x_1,\dots,x_k)$ de k vecteurs à laquelle on a adjoint un $(k+1)$-ième vecteur x_{k+1} linéairement indépendant des k premiers, c'est-à-dire n'appartenant pas à $\text{Vect}(x_1,\dots,x_k)$. Ce sous-espace vectoriel étant de cardinal p^k, cela laisse exactement p^n-p^k possibilités pour x_{k+1} (chaque vecteur qui n'est pas dans $\text{Vect}(x_1,\dots,x_k)$ est acceptable).
Par produit, on en déduit que le nombre de famille libres de $k+1$ vecteurs de $\mathbb{K}^n$ est $(p^n-1)(p^n-p)\dots(p^n-p^{k-1})(p^n-p^k)$, ce qui prouve que la propriété à démontrer est héréditaire :

$$(0 < k < n \quad \text{et} \quad P_k) \implies P_{k+1}.$$

Conclusion : d'après le principe de récurrence (finie) la propriété est valable pour tout entier $k > 0$ tel que $k \leqslant n$.

4. On peut identifier une matrice de $\text{GL}_n(\mathbb{K})$ à une famille libre de n vecteurs de $\mathbb{K}^n$: celle de ses n vecteurs colonnes (ou celle de ses n vecteurs lignes). Le cardinal de $\text{GL}_n(\mathbb{K})$ est donc le nombre de familles libres de n vecteurs de $\mathbb{K}^n$, c'est-à-dire

$$(p^n-1)(p^n-p)\dots(p^n-p^{n-1}) = \prod_{i=0}^{n-1}(p^n-p^i).$$

Exercice 2

Thèmes

arithmétique (nombre premier, diviseurs, coefficients de Bézout, décomposition en produit de facteurs premiers)
corps (finis, groupe des éléments inversibles)
groupes (finis, générateur, ordre, groupe cyclique)

Résultats majeurs

propriétés de l'indicatrice d'EULER
théorème de BÉZOUT
théorème fondamental de l'arithmétique

Remarques

5.(b) la bonne définition de P ne dépend pas du fait que m_1 et m_2 sont premiers entre eux. Le théorème chinois ne donne pas la bijectivité. Il faut prouver l'égalité des cardinaux des ensembles. Évoquer la « dimension » des ensembles est absurde. 5.(d) Il est nécessaire de généraliser la question 5.(c) avant de l'utiliser.

Énoncé

5. Soit n un entier naturel. On note $\mathscr{D}_n$ l'ensemble des entiers naturels qui divisent n. On souhaite montrer que pour tout entier n strictement positif on a l'égalité $n = \sum_{d\in\mathscr{D}_n} \varphi(d)$. On pose $f(n) = \sum_{d\in\mathscr{D}_n} \varphi(d)$.

   (a) Soit p un nombre premier. Pour tout entier i, calculer $\varphi\left(p^i\right)$. En déduire la valeur $f\left(p^k\right)$ pour tout entier k strictement positif.

   (b) Soit m_1 et m_2 deux entiers naturels premiers entre eux. Montrer que l'application

$$P : \begin{array}{c} \mathscr{D}_{m_1} \times \mathscr{D}_{m_2} \to \mathscr{D}_{m_1 m_2} \\ (\, d_1 \,,\, d_2 \,) \mapsto d_1 d_2 \end{array}$$

   est bien définie et qu'elle est bijective.

   (c) En déduire que lorsque m_1 et m_2 sont deux entiers naturels premiers entre eux on a la relation $f(m_1)f(m_2) = f(m_1 m_2)$.

   (d) Montrer que pour tout entier n strictement positif on a l'égalité

$$n = \sum_{d\in\mathscr{D}_n} \varphi(d).$$

6. Soit $(\mathbb{K}, +, \cdot)$ un corps de cardinal fini égal à $c+1$. On a $\mathbb{K}^* = \mathbb{K}\backslash\{0\}$ et on souhaite montrer que le groupe $(\mathbb{K}^*, \cdot)$ de cardinal c est cyclique.
Pour tout entier d de $\mathscr{D}_c$, on note $N(d)$ le nombre d'éléments de $(\mathbb{K}^*, \cdot)$ qui sont d'ordre d.
   (a) Déterminer la valeur de $\displaystyle\sum_{d\in\mathscr{D}_c} N(d)$.
   (b) Soit d un élément de $\mathscr{D}_c$.
      i. On suppose qu'il existe un élément x d'ordre d dans $\mathbb{K}^*$ et on note H le sous-groupe de $(\mathbb{K}^*, \cdot)$ engendré par x. En introduisant un polynôme judicieux, montrer que tout élément d'ordre d de $\mathbb{K}^*$ est dans H.
      ii. Montrer que pour tous les éléments d de $\mathscr{D}_c$ on a l'inégalité $N(d) \leqslant \varphi(d)$.
   (c) Montrer que pour tout entier d de $\mathscr{D}_c$ on a l'égalité $N(d) = \varphi(d)$. En déduire que $(\mathbb{K}^*, \cdot)$ est un groupe cyclique.

Corrigé

5. (a) Si $i = 0$, $\varphi(p^i) = \varphi(1) = 1$.
Si $i \geqslant 1$, les nombres premiers avec p^i sont les nombres qui ne sont pas des multiples de p. L'intervalle $[\![1, p^i]\!]$ contient une proportion $\dfrac{1}{p}$ de multiples de p, à savoir les p^{i-1} nombres du type λp pour $\lambda \in [\![1, p^{i-1}]\!]$. On a donc
$$\varphi\left(p^i\right) = p^i - p^{i-1} = p^i\left(1 - \frac{1}{p}\right).$$
Par ailleurs, pour tout entier $k > 0$,
$$\mathscr{D}_{p^k} = \{p^i, 1 \leqslant i \leqslant k\} = \{1, p, \ldots, p^k\}.$$
On a alors :
$$\begin{aligned} f\left(p^k\right) &= \sum_{d\in\mathscr{D}_{p^k}} \varphi(d) = \sum_{i=0}^{k} \varphi(p^i) = \varphi(p^0) + \sum_{i=1}^{k} \varphi(p^i) \\ &= \varphi(1) + \sum_{i=1}^{k}\left(p^i - p^{i-1}\right) = 1 + \sum_{i=1}^{k} p^i - \sum_{i=1}^{k} p^{i-1} \\ &= 1 + \sum_{i=1}^{k} p^i - \sum_{i=0}^{k-1} p^i = 1 + p^k - p^0 = p^k. \end{aligned}$$

(b) Il ne s'agit pas ici de montrer que l'expression $P(d_1, d_2) = d_1 d_2$ est bien définie pour tous $d_1 \in \mathscr{D}_{m_1}$ et $d_2 \in \mathscr{D}_{m_2}$ mais de justifier que P prend bien ses valeurs dans l'ensemble image indiqué, $\mathscr{D}_{m_1 m_2}$. Ce fait est relativement évident mais il convient d'en fournir une preuve qui se ramène à la définition de la divisibilité. La relation de divisibilité est compatible avec le produit. Pour des entiers naturels (ce serait aussi valable avec des entiers relatifs) a, b, c et d :

$$\begin{aligned} a \mid b, c \mid d &\Leftrightarrow \exists k, \ell \in \mathbb{N}, b = ka, d = \ell c \\ &\Rightarrow \exists k, \ell \in \mathbb{N}, bd = (ka)(\ell c) = (k\ell)(ac) \\ &\Rightarrow \exists m \in \mathbb{N}, bd = m(ac) \\ &\Leftrightarrow ac \mid bd. \end{aligned}$$

Le produit d'un diviseur de m_1 par un diviseur de m_2 est donc bien un diviseur du produit de m_1 par m_2. L'application P est donc bien définie à valeurs dans $\mathscr{D}_{m_1 m_2}$.
Montrons maintenant qu'elle est bijective.

Injectivité : considérons (d_1, d_2) et (d_1', d_2') dans $\mathscr{D}_{m_1} \times \mathscr{D}_{m_2}$ tels que $P(d_1, d_2) = P(d_1', d_2')$. On a alors $d_1 d_2 = d_1' d_2'$ et en particulier $d_1 \mid d_1' d_2'$ mais également $d_1' \mid d_1 d_2$. De plus m_1 et m_2 étant premiers entre eux, il en est de même de leurs diviseurs respectifs : d_1 et d_1' sont premiers avec d_2 et d_2'.
Le lemme de Gauss permet alors d'affirmer que $d_1 \mid d_1'$ et symétriquement $d_1' \mid d_1$. On en déduit $d_1 = d_1'$ (des entiers naturels se divisant l'un l'autre sont nécessairement égaux). On obtient par le même procédé (ou du fait que $d_1 d_2 = d_1' d_2'$) $d_2 = d_2'$ et donc $(d_1, d_2) = (d_1', d_2')$, ce qui prouve que P est injective.

Surjectivité : Considérons désormais un diviseur d de $m_1 m_2$ et posons

$$d_1 = \mathrm{PGCD}(d, m_1) \text{ et } d_2 = \mathrm{PGCD}(d, m_2).$$

On a ainsi $d_1 \in \mathscr{D}_{m_1}$ et $d_2 \in \mathscr{D}_{m_2}$. Nous allons montrer que $d = d_1 d_2$.
Les entiers m_1 et m_2 étant premiers entre eux, il en est de même de d_1 et d_2. Comme $d_1 \mid d$ et $d_2 \mid d$, le fait que d_1 et d_2 sont premiers entre eux entraîne $d_1 d_2 \mid d$ (c'est une conséquence du lemme de Gauss).
De plus, l'identité de Bézout donne

$$\exists u_1, v_1 \in \mathbb{Z}, \quad du_1 + m_1 v_1 = d_1$$

et

$$\exists u_2, v_2 \in \mathbb{Z}, \quad du_2 + m_2 v_2 = d_2.$$

En faisant le produit terme à terme de ces deux égalités, on obtient

$$d(du_1u_2 + m_1v_1u_2 + u_1m_2v_2) + m_1m_2v_1v_2 = d_1d_2$$

et comme $d \mid m_1m_2$, on en déduit $d \mid d_1d_2$.
On a à la fois $d_1d_2|d$ et $d|d_1d_2$. On a donc $d = d_1d_2$ et finalement $P(d_1, d_2) = d_1d_2 = d$, ce qui prouve que P est surjective.

Remarque. On pourrait aussi raisonner en utilisant les décompositions en produit de facteurs premiers puisque l'hypothèse $n \wedge m = 1$ nous assure que les nombres premiers intervenant dans les décompositions respectives de n et m ne sont pas les mêmes.

(c) Si $m_1, m_2 \in \mathbb{N}$ sont premiers entre eux, on a

$$\begin{aligned} f(m_1)f(m_2) &= \sum_{d_1 \in \mathscr{D}_{m_1}} \varphi(d_1) \sum_{d_2 \in \mathscr{D}_{m_2}} \varphi(d_2) \\ &= \sum_{(d_1,d_2) \in \mathscr{D}_{m_1} \times \mathscr{D}_{m_2}} \varphi(d_1)\varphi(d_2) \\ &\underset{(1)}{=} \sum_{(d_1,d_2) \in \mathscr{D}_{m_1} \times \mathscr{D}_{m_2}} \varphi(d_1d_2) \\ &\underset{(2)}{=} \sum_{d \in \mathscr{D}_{m_1m_2}} \varphi(d) \\ &= f(m_1m_2), \end{aligned}$$

avec (1) car d_1 et d_2 sont premiers entre eux (en tant que diviseurs respectifs des entiers premiers entre eux m_1 et m_2) et (2) grâce à la bijection obtenue dans la question précédente.

(d) L'égalité demandée est donc $n = f(n)$ pour tout $n > 0$. Le théorème fondamental de l'arithmétique nous assure que tout entier $n > 0$ se décompose de manière unique, à l'ordre près des facteurs, comme produit de facteurs premiers. Plus précisément, pour tout $n > 0$, il existe un unique entier $k \in \mathbb{N}$, une unique suite ordonnée finie de nombres premiers $p_1 < \cdots < p_k$ et une unique suite finie d'entiers $\alpha_1, \ldots, \alpha_k$ strictement positifs tels que [8]

$$n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}.$$

Procédons par récurrence sur le nombre $k \in \mathbb{N}$ de diviseurs premiers de n en utilisant le résultat de la question précédente. Définissons le prédicat P_k suivant, dépendant de la variable $k \in \mathbb{N}$:

8. On convient que $k = 0 \Leftrightarrow n = 1$: un produit vide est égal à 1, de même qu'une somme vide est égale à 0.

P_k : tout entier $n \in \mathbb{N}^*$ possédant exactement k diviseurs premiers distincts vérifie l'égalité $n = f(n)$.

Tout d'abord, observons que si $k = 0$ (c'est-à-dire pour le seul entier $n = 1$ qui ne possède aucun diviseur premier), le résultat est trivial :

$$\mathscr{D}_1 = \{1\} \quad \text{et} \quad \varphi(1) = 1.$$

Si $n \neq 1$, considérons la décomposition de n en produit de facteurs premiers. Soit $k \in \mathbb{N}^*$ et $p_1, \ldots, p_k$ des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_k$ des entiers naturels non nuls tels que $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Initialisation : P_1 est vraie. En effet, on a vu dans la question 5.(a) que $f\left(p_1^{\alpha_1}\right) = p_1^{\alpha_1}$.

Hérédité : supposons que P_k est vraie pour un certain entier $k \geqslant 1$. Considérons alors un entier $n > 0$ possédant exactement $k+1$ diviseurs premiers deux à deux distincts.
On applique le résultat de la question précédente avec

$$m_1 = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{et} \quad m_2 = \frac{n}{m_1} = p_{k+1}^{\alpha_{k+1}}.$$

Comme m_1 et m_2 ainsi définis sont bien premiers entre eux (car les nombres premiers intervenant dans leur écriture respectives sont différents), la question 5.(c) nous assure que

$$f(n) = f(m_1 m_2) = f(m_1) f(m_2).$$

Comme m_1 possède exactement k diviseurs premiers deux à deux distincts, on peut lui appliquer l'hypothèse de récurrence : on a $f(m_1) = m_1$. Comme m_2 possède un seul diviseur premier, l'initialisation nous permet d'affirmer que $f(m_2) = m_2$. On a donc

$$f(n) = f(m_1) f(m_2) = m_1 m_2 = n,$$

ce qui prouve que P_{k+1} est vraie.

Conclusion : P_0 et P_1 sont vraies et, pour tout $k \in \mathbb{N}^*$, on a

$$P_k \Rightarrow P_{k+1}.$$

d'après le principe de récurrence, P_k est donc vraie pour tout $k \in \mathbb{N}$: quel que soit le nombre de diviseurs premiers de n, on a

$$n = f(n).$$