mathématiques

Bernard
Gostiaux

Exercices de mathématiques spéciales

Algèbre
Tome 1

puf

Exercices de mathématiques spéciales

Tome 1

Algèbre

COLLECTION DIRIGÉE PAR PAUL DEHEUVELS

EXERCICES DE MATHÉMATIQUES SPÉCIALES

MP, MP*

nouveaux programmes

TOME 1

Algèbre

BERNARD GOSTIAUX

PRESSES UNIVERSITAIRES DE FRANCE

ISBN 2 13 048727 0
ISSN 0246-3822

Dépôt légal — 1re édition : 1997, septembre

108, boulevard Saint-Germain, 75006 Paris

Avant-Propos

Nous vivons une curieuse époque, avec des bouleversements nombreux, même dans la façon de concevoir et d'enseigner les sciences.

L'un de ces bouleversements concerne la Physique qui, après avoir accordé pendant des décennies une part importante à la théorie, redore le blason de l'expérience, (et l'utilisation de l'ordinateur y est pour beaucoup).

Mais, comme malheureusement le bon sens n'est pas la chose du monde la mieux partagée, même chez de grands scientifiques, (quel humoriste ce Descartes), au lieu d'un rééquilibrage on assiste à un mouvement de bascule qui en contre coup affecte les Mathématiques.

Celles-ci se trouvent réduites au rôle d'outil secondaire, on leur demande de fournir une liste de résultats utilisables par... l'utilisateur justement, sans que ce dernier ait à comprendre comment l'outil est obtenu.

C'est oublier un peu vite que le premier rôle des mathématiques devrait être de former les capacités d'analyse et de raisonnement qui permettent de faire face aux problèmes posés.

C'est en transformant les mathématiques en collection de résultats qu'on les rend rébarbatives, et pour reprendre des termes de ceux qui nous gouvernent, « tyranniques et intellectuellement mutilantes ».

Mieux vaudrait une tête bien faite que bien pleine, donc allégeons les programmes, (au diable le « à quoi ça sert » et le rendement immédiat), et connaissons mieux.

C'est dans cet état d'esprit que je vais m'efforcer de rédiger les exercices qui suivent, en analysant les situations rencontrées pour y appliquer mes connaissances.

À Catherine, sans qui rien ne serait.
Merci à mes élèves qui m'ont beaucoup appris.

Pour aborder un problème le mieux est d'en déterminer la nature, sans esprit préconçu.

S'agit-il d'un problème de nature algébrique, (linéaire ou non), topologique, géométrique, ou de plusieurs natures à la fois.

Est-il de caractère existentiel, (« Montrer qu'il existe... ») auquel cas je pourrai faire la liste des moyens d'obtenir l'existence de quelque chose, (Théorème des valeurs intermédiaires, point fixe, Cauchy Lipschitz...), est-il de nature « logique », (« Montrer l'équivalence des conditions... »), de nature « calculatoire » : c'est ce qu'il faut essayer de déterminer d'abord.

Cette première analyse correctement faite est souvent la clé du succès. On essaye ensuite de trouver la meilleure façon de traiter le problème en n'oubliant pas quelques idées de base.

1°) Pour obtenir un résultat valable pour tous les éléments d'un ensemble E construit à partir d'un sous-ensemble F, si ce résultat est stable par le procédé constructif, il suffira de l'établir sur F. On traitera ainsi une propriété « stable par linéarité » sur une base d'un espace vectoriel, une propriété stable par continuité sur une partie partout dense par exemple. Ces procédés peuvent se combiner, comme dans la justification du lemme de Lebesgue, et cette attitude face à un problème ne fait que généraliser l'idée de la récurrence. Voir par exemple 6.25, (analysé au chapitre 1, n° 33).

2°) On ne compare bien que des choses « de même nature », ce qui conduit, pour comparer un nombre et une intégrale, ou un nombre et une somme, à transformer ce nombre en intégrale, ou en somme, en introduisant une intégrale ou une somme de valeur 1. Pensez par exemple à la justification des Théorèmes de Fejer ou de Dirichlet pour les séries de Fourier, à la justification de Stone Weierstrass par les polynômes de Bernstein ou par produit de convolution, mais pensez aussi à l'utiliser avec les matrices orthogonales ou unitaires, (voir 5.26).

3°) Pour justifier une égalité de deux objets, il est fréquent de montrer leur égalité avec un troisième construit à partir des deux précédents.

Vous pouvez remarquer que ces idées s'appuient sur une bonne connaissance du cours, c'est-à-dire sur la connaissance de la façon dont on le justifie, et pas seulement des résultats.

Dans un premier chapitre, j'examinerai des énoncés pour déterminer leur nature. Ils seront résolus dans les chapitres les concernant plus spécifiquement, chacun de ces chapitres commençant par des remarques qu'il est bon d'avoir présentes à l'esprit.

Les exercices ne posant pas de problèmes particuliers, du type calcul de e^A pour $A \in \mathcal{M}_n(\mathbb{C})$ par exemple, seront directement traités dans les chapitres particuliers.

Il en sera de même pour les exercices qui résistent à une première analyse et qu'on trouve, à force de chercher dans tous les sens...

Je suppose le cours connu, donc je ne ferai pas de rappels directs des résultats classiques. Je considérerai plutôt des exercices à la limite du programme, ceux où l'on construit un raisonnement s'appuyant sur les résultats du cours pour conclure, et non ceux qui se résolvent par une simple application de ces résultats.

Quelques remarques pour conclure.

Soyez sensible à la **symétrie des données** : si des variables jouent le même rôle, elles interviennent de la même façon dans la conclusion (voir exercice 4.22).

Connaître le cours, ce n'est pas se contenter d'une collection de résultats, mais c'est savoir comment ils sont justifiés pour pouvoir les étendre le cas échéant, ou s'inspirer des justifications. Voir 4.23.

Dans un groupe, une égalité c'est une différence nulle : savoir penser aux deux points de vue à partir d'un seul (exercice 11.4).

Aborder un exercice doit se faire de **manière dynamique**, en explorant les conséquences de chaque nouvelle donnée, ou de chaque résultat trouvé, non seulement dans ce qu'on cherche encore, mais aussi dans ce que l'on connaît déjà, car ces « connaissances » peuvent s'en trouver améliorées.

À ce sujet, l'exercice 11.4 est très intéressant.

J'ai parlé au début des exercices **d'aspect existentiel**. Parmi les résultats affirmant l'existence d'un élément, penser aux bornes atteintes, pour les fonctions continues d'un compact dans $\mathbb{R}$, voir exercices 6.14, ou 5.17, 5.18.

Enfin il existe une démarche scientifique que l'on devrait développer, même si ce n'est pas toujours facile : c'est celle qui consiste à **analyser un problème donné, en partant éventuellement de cas particuliers**, pour en dégager la nature, entrevoir une solution, puis passer à la justification théorique. Cette démarche est analogue au **passage de l'expérimentation à la modélisation** en physique par exemple. L'exercice 13.9, (analysé au chapitre 1 au numéro 31) est révélateur de cet état d'esprit qui devrait être plus répandu.

Une bonne connaissance de la nature des objets mathématiques considérés permet souvent de trouver une solution élégante parce qu'efficace. Ainsi, une question portant sur des intégrales peut être facilitée si on se détache des valeurs prises pour des fonctions données, pour s'attacher à **l'aspect forme linéaire positive de l'intégrale**.

J'ai donné, dans cet état d'esprit, deux solutions de l'exercice 4.4, l'une alourdie parce qu'on est passé d'une matrice à son action sur les vecteurs, l'autre, plus courte, parce qu'on est resté dans l'algèbre des endomorphismes, le résultat cherché étant purement matriciel.

N'allez pas croire enfin, que l'on puisse se tirer d'affaire sans un minimum, (hélas très lourd) de connaissances.

Cela va de résultats précis, comme les Théorèmes de Baire, de Stone Weierstrass par exemple, à des modes de raisonnement comme **le procédé de la suite diagonale**, (voir 5.15, analysé au chapitre 1, n° 28, ou 6.25), ou à la notion de groupe opérant sur un ensemble et à l'équation aux classes, (voir 2.35, 2.36).

TABLE DES MATIÈRES

Tome 1. Algèbre

Tome 2. Topologie, Analyse

Tome 3. Géométrie, géométrie différentielle

Analyse d'énoncés

1. Soit A et B dans $\mathcal{M}_n(\mathbb{C})$ telles qu'il existe λ dans $\mathbb{C}$ avec $\lambda AB + A + B = 0$. Montrer qu'elles commutent.

L'identité donnée et le résultat sont stables par passage à des matrices semblables d'où l'idée de passer par une base mieux adaptée en commençant peut-être par accrocher un vecteur propre commun, d'autant plus que si elles commutent, tout sous-espace propre pour une est stable par l'autre... d'où l'existence de vecteurs propres communs si le problème est résolu. Voir 4.4, où une surprise vous attend.

---

2. Soit f un morphisme additif d'un espace vectoriel réel E dans lui-même, borné sur la boule unité de E, (fermée). Montrer que f est linéaire.

Il s'agit de justifier : $\forall(\lambda, x) \in \mathbb{R} \times E, f(\lambda x) = \lambda f(x)$. La construction de $\mathbb{R} = \overline{\mathbb{Q}}$, avec $\mathbb{Q}$ déduit de $\mathbb{Z}$, lui-même de $\mathbb{N}$ incite à justifier $f(rx) = rf(x)$ pour r rationnel, à partir de l'aspect morphisme additif, et après, le passage à $\mathbb{R}$ ne peut se faire qu'avec la densité de $\mathbb{Q}$ dans $\mathbb{R}$, et la continuité de f qui doit se justifier à partir de l'aspect borné. Voir 6.1.

---

3. Soit (a_n) une suite de réels tendant vers $+\infty$ et telle que $a_{n+1} - a_n$ tende vers 0. Montrer qu'il existe φ strictement croissante de $\mathbb{N}$ dans $\mathbb{N}$, telle que $(a_{\varphi(n)} - n)$ tende vers 0.

Construire une suite croissante d'entiers, c'est certainement par étapes, prendre la borne inférieure d'un ensemble (non vide) d'entiers tous strictement supérieurs au dernier construit.

Pour cela, on va « dépasser n », mais il ne faudrait pas dépasser à la fois, n, $n+1$, $n+2$, ..., $n+p$, d'où l'idée de se placer déjà dans une zone où $|a_{k+1} - a_k| < \lambda$ avec $\lambda < 1$, et même $\frac{1}{2}, \frac{1}{3}$, ... c'est à voir en 8.4.

---

4. Soit E un espace vectoriel complexe de dimension finie, a un endomorphisme de E, montrer qu'il existe $R > 0$ tel que pour tout s de $]-R, R[$ on ait :

$$\det(\mathrm{Id} - sa) = \exp\left(-\sum_{k=1}^{\infty} \frac{s^k}{k} \operatorname{trace}(a^k)\right).$$

L'endomorphisme a intervient par un déterminant, et par des traces, notions indépendantes de la base choisie pour traduire a, donc on peut travailler sur une forme intéressante à la fois pour les traces et le déterminant, à savoir la forme triangulaire, ce qui est un droit sur $\mathbb{C}$ en dimension finie.

La forme de la série, (et l'exponentielle) fait penser à du $\ln(1-z)$: il y aura un problème de définition d'un logarithme complexe, voir en 10.1.

---

5. Pour tout P de $\mathbb{C}[X]$, on pose $L(P)(z) = e^{-z} \sum_{n=0}^{\infty} \frac{P(n)}{n!} z^n$.

Montrer que l'on définit ainsi un isomorphisme de $\mathbb{C}[X]$ sur lui-même.

C'est de l'algèbre linéaire en dimension infinie, l'aspect bijectif de L, linéaire, provenant de « image d'une base est une base », le seul côté injectif ou surjectif ne suffisant pas.

La définition de L(P) est linéaire en P, (justifier l'existence). Pour l'isomorphisme, choisir une base « adaptée » et vu les $P(n)$, pourquoi ne pas penser « interpolateurs de Lagrange » et prendre $P_k(x) = x(x-1)...(x-k+1)$? Voir en 3.1.

---

6. Soit $a > 0$. Trouver toutes les fonctions f dérivables sur $]0, +\infty[$ vérifiant $f'(x) = f\left(\frac{a^2}{x}\right)$.

Comme $x \rightsquigarrow \frac{a^2}{x}$ est un C^∞ difféomorphisme de $]0, +\infty[$ sur lui-même, f étant dérivable, le second membre est dérivable donc f' est de classe C^1, (d'où f de classe C^2), et par récurrence f est de classe C^∞. On peut espérer établir une équation différentielle vérifiée par f. Voir en 13.3.

---

7. Soit les applications f et g de $\mathbb{C}$ dans $\mathbb{C}$ définies respectivement par $f(z) = z^2 + z + 1$ et $g(z) = z^2 - z + 1$, et A une partie finie de $\mathbb{C}$ telle que $f(A) \subset A$ et $g(A) \subset A$. Montrer que $A = \{i, -i\}$.

Trouver les polynômes P de $\mathbb{C}[X]$ tels que

$$P(X^2 + X + 1) = P(X)P(X + 1).$$

Exercice difficile. En fait, les modules des éléments de A étant en nombre fini, admettent une borne supérieure atteinte, en z_0 par exemple. En traduisant $|f(z_0)| \leqslant |z_0|$ et $|g(z_0)| \leqslant |z_0|$, en remarquant que $f(z_0) - g(z_0) = 2z_0$, peut-être que l'égalité dans l'inégalité triangulaire donnera quelque chose...

La suite est plus simple. Les polynômes de $\mathbb{C}[X]$ étant scindés, on considérera sans doute A = l'ensemble fini des zéros de P. Voir 3.2.

---

8. Soit P un polynôme de degré impair de $\mathbb{R}[X]$, et f une application de classe C^∞ de $\mathbb{R}$ dans $\mathbb{R}$, telle que

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, \left|f^{(n)}(x)\right| \leqslant P(x).$$

Que dire de f ?

L'hypothèse $f \in C^\infty(\mathbb{R}, \mathbb{R})$ fait penser à des développements en série entière, la convergence de la série de Taylor en x_0 vers f se faisant en majorant (localement) le reste d'ordre n en considérant $\|P\|_\infty$, $\| \ \|_\infty$ sur un compact.

Quant au degré impair, il est sans doute là pour donner un zéro de P... Voir 10.4.

---

9. Soit $f \in C^1(\mathbb{R}^n, \mathbb{R}^n)$, telle que, $\forall (x, y)$ de $(\mathbb{R}^n)^2$, $\|f(x) - f(y)\| \geqslant \|x - y\|$. Montrer que f est un C^1 difféomorphisme.

L'hypothèse assure l'injectivité. Il faut alors montrer que $f(\mathbb{R}^n) = \Omega$ est égal à $\mathbb{R}^n$. On peut penser à justifier et utiliser le Théorème du Difféomorphisme local, ce qui donnerait Ω ouvert car voisinage de chacun de ses points. Après..., avoir Ω fermé, dans $\mathbb{R}^n$ connexe... voir 12.1.

---

10. Soit X un espace métrique compact, et L_C l'ensemble des applications C. Lipschitziennes de X dans $\mathbb{R}$. Montrer que la convergence simple d'une suite d'éléments de L_C implique la convergence uniforme.

Topologie générale ou espace fonctionnel ? En fait l'aspect C. Lipschitzien se formule en utilisant deux points, donc c'est stable par convergence simple des f_n vers f, qui est aussi C. Lipschitzienne. Mais alors $f - f_n$, 2C Lipschitzienne, « petite » en x le sera localement, et d'un recouvrement ouvert de X compact... c'est de la topologie générale. Voir 6.2.

---

11. Soit $P \in \mathbb{R}[X]$. Montrer que $\int_{-1}^{1} P^2(x)dx = -i \int_0^{\pi} P^2(e^{i\theta})e^{i\theta}d\theta$.

En déduire, si $P(X) = \sum_{k=0}^{n} a_k X^k$, l'inégalité :

$$\sum_{0 \leqslant k, l \leqslant n} \frac{a_k a_l}{k+l+1} \leqslant \pi \sum_{k=0}^{n} a_k^2.$$

En fait $P \rightsquigarrow \int_{-1}^{1} P^2(x)dx$ étant une forme quadratique, on peut lui associer sa forme bilinéaire $(P, Q) \rightsquigarrow \int_{-1}^{1} P(x)Q(x)dx$ et vérifier alors l'égalité sur la forme bilinéaire et sur les vecteurs d'une base de $\mathbb{R}[X]$: le calcul est simplifié. Toujours analyser la situation en se disant « comment interviennent les données », pour ramener la vérification à un cas plus simple. Voir 5.3.

---

12. Soit $f \in \mathscr{C}^1([0, 1], \mathbb{R})$ telle que $f(0) = 0$, $0 < f'(t) \leqslant 1$ sur $[0, 1]$. Montrer que $\left(\int_0^1 f(t)dt\right)^2 \geqslant \int_0^1 f^3(t)dt$.

Hum, la fonction f intervenant par un cube, cela ne semble pas être quadratique. Par ailleurs f croit et $f(0) = 0$ donc f est à valeurs positives, on doit établir une inégalité, ..., et si on revenait à une idée simple : pour justifier $u(x) \geqslant v(x)$, on étudie les variations de $u(x) - v(x)$, en introduisant ici une borne variable x au lieu de 1 dans l'intégrale ?

On étudie donc les variations de $x \rightsquigarrow g(x) = \left(\int_0^x f(t)dt\right)^2 - \int_0^x f^3(t)dt$. Voir 7.5.

---

13. Soit une suite $(f_n)_{n \in \mathbb{N}}$, décroissante, de fonctions en escalier, positives ou nulles, avec f_1 à support compact, qui converge simplement vers 0, sur $\mathbb{R}$. Montrer que $\lim_{n \to +\infty} \int_{-\infty}^{+\infty} f_n(t)dt = 0$.

Il y a d'abord un problème d'existence des $\int_{-\infty}^{+\infty} f_n(t)\mathrm{d}t$. Or f_1 est nulle hors d'un compact, donc les $f_n(t)$ compris entre 0 et $f_1(t)$, aussi. On se ramène à un segment, compact, $[a, b]$.

En un point de continuité x, f_n en escalier est « localement constante » : si $f_n(x)$ est petit, ce sera vrai sur un ouvert $\omega(x)$, et (décroissance) *a fortiori* vrai $\forall p \geqslant n$: on va associer aux x de $[a, b]$ des ouverts $\omega(x)$ ..., en voyant que faire pour les points de discontinuité, d'où recouvrement fini... c'est de la compacité. Voir en 6.3.

---

14. Soit A dans $\mathcal{M}_{n,p}(\mathbb{R})$ de rang n. Montrer que $A\,{}^tA$ est inversible. Que dire de ${}^tAA$ si A est de rang p ?

Matrice inversible... On peut penser déterminant, mais en fait $B = A\,{}^tA$ est symétrique réelle, il y a de la forme quadratique là-dessous, d'autant que la forme quadratique est positive. Voir 5.4.

---

15. Soit z dans $\mathbb{C}$ tel que $\mathrm{Im}z > 0$. Montrer que

$$\sup_{t \in \mathbb{R}} \left|\frac{t-i}{t-z}\right| = \frac{|z+i| + |z-i|}{2\mathrm{Im}(z)}.$$

Il s'agit de la borne supérieure d'une fonction de $\mathbb{R}$ dans $\mathbb{R}$ continue, qui tend vers 1 en + ou – l'infini: cette borne supérieure existe et est atteinte. On peut étudier la fonction $t \rightsquigarrow \varphi(t) = \left|\frac{t-i}{t-z}\right|^2$, (dérivée...) mais... on peut aussi se dire que sur le plan complexe, pour τ complexe différent de z, on sait étudier la fonction homographique $\tau \rightsquigarrow \frac{\tau - i}{\tau - z}$, et voir ce que devient l'axe des x. Aussi je donnerai une solution géométrique de cet exercice. Voir 14.5.

---

16. Soit A dans $\mathcal{M}_n(\mathbb{C})$. On désigne par $f_1, f_2, \ldots, f_n$, n fonctions de A, à valeurs complexes, telles que le polynôme caractéristique $\chi_A(X)$ de A soit égal à :

$$(-1)^n(X^n + f_1(A)X^{n-1} + \ldots + f_{n-1}(A)X + f_n(A)).$$

a) Montrer que, pour tout i compris entre 1 et n, et tout couple (A, B) de $(\mathcal{M}_n(\mathbb{C}))^2$, on a $f_i(AB) = f_i(BA)$.

b) Soit ϕ une fonction polynomiale de $\mathcal{M}_n(\mathbb{C})$ dans $\mathbb{C}$ vérifiant l'égalité $\phi(AB) = \phi(BA)$, pour tout couple de $(\mathcal{M}_n(\mathbb{C}))^2$. Montrer que ϕ est un polynôme en $f_1, ..., f_n$.

C'est *a priori* de l'algèbre, le a) revenant à justifier l'égalité des polynômes caractéristiques de AB et BA. Pour la suite...

En fait, sur $\mathbb{C}$, les $f_j(A)$ s'expriment à l'aide des fonctions symétriques de $\lambda_1, \lambda_2, ..., \lambda_n$, valeurs propres supposées distinctes de A. Il faut donc passer de A ayant des valeurs propres distinctes à A quelconque : c'est peut-être un problème de densité ; encore faudra-t-il vérifier que ϕ « dépend symétriquement » de n variables distinctes, en utilisant le a). Il y a plus d'analyse que d'algèbre. Allez voir en 6.4.

---

17. Soit une suite réelle $(a_n)_{n \in \mathbb{N}}$ qui converge vers 1. On définit une suite $(p_n)_{n \in \mathbb{N}}$ en posant $a_n = \sum_{k=0}^{n} \frac{p_k}{(n-k)!}$.

Déterminer la limite de $(p_n)_{n \in \mathbb{N}}$.

L'existence des p_n ne pose pas de problème mais après... En fait $\sum_{k=0}^{n} p_k \cdot \frac{1}{(n-k)!}$ est le coefficient c_n du terme de degré n dans le produit de deux séries entières, de termes généraux $p_n x^n$ et $\frac{x^n}{n!}$, cette dernière ayant pour somme e^x, inversible. Tiens, tiens, ... Il y a sans doute là un moyen de calculer les p_n. Voir en 10.11.

---

18. Soit E un espace vectoriel normé de dimension finie, G le groupe des automorphismes de E et a dans L(E). On pose $F_a = \{g^{-1}ag | g \in G\}$. Montrer que F_a est fermé si et seulement si a est diagonalisable.

Topologie ou algèbre : qu'est-ce qui l'emporte ? Comment caractériser a diagonalisable ? Par un polynôme caractéristique scindé et des dimensions de sous-espaces propres égales aux multiplicités des valeurs propres, donc des rangs de $a - \lambda_j id_E$ connus, donc des mineurs nuls et ça c'est continu par rapport aux coefficients des matrices, car polynomial. Que vient faire b semblable à a là-dedans ? Semblable, donc les rangs sont les mêmes... Il y a beaucoup d'algèbre sur la diagonalisation. Un petit tour en 4.24.

---

19. Calculer le déterminant d'ordre n :

$$D_n = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-2} & x_1^{n+1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-2} & x_2^{n+1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-2} & x_n^{n+1} \end{vmatrix}.$$

Cela sent le Vandermonde à plein nez ! Par ailleurs, un déterminant est une forme linéaire alternée des colonnes. Si on avait un moyen d'exprimer la dernière colonne comme combinaison linéaire des précédentes et de la colonne des x_i^{n-1}, i variant, on récupérerait du Vandermonde.

Les x_i jouant des rôles symétriques, allons chercher (en 4.25) les fonctions symétriques des x_i...

---

20. Soit A une matrice carrée réelle et A' une matrice de même taille telle que AA'A = A. Soit U dans $\mathcal{M}_{n,p}(\mathbb{R})$.

On pose $A = U\,{}^tU$, $V = A' - {}^tA'$ et $W = {}^tUVU$. Montrer que $W = 0$.

On pose $P = {}^tUA'U$, montrer que P est un projecteur symétrique.

Soient X dans $\mathcal{M}_{n,p}(\mathbb{R})$ et Y une matrice réelle définie positive d'ordre n. On pose $Z = Y + X\,{}^tX$. Montrer que $I_p - {}^tXZ'X$ est symétrique définie positive, (on pourra mettre Y sous la forme $T\,{}^tT$).

Le bel exercice qui donne du fil à retordre, (et il m'en a donné), mais qui illustre la démarche « vivante » qu'il faut avoir, en injectant chaque résultat trouvé dans tout ce que l'on connaît pour en voir les conséquences, un peu comme aux échecs où l'on évalue les conséquences du coup joué. Ainsi, $A = U\,{}^tU$ étant symétrique, on peut utiliser l'égalité $A = {}^tA$ en transposant la relation où A' intervient et s'apercevoir que cela entraîne l'égalité AVA = 0.

Puis V étant antisymétrique, W l'est aussi, donc iW est hermitienne, donc diagonalisable, donc W aussi, donc W sera nulle si et seulement si 0 est seule valeur propre, ce qui conduit à calculer les puissances de W, pour récupérer du ... $U\,{}^tU$ ... = ... A ... suffisamment pour avoir AVA.

De même, P symétrique, donc diagonalisable, (j'y pense tout de suite) sera projecteur si et seulement si il n'a que 0 et 1 pour valeurs propres. Je ne me focalise pas sur $P^2 = P$, mais je cherche un polynôme en $X^\alpha(1-X)^\beta$ annulé par P...

Le bel exercice, que j'ai placé en 11.4 pour sa petite touche hermitienne.

---

21. Soit une matrice carrée complexe d'ordre n sur $\mathbb{C}$. Montrer l'équivalence de M est nilpotente et de : trace $M^k = 0$ pour $k = 1, 2, ..., n$.

En utilisant le Théorème de Dunford, on sait que ceci équivaut à la nullité des valeurs propres, $\lambda_1, ..., \lambda_n$, et la trace de M^k est la somme des (λ_j^k) si j varie. Mais pour j fixé et k variant, les λ_j^k interviennent dans Taylor Lagrange pour $P(x+\lambda_j)$... Pourrait-il y avoir une approche polynomiale ? Vous le saurez en 3.10.

---

22. Soit f: $[0, 1] \mapsto \mathbb{R}$ continue telle que pour tout entier k, $\int_0^1 t^k f(t)\mathrm{d}t = 0$. Montrer que f est nulle.

En somme, f est orthogonale aux monômes $t \rightsquigarrow t^k$, (donc aux polynômes), pour le produit scalaire $\langle u, v\rangle = \int_0^1 u(t)v(t)\mathrm{d}t$ sur $E = \mathscr{C}^0([0, 1], \mathbb{R})$, cette orthogonalité ne s'étendrait-elle pas aux fonctions continues par Stone Weierstrass... Voir 9.12.

---

23. Soit f dans $\mathscr{C}^0([a, b], \mathbb{R})$ telle que $\int_a^b f(t)t^n\mathrm{d}t = 0$ pour tout n compris entre 0 et $p-1$. Montrer que f change de signe au moins p fois sur $]a, b[$.

Comme ci-dessus, il y a orthogonalité de f avec le sous-espace F des fonctions polynomiales de degré $p-1$ au plus. Si on met en évidence les changements de signes de f sur $]a, b[$ et s'il y en a moins de p... Cette fois c'est du produit scalaire, que je traite en 5.14.

---

24. Soit F un fermé de $\mathbb{R}^n$ et $(f_p)_{p\in\mathbb{N}}$ une suite d'applications continues de F dans $\mathbb{R}$, simplement bornée, (c'est-à-dire que pour chaque x de F, la suite des $f_n(x)$ est bornée). Montrer que, pour toute boule ouverte B de F, il existe une boule ouverte B' de F, contenue dans B, sur laquelle la suite des f_p est uniformément bornée.

Analysons les données : F, fermé de $\mathbb{R}^n$ est complet. On a des f_n continues, en quantité dénombrable, et qui peuvent fournir des ouverts ou des fermés par images réciproques...

On veut une boule ouverte B' telle que

$$\exists p_0, \forall x \in B', \forall k \in \mathbb{N}, |f_k(x)| \leqslant p_0, \ldots$$

mais la condition $|f_k(x)| \leqslant p_0$ définit un fermé, le $\forall k$... donne une intersection de fermés, et un $B' \subset$ un fermé c'est un fermé d'intérieur non vide. Si avec tout cela vous ne sentez pas du Baire dans l'air, allez traîner du côté de 6.10.

---

25. Soient f et g deux homéomorphismes de [0, 1] dans lui-même dont 0 et 1 sont les seuls points fixes. Montrer qu'il existe un homéomorphisme h de [0, 1] dans lui-même tel que :

$$f \circ h = h \circ g.$$

En fait, f et g, bijectives bicontinues de [0, 1] sur lui-même sont strictement monotones. Avec $f(0) = 0$ et $f(1) = 1$, on a f strictement croissante ainsi que g.

Avoir $f \circ h = h \circ g$, avec f et g bijectives, c'est aussi vérifier l'égalité $f \circ h \circ g^{-1} = h$, ce qui, ... si on connaît $h(x)$, oblige à poser $h(g^{-1}(x)) = f^{-1}(h(x))$, donc ce qui détermine h en $g^{-1}(x)$, en $g^{-2}(x)$, ..., en $g^{-n}(x)$, $\forall n \in \mathbb{N}$, à partir du seul choix de $h(x)$, mais donnera aussi, en remplaçant x par $g(x), g^2(x)$, ..., les valeurs de h sur tous les $g^n(x)$: on n'est pas très libre. En fait, il faut voir ce que font ces suites $(g^n(x))_{n \in \mathbb{Z}}$, et s'apercevoir que la relation à vérifier est peut-être un moyen de définir h, à partir de sa connaissance sur un intervalle convenable. Allez en 7.15.

---

26. Soit une suite complexe telle que $\lim_{n \to +\infty} \sqrt[n]{|a_n|} = l$. Quel est le rayon de convergence de la série des $\dfrac{a_n z^n}{n!}$? On note f la fonction somme et l'on suppose que $\lim_{|z| \to +\infty} \dfrac{\ln|f(z)|}{|z|} = l'$. Montrer que $l = l'$.

Vu la fin de l'exercice, on doit trouver un rayon de convergence infini.

Puis, relier $|f(z)|$ et les a_n, cela nécessite la connaissance des a_n à l'aide de f seulement : ce sont les formules de Cauchy qui peuvent servir.

Enfin, traduire $\lim_{n \to +\infty} \sqrt[n]{|a_n|} = l$, c'est avoir $|a_n| \leqslant (l+\varepsilon)^n$ pour $n \geqslant n_0$, d'où, à une somme partielle près, $|f(z)| \leqslant e^{(l+\varepsilon)|z|}$.

Cette inégalité passe aux logarithmes, et si $|z|$ tend vers l'infini, la somme partielle, polynôme en $|z|$, ne fera pas le poids ! Voir 10.20.

---

27. Déterminer un équivalent, lorsque a tend vers 0^+, de

$$I(a) = \int_0^{+\infty} \frac{dt}{(1+t^4)(t^2+a^2)}.$$

Si on pose $f(t,a) = \dfrac{1}{(1+t^4)(t^2+a^2)}$, on s'aperçoit, (souci d'une convergence dominée, pour se débarrasser de la partie « infinie » du support), que pour $t \geqslant t_0 > 0$, on a :

$f(t,a) \leqslant g(t) = \dfrac{1}{(1+t^4)t_0^2}$: le paramètre a disparaît, et la contribution de $[t_0, +\infty[$ dans l'intégrale est bornée en a. Vers 0, la fonction $t \rightsquigarrow \dfrac{1}{1+t^4} = \varphi(t)$, est continue, avec $\varphi(0) \neq 0$, donc équivalente à $\varphi(0)$, or une intégrale en $\int_0^{\alpha} \dfrac{dt}{t^2+a^2} = \dfrac{1}{a} \operatorname{Arctg} \dfrac{\alpha}{a}$ est équivalente à $\dfrac{\pi}{2a}$ si a tend vers 0^+ : on peut trouver l'équivalent. Voir 9.14.

---

28. Soit E l'espace vectoriel des suites $x = (x_k)_{k \in \mathbb{N}}$ de réels telles que $\sum_{k=0}^{+\infty} (x_k)^2$ converge. Pour x et y dans E, on pose $\langle x, y \rangle = \sum_{k=0}^{+\infty} x_k y_k$, et l'on note $\| \ \|$ la norme associée.

Soit $(x^{(n)})_{n \in \mathbb{N}}$ une suite bornée d'éléments de E. Montrer qu'il existe une sous-suite $(y^{(k)})_{k \in \mathbb{N}}$ de la suite $(x^{(n)})_{n \in \mathbb{N}}$, et un élément a de E tels que, pour tout z de E, $\langle y^{(k)}, z \rangle$ tend vers $\langle a, z \rangle$.

Brr... Que d'hypothèses ! D'abord, on est dans un préhilbertien. Ensuite on cherche un élément a, et une suite extraite, vérifiant une

condition valable pour tout z de E. C'est exhorbitant ! Si on pouvait remplacer ce pour tout z par... pour tout élément d'une famille totale ? (Pensez à chercher une telle famille dans les préhilbertiens.)

Ensuite, on a une suite de suites et on veut construire quelque chose ? C'est le domaine d'utilisation du *procédé de suite-diagonale* cela. Enfin, bornée, des réels, suite extraite... n'y aurait-il pas de la compacité ? Laissez mijoter cela, et, si vous ne trouvez pas, allez voir en 5.15.

---

29. Soit une suite de complexes $(c_k)_{k \in \mathbb{N}}$. On pose

$$f(x) = \sum_{k=-n}^{n} c_k e^{ikx}.$$

On suppose que $f(x)$, pour tout x réel, est un réel positif ou nul. On note Q le polynôme tel que $f(x) = e^{-inx} Q(e^{ix})$. Montrer que les zéros de Q qui sont des nombres complexes de module 1 ont, dans Q, une multiplicité paire.

Comment aborder cela. Est-ce du Fourier, des polynômes trigonométriques, voyons... En fait, par Liebnitz, les dérivées de f et de $x \rightsquigarrow Q(e^{ix})$ sont reliées, alors, si la multiplicité d'un zéro de Q donnait un zéro multiple de f, fonction de variable réelle à valeurs réelles, (positives qui plus est), on aurait du Taylor Young et l'équivalent de $f(x)$ au voisinage de x_0 doit être une puissance paire de $(x - x_0)$, (pas de changement de signe !). C'est du développement limité cela. Voyons d'un peu plus près en 7.19.

---

30. Soient treize réels distincts. Montrer qu'il en existe deux parmi eux vérifiant :

$$0 < \frac{x-y}{1+xy} < 2 - \sqrt{3}.$$

Si vous n'avez jamais appris vos formules de trigonométrie, c'est le moment car sinon, comment penser que x et y pourrait être des tangentes, $x = \tan\alpha$ et $y = \tan\beta$ par exemple, et qu'alors

$$\frac{x-y}{1+xy} = \frac{\tan\alpha - \tan\beta}{1 + \tan\alpha\tan\beta}, \text{ c'est } \tan(\alpha - \beta).$$

Il n'y a plus qu'à s'interroger sur les intervalles déterminés par treize angles compris entre $-\frac{\pi}{2}$ et $\frac{\pi}{2}$. Allez en 7.18.

---

31. Soit E un espace vectoriel normé de dimension finie sur $\mathbb{C}$. Trouver tous les morphismes continus de $(\mathbb{R}, +)$ dans $(GL(E), o)$.

Diantre ! Comment aborder cela. Voyons, parmi les e.v.n. de dimension finie il y a $\mathbb{C}$, (et même $\mathbb{R}$?), et un morphisme de $\mathbb{R}$ additif dans $(GL_1(\mathbb{R}), o)$, qui n'est autre que $\mathbb{R}^*$, les automorphismes étant les homothéties, un morphisme disais-je, est du type « exponentielle ». Est-ce que cela se généraliserait avec des applications en $t \rightsquigarrow e^{ta}$, $a \in \mathcal{M}_n(\mathbb{C})$? C'est de l'équation différentielle résolue... On doit y arriver en 13.9.

---

32. Soient P, Q, R, S dans $\mathcal{M}_n(\mathbb{C})$, calculer $\det \begin{pmatrix} I_n & O \\ P & Q \end{pmatrix}$ et $\det \begin{pmatrix} R & O \\ S & I_n \end{pmatrix}$.

Soient A, B, C, D dans $\mathcal{M}_n(\mathbb{C})$ tels que $AC = CA$. Calculer $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix}$.

Il est évident que les deux premiers déterminants valent det Q et det R respectivement.

Quel est le lien avec la suite ? Peut-être qu'on peut trouver P, Q, R et S tels que

$$\begin{pmatrix} I_n & O \\ P & Q \end{pmatrix}\begin{pmatrix} R & S \\ O & I_n \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} ?$$

Allez voir en 4.34, où vous serez amené à supposer d'abord A inversible, puis à étendre le résultat grâce à la densité de $GL_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})$.

---

33. Soit H un espace de Hilbert réel. On suppose qu'il existe dans H une suite orthonormée $(e_i)_{i \geqslant 1}$ telle que l'espace Vect $\{e_i, i \geqslant 1\}$ soit partout dense dans H.

Soit $(x_n)_{n \geqslant 1}$ une suite d'éléments de H, telle que, pour tout n, $\|x_n\| \leqslant 1$.

Montrer qu'il existe une suite extraite $(x_{\varphi(n)})_{n \geqslant 1}$ et x^* dans H tels que :

$$\forall y \in H, \lim_{n \to +\infty} \langle x_{\varphi(n)}, y \rangle = \langle x^*, y \rangle .$$

Montrer que $\|x^*\| \leqslant 1$. Que peut on dire si $\|x^*\| = 1$.

Si on analyse l'énoncé, on s'aperçoit qu'il s'agit de démontrer une propriété $P(y)$, valable pour tout y de H, avec H adhérence de $F = \text{Vect}\{e_i, i \geqslant 1\}$. On peut donc penser vérifier la propriété sur les e_i, l'avoir sur F par linéarité, puis sur H par densité.

Comme les e_i sont dénombrables, on peut s'attendre à une extraction dénombrable de suites, et au procédé de la suite diagonale. Allez voir en 6.25.

---

34. Soit α réel. Déterminer $\lim_{n \to +\infty} \begin{pmatrix} 1 - \frac{\alpha}{n} & \\ \frac{\alpha}{n} & 1 \end{pmatrix}^n$.

A première vue, pas de problème, on calcule une puissance $n^{\text{ième}}$ d'une matrice 2×2, et on passe à la limite... Cependant, la forme de la matrice rappelle celle d'une... rotation, non vous n'y êtes pas, d'une similitude élevée à la puissance n. Cela se détermine facilement. C'est fait en 4.39.

---

35. Soit E l'ensemble des $(n+1)$ · uplets de complexes distincts.

Pour $Z = (z_0, z_1, ..., z_n)$ de E et P de $\mathbb{C}_n[X]$, on pose $N_Z(P) = \sum_{k=0}^{n} |P(z_k)|$. Montrer que N_Z est une norme sur $\mathbb{C}_n[X]$.

Pour Z et Z' dans E, comparer N_Z et $N_{Z'}$, et trouver $c > 0$ tel que $N_Z \leqslant c N_{Z'}$.

Vérifier que l'on a une norme, cela semble facile. On est en dimension finie où toutes les normes sont équivalentes, donc c existe. Il semble plus intéressant de réagir à : $n+1$ éléments distincts, je pense polynômes interpolateurs de Lagrange. C'est pourquoi j'ai traité cet exercice en algèbre, en 3.17.

---

36. Limite de la suite de terme général $u_n = n \int_1^{1+\frac{1}{n}} (1+t^n)^{\frac{1}{n}} dt$.

La présence d'un t^n et d'un ndt, m'incite à poser $u = t^n$, ce qui ramène l'intégrale sur $\left[1, \left(1+\frac{1}{n}\right)^n\right]$, avec $\left(1+\frac{1}{n}\right)^n$ qui tend vers e en croissant : cela doit être bon. Pour confirmation, aller en 8.22.

---

37. Soit $P \in \mathbb{R}[X]$ un polynôme admettant n racines réelles simples strictement supérieures à 1.

On pose $Q(X) = (X^2+1)P(X)P'(X) + X(P^2(X) + P'^2(X))$.

Montrer que Q admet au moins $2n-1$ racines réelles distinctes.

On est sur $\mathbb{R}$, des zéros d'une fonction continue peuvent s'obtenir par le Théorème des valeurs intermédiaires.

Par ailleurs, $\frac{P'}{P}$ fera intervenir les $\frac{1}{x-x_i}$, (les x_i étant les zéros simples de P), de limites infinies de signes différents si $x \to x_i^+$ ou x_i^- ... Enfin, annuler un produit c'est annuler l'un de ses facteurs... Et si on commençait par factoriser Q, considéré comme trinôme en X, (P et P' devenant des coefficients) ? C'est traité en 3.18.

---

38. Soit G un groupe fini, et H un sous-groupe de G, distinct de G. Pour x dans G, on pose $\bar{x} = \{g^{-1}xg, g \in G\}$. Montrer qu'il existe x dans G tel que $\bar{x} \cap H = \emptyset$.

Montrer que ce résultat devient faux si G n'est pas fini.

Comme $\bar{x}$ est l'orbite de x quand on fait agir G sur lui-même par automorphismes intérieurs, n'y aurait-il pas là une équation aux classes à considérer ?

Allez en 2.36 pour le savoir.

---

39. Soit E l'ensemble des matrices symétriques réelles d'ordre n.

a) Soit A dans E avec $I_n - A$ définie positive. Montrer que la suite $\left(\sum_{k=0}^{2p-1} (\text{trace } A^k)\right)_{p \in \mathbb{N}^*}$ est majorée.

b) On suppose de plus A à coefficients positifs. Montrer que $(I_n - A)^{-1}$ est à coefficients positifs.

Que sais-je sur la trace : elle est linéaire, et deux matrices semblables ont même trace. Je suis donc incité à penser $I_n + A + A^2 + ... + A^{2p-1}$, et, à l'identité :

$(I_n + A + ... + A^{2p-1})(I_n - A) = I_n - A^{2p}$, à « simplifier » par $(I_n - A)$, donc à justifier l'inversibilité de cette matrice ; se placer dans une base de diagonalisation de A... C'est faisable. Voir 5.24.

---

40. Soient a et b deux nombres complexes et M la matrice de $\mathcal{M}_n(\mathbb{C})$, de terme général m_{ij} avec $m_{ij} = a$ si $i > j$, $m_{ij} = 0$ si $i = j$ et $m_{ij} = b$ si $i < j$.

Valeurs propres, sous-espaces propres, et diagonalisation éventuelle de M.

Passons sur les cas faciles à traiter de $a = b = 0$, puis de $a = 0$ et $b \neq 0$ ou $a \neq 0$ et $b = 0$, et enfin de $a = b$.

Pour traiter le cas général, il faut dissocier le bloc des a de celui des b. Un moyen, c'est d'ajouter des x partout dans la matrice, et de constater que pour $x = -a$, elle devient triangulaire, et que pour $x = -b$, elle le devient aussi, d'où un calcul du polynôme caractéristique, que vous découvrirez en 4.49.

---

41. Montrer que, pour tout entier naturel n, on a $2^{(2^{6n+2})} + 3$ divisible par 19.

Il s'agit de calculs dans $\mathbb{Z}/19\mathbb{Z}$, avec 19 premier, donc (Théorème de Fermat) $a^{18} \equiv 1(19)$ pour tout a non nul modulo 19. On va donc, après modification de l'exposant, chercher à combien il est congru modulo 18 pour se simplifier la vie. Voir 2.37.

---

42. Soit E un espace vectoriel sur un corps K commutatif de caractéristique nulle, et $p_1, ..., p_k$ des projecteurs de E dont la somme est un projecteur. Montrer que si $i \neq j$, $p_i p_j = 0$.

Par quoi caractérise-t-on un projecteur, par l'égalité $p^2 = p$. De plus $E = \text{Ker } p \oplus \text{Im } p$, avec 1 et 0 seules valeurs propres, p diagonalisable, d'où trace $(p) = 1 \cdot \dim(\text{Im } p)$...

La trace est linéaire, on considère $p_1 + ... + p_k$, c'est bien le diable si à partir de ces ingrédients et avec un zeste de récurrence, la sauce ne prendra pas en 4.50.

---

43. Soit $A \in \mathcal{M}_n(\mathbb{C})$. On définit une suite A_k de matrices en posant $A_0 = A$ et, pour $k \geqslant 1$,

$$A_k = A\left(A_{k-1} - \frac{1}{k}\,\mathrm{trace}(A_{k-1})I_n\right).$$

Montrer que $A_n = 0$.

C'est déroutant, mais après réflexion, on constate que A_k est un polynôme en A, donc on peut espérer accrocher un polynôme annulant A, de degré $n+1$, avec X en facteur, donc justifier une égalité du type $A_n = A\chi_A(A)$, avec $\chi_A(X)$ polynôme caractéristique de A.

Le calcul étant sordide, une hypothèse du type A diagonale, (d'où des A_k diagonales) peut peut-être simplifier le calcul des traces.

Comme il s'avère que les fonctions symétriques des racines interviennent, je l'ai traité en 3.30, dans les exercices sur les polynômes.

---

44. L'entier $k \geqslant 2$ étant fixé, on définit f: $\mathbb{N} \mapsto \mathbb{N}$ par $f(n) = n + \mathrm{E}((n+n^{1/k})^{1/k})$.

Déterminer l'image de f.

Voici un énoncé « new look ». En effet, pour avoir une idée de ce qu'il faut justifier, mieux vaut utiliser un ordinateur, (ou une calculette programmable), pour faire calculer, pour $k = 2, 3, 4$ par exemple, les images des 100 ou 200 premiers entiers.

On s'aperçoit que pour $k = 2$, manquant 1, 4, 9, 16, 25..., les carrés quoi ; que pour $k = 3$ les cubes ne sont pas là, ce qui permet de justifier que $f(\mathbb{N}) = \mathbb{N} - \{m^k, m \in \mathbb{N}^*\}$, ce qui se fait en manipulant judicieusement l'encadrement.

$x - 1 < \mathrm{E}(x) \leqslant x$, valable pour tout x.

Voir en 2.39 pour plus de détails.

---

45. Soit A dans $\mathcal{M}_n(\mathbb{R})$, de terme général a_{ij}, avec $a_{ii} = 0$ pour tout i, et, si $i \neq j$, $a_{ij} + a_{ji} = 1$. Montrer que rang (A) $\geqslant n-1$.

Vu les hypothèses, on sent qu'il faut considérer $A + {}^tA$ qui est de terme constant 1 en dehors de la diagonale, avec des 0 sur la diagonale, ou encore avec J matrice de terme général 1, on a : $A + {}^tA = J - I_n$.

Comment relier au rang de A. Peut-être en cherchant le rang du système homogène $AX = 0$? Ce qui conduit, si le vecteur colonne X est tel que $AX = 0$ à considérer ${}^tX{}^tA = 0$, et aussi, pour profiter des deux égalités, à prendre

$${}^tX(A + {}^tA)X = 0 = {}^tXJX - {}^tXX \ldots$$

Aller voir en 4.57 si vous ne parvenez pas à résoudre avec tout cela.

---

46. Montrer que l'ensemble des suites à valeurs dans $\mathbb{N}$ n'est pas dénombrable.

S'il l'était, on aurait une « suite de suites », cela, c'est de la suite diagonale. Allez en 2.41 pour la mise en forme.

CHAPITRE II

Algèbre générale, arithmétique

Ce chapitre est celui où les structures sur les ensembles ont le plus d'importance. Il importe en effet de savoir de quelles lois de composition, relations d'ordre ou d'équivalence tel ou tel ensemble est muni, pour savoir de quels outils on dispose.

De plus, si on sait comment une structure donnée est introduite, on saura bien souvent comment traiter une question.

Ainsi, dans la structure de groupe, le fait de savoir qu'à tout sous-groupe on associe une (au moins) relation d'équivalence dont les classes d'équivalences sont équipotentes au sous-groupe, se traduit par des relations de divisibilité entre cardinaux du sous-groupe et du groupe, s'il est de cardinal fini. De ce fait, bien des questions d'arithmétique sont en fait résolues en considérant des groupes convenables.

Voir des applications de ceci et du **Théorème de Lagrange** en 2.1, 2.2., 2.6, 2.10, 2.13.

Une autre conséquence du Théorème de Lagrange est le fait que l'ordre d'un élément divise l'ordre du groupe, (2.23).

Après la structure de groupe vient celle d'anneau, et la notion d'idéal, (voir 2.3, 2.12, 2.14).

Ces deux structures existent sur $\mathbb{Z}$, qui de plus, est un anneau ordonné, d'où l'existence d'une division euclidienne, qui conduit à la numération, mais aussi à la notion de nombres premiers et à l'existence des décompositions en produit de puissances de nombres premiers, ce qui est fondamental pour ce qui touche à la divisibilité, (voir 2.5, 2.14, 2.18, 2.26).

Les identités, bien souvent valables dans les anneaux commutatifs, doivent être présentes à l'esprit, (voir 2.4).

Enfin, pensez à ces outils que sont :

- **Bézout**, (quand j'entends « premiers entre eux », je pense Bézout, (voir 2.16, 2.25),
- le petit **Théorème de Fermat**, (2.8), (2.37),
- la formule du **binôme de Newton**, (2.15), valable sur les anneaux commutatifs,

• la récurrence,

• l'existence d'un plus petit élément dans une partie non vide de $\mathbb{N}$, et d'un plus grand dans une partie non vide, majorée,

• le fait qu'un groupe n'est jamais réunion de deux sous-groupes sans que l'un contienne l'autre, (2.31),

• l'équation aux classes, quand un groupe opère sur un ensemble, (exercices 2.35 et 2.36),

• une expression en $a^r - 1$, (ou $A^n - I$ dans le cas de matrices), doit déclencher le réflexe « factorisation » en $(a-1)(a^{r-1} + ... + 1)$; voir 2.38,

• un sous-groupe distingué, c'est un noyau de morphisme de groupe, (2.2.),

• et de même, un idéal bilatère est un noyau de morphisme d'anneau,

• s'il vous faut un groupe non commutatif, pensez permutations d'un ensemble ; (2.7),

• pour un anneau non commutatif, $\mathcal{M}_n(K)$ fera l'affaire, (2.14).

Quand on manipule une suite de suites, un procédé de raisonnement est très utile : *celui de la suite diagonale.*

De quoi s'agit-il ? Eh bien, si on considère une indexation $(u^{(n)})_{n \in \mathbb{N}}$, de suites, avec $u^{(n)}$ suite de X, de terme général $u_p^{(n)}$, pour p variant dans $\mathbb{N}$, il s'agit de construire une suite v dont le $p^{\text{ième}}$ terme v_p sera calculé en fonction du $p^{\text{ième}}$ terme de la $p^{\text{ième}}$ suite, donc de $u_p^{(p)}$, le « calcul » se faisant de façon à obtenir ce que l'on veut.

Si ce procédé est surtout employé en topologie, voyez quand même en 2.41 une utilisation de ce mode de raisonnement.

Énoncés

2.1. Soit n dans $\mathbb{N}^*$ et a dans $\mathbb{Z}/n\mathbb{Z}$. On définit f_a de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ par $f_a(x) = ax$. Est-ce un morphisme d'anneau ?

On suppose a et n premiers entre eux, n ne divisant pas $a^{n-1} - 1$. Montrer que n n'est pas premier.

2.2. Soit G un groupe fini, H un sous-groupe de G et p le plus petit diviseur premier de card G. On suppose que $\dfrac{\text{card G}}{\text{card H}} = p$. Montrer que pour tout x de G, $x\text{H}x^{-1} = \text{H}$.

2.3. L'anneau $\mathbb{Z}[X]$ est-il principal ?

2.4. Condition nécessaire sur m pour que $2^m + 1$ soit premier.

2.5. Pour quelles valeurs entières $n \geqslant m$ a-t-on $\displaystyle\sum_{i=m}^{n} \frac{1}{i} \in \mathbb{N}$?

2.6. Trouver les morphismes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

2.7. Soit G un groupe commutatif et x et y deux éléments de G d'ordres respectifs α et β. Que peut-on dire de l'ordre de xy ?

Préciser dans le cas où α et β sont premiers entre eux.

Que peut-on dire si G n'est pas commutatif ?

2.8. Soient p et q deux nombres premiers tels que $q = 2p + 1 \geqslant 7$ et (a, b, c) dans $\mathbb{Z}^3$ tel que $a^p + b^p + c^p = 0$.

Montrer que p divise abc.

2.9. Soit G un groupe d'ordre $2p$, p premier. Montrer que G contient un élément d'ordre p.

2.10. Soit G abélien d'ordre pq, p et q premiers, distincts. Montrer que G est monogène.

2.11. Soit p premier, et U_p le sous-groupe multiplicatif de $\mathbb{C}^*$, engendré par l'ensemble des nombres $\exp\left(\dfrac{2i\pi}{p^\alpha}\right)$, où α décrit $\mathbb{N}$. Montrer que U_p ne peut être décomposé en produit direct de groupes non triviaux.

2.12. Soit A un anneau commutatif unitaire. Pour chaque x de A on note (x) l'idéal engendré par x. Soit a et b dans A. Montrer que si $(a)+(b)$ est un idéal principal, alors $(a)\cap(b)$ est également principal.

2.13. Soit p un nombre premier impair et q un diviseur premier de 2^p-1. Montrer que $q\equiv 1(2p)$.

2.14. Soit un anneau commutatif A. Vérifier que les éléments nilpotents de A forment un idéal. Ce résultat subsiste-t-il si A est non commutatif.

Avec n entier $\geqslant 2$, déterminer les éléments nilpotents de $\mathbb{Z}/n\mathbb{Z}$.

2.15. Soit n entier naturel et d_n le nombre de coefficients C_n^k, $0\leqslant k\leqslant n$, qui sont impairs. Montrer que d_n est une puissance de 2. (On pourra utiliser le développement de n en base 2.)

2.16. Soit G un groupe abélien tel qu'il existe n dans $\mathbb{N}^*$ vérifiant : $\forall x\in G, x^n=e$, élément neutre.

On suppose que $n=ab$ avec a et b premiers entre eux.

On pose $G_a=\{x^a \mid x\in G\}$, et $G_b=\{x^b, x\in G\}$.

Montrer que G_a et G_b sont des sous-groupes.

Montrer que, pour tout x de G, il existe un et un seul couple (u, v) de $G_a\times G_b$ tel que $x=uv$.

On suppose n impair. Montrer que $x\longrightarrow x^2$ est un automorphisme de G. Quelle est son application réciproque. Même question pour $x\longrightarrow x^k$, avec k entier premier à n.

2.17. Soit p un entier premier, congru à 1 modulo 4, et soit

$$S=\{(x,y,z)\in\mathbb{N}^3, x^2+4yz=p\}.$$

Montrer que l'on définit une application φ de S dans S en posant :

$\varphi(x,y,z)=(x+2z,z,y-z-x)$ si $x<y-z$;

$\varphi(x,y,z)=(2y-x,y,z+x-y)$ si $y-z<x<2y$;

$\varphi(x,y,z)=(x-2y,z-y+x,y)$ si $2y<x$.

Montrer que φ est une involution sur S, ayant un seul point fixe.

Que dire de la parité du cardinal de S ?

Montrer que toute involution d'un ensemble de cardinal impair possède au moins un point fixe. En déduire qu'il existe (u, v) dans $\mathbb{N}^2$ tel que $u^2+v^2=p$.

2.18. Pour n entier strictement positif, on note σ_n la somme des diviseurs (> 0) de n. Montrer que si m et n sont premiers entre eux, $\sigma_{mn} = \sigma_m \sigma_n$.

2.19. K est un corps de caractéristique nulle, G un sous-groupe fini de $\mathrm{GL}(n, \mathrm{K})$, de cardinal p.

Que peut-on dire de $\frac{1}{p} \sum_{M \in G} M$. Cas particulier de $\sum_{M \in G} M$ de trace nulle.

2.20. Montrer qu'il existe une infinité de points de $\mathbb{Q}^2$ sur le cercle $\Gamma = \{(x, y) \in \mathbb{R}^2 \,;\, x^2 + y^2 = 1\}$.

2.21. Nombre de relations binaires réflexives sur un ensemble à n éléments.

2.22. Soit n un entier $\geqslant 1$. Trouver n entiers consécutifs non premiers.

2.23. Montrer que 21 divise $2^{(4^n)} + 5$, pour tout n de $\mathbb{N}^*$.

2.24. Déterminer les deux derniers chiffres de l'écriture décimale de 3^{1993}.

2.25. Soit p un nombre premier. Trouver le nombre d'éléments inversibles dans $\mathbb{Z}/p^m\mathbb{Z}$.

2.26. Trouver tous les couples (x, y) de $\mathbb{N}^2$, tels que $x \neq y$ et $x^y = y^x$.

2.27. Soient $N_1, N_2, \ldots, N_q$ dans $\mathbb{Z}^*$, distincts, on pose $p_k = \prod_{i=1}^{q} (N_i + k)$ et on suppose que pour tout k de $\mathbb{Z}$, p_0 divise p_k. Montrer qu'il existe i tel que $|N_i| = 1$.

Si on suppose de plus que, pour tout i, $N_i \geqslant 1$, montrer que $N_1, \ldots, N_q$ sont les q premiers entiers naturels.

2.28. Soit (a, b) dans $\mathbb{N}^2$ avec $a \geqslant b > 0$. On sait qu'il existe (u, v) dans $\mathbb{Z}^2$ tel que $au + bv = a \wedge b = \mathrm{pgcd}(a, b)$.

Montrer qu'on peut trouver u et v sous la forme $u = \det A$ et $v = \det B$, où A et B sont deux matrices de la forme

$$\begin{pmatrix} * & 1 & 0 & \cdots\cdots & 0 & 0 \\ -1 & * & 1 & \cdots\cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & & * & 1 \\ 0 & 0 & 0 & & -1 & * \end{pmatrix}$$

les coefficients diagonaux et l'ordre étant à préciser.

2.29. Soit $p \in \mathbb{N}^*$, un entier non premier. Montrer que p ne divise pas $1 + (p-1)!$

2.30. Soit un entier premier $p \geqslant 5$, et N dans $\mathbb{N}$ défini par : $\sum_{k=1}^{p-1} \frac{1}{k^2} = \frac{N}{(p-1)!^2}$. Montrer que p divise N.

2.31. Que peut-on dire d'un anneau A tel que yx soit dans $\{xy, -xy\}$ pour tout couple (x, y) de A^2 ?

2.32. a) Soit $0 \leqslant p \leqslant n$, $(n, p) \in \mathbb{N}^2$. Calculer $\sum_{k=0}^{p} (-1)^k C_n^k C_{n-k}^{p-k}$.

b) Soit A_n le nombre de permutations σ de S_n, (groupe symétrique d'ordre n) n'ayant pas de point fixe. Montrer que $\sum_{k=0}^{n} C_n^k A_{n-k} = n!$

c) Montrer que $A_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$.

2.33. Soit $E = \{a + b\sqrt{2} \,;\, (a, b) \in \mathbb{Q}^2\}$. Montrer que c'est un sous-corps de $\mathbb{R}$, et en déterminer tous les automorphismes.

2.34. a) Montrer que le polynôme $X^3 - 2$ est irréductible dans $\mathbb{Q}[X]$.

On désigne par α l'une de ses racines complexes.

b) On pose $A = \{a + b\alpha + c\alpha^2 \,;\, (a, b, c) \in \mathbb{Q}^3\}$. Montrer que A est un sous-corps de $\mathbb{C}$.

2.35. a) Soit un groupe fini G, de cardinal p^α, $\alpha \geqslant 1$ et p nombre premier. On suppose que G agit sur un ensemble fini E. On note :

$E^G = \{x \in E, \forall g \in G, g \cdot x = x\}$.

Montrer que card (E) ≡ card (E^G) modulo (p).

b) Soit H un groupe fini d'ordre n, et p un diviseur premier de n. Montrer que H contient au moins un élément d'ordre p. On pourra considérer l'ensemble E des $(x_1, ..., x_p)$ de H^p tels que $x_1 x_2 ... x_p = 1$, (neutre de H), et faire opérer $\mathbb{Z}/p\mathbb{Z}$ sur E.

c) Soit H un groupe abélien fini d'ordre n, et m un entier tel que $\forall x \in H, x^m = 1$. Montrer qu'il existe α dans $\mathbb{N}$, tel que n divise m^α.

2.36. a) Soit G un groupe fini et H un sous-groupe de G, distinct de G. Pour x dans G, on pose $\bar{x} = \{g^{-1}xg, g \in G\}$. Montrer qu'il existe x dans G tel que $\bar{x} \cap H = \emptyset$.

b) Montrer que ce résultat devient faux si G n'est pas fini.

2.37. Montrer que, pour tout entier naturel n, $2^{(2^{6n+2})} + 3$ est divisible par 19.

2.38. Soit a et r des entiers supérieurs ou égaux à 2. Montrer que si $a^r - 1$ est premier, alors r est premier et $a = 2$.

2.39. L'entier $k \geqslant 2$ étant fixé, on définit f: $\mathbb{N} \mapsto \mathbb{N}$ par

$f(n) = n + E((n + n^{1/k})^{1/k})$.

Déterminer l'image de f.

2.40. On considère l'ensemble $\mathscr{A}$ des fonctions de variable réelle de la forme $P(x) + Q(x)\sqrt{1-x^2}$, où P et Q sont deux fonctions polynômes réelles.

Vérifier que $\mathscr{A}$ est un anneau pour les lois naturelles.

Quels sont les éléments inversibles de $\mathscr{A}$.

Montrer que x est irréductible dans $\mathscr{A}$.

2.41. Montrer que l'ensemble des suites à valeurs dans $\mathbb{N}$ n'est pas dénombrable.

2.42. Soit un groupe G où tout élément a pour carré l'élément neutre.

a) Montrer que G est abélien.

b) Soit H un sous-groupe de G, différent de G et a de G non dans H. Montrer que $H \cap aH = \emptyset$ et que $H \cup aH$ est un sous-groupe de G.

Solutions

2.1. Il est évident que f_a est un morphisme de groupe additif. Par contre, si f_a est morphisme d'anneau, l'égalité

$$f_a(xy) = a(xy) = f_a(x)f_a(y) = (ax)(ay) = a^2xy,$$

devant être valable pour tout x et y, donne, (avec $x = y = 1$), $a^2 = a$, donc pour $a = 0$ ou 1, f_0, (qui est nulle) et f_1, (identité) sont des morphismes d'anneau. Si n est premier, dans le corps $\mathbb{Z}/n\mathbb{Z}$ le polynôme $X^2 - X = 0$ n'a que ces deux zéros, 0 et 1. Si n n'est pas premier, tout autre élément a tel que $a^2 = a$ conduit à un morphisme d'anneau. C'est le cas de $a = 3$ dans $\mathbb{Z}/6\mathbb{Z}$ par exemple car $3^2 = 3$ dans cet anneau.

On peut préciser le noyau de f_a, morphisme de groupe additif, on a $f_a(x) = ax = 0 \Leftrightarrow ax$ divisible par n, (on confond ici les éléments de $\mathbb{Z}/n\mathbb{Z}$ et leurs représentants dans $[0, n-1]$), donc, avec $d = \text{pgcd}(a, n)$, en écrivant $a = da'$ et $n = dn'$ avec a' et n' premiers entre eux, on a encore :

$$f_a(x) = 0 \Leftrightarrow da'x \text{ divisible par } dn',$$

$$\Leftrightarrow a'x \text{ divisible par } n', \text{ avec } a' \text{ et } n' \text{ premiers entre eux, c'est équivalent à } x \text{ multiple de } n'.$$

On a f_a injective $\Leftrightarrow (n' = n) \Leftrightarrow \text{pgcd}(a, n) = 1$, et dans ce cas f_a est automorphisme de groupe, sinon $\text{Ker}\, f_a$ est formé des éléments de $\mathbb{Z}/n\mathbb{Z}$ multiples de $\dfrac{n}{\text{pgcd}(a, n)}$.

Si a et n sont premiers entre eux, et n premier, $\mathbb{Z}/n\mathbb{Z}$ étant un corps, $(\mathbb{Z}/n\mathbb{Z}) - \{0\}$ est groupe multiplicatif ayant $n-1$ éléments, donc tout élément x non nul vérifie l'égalité $x^{n-1} = 1$. Comme ici $a \neq 0$, modulo n, on a $a^{n-1} - 1 \equiv 0(n)$ ce qui contredit l'hypothèse n ne divise pas $a^{n-1} - 1$. Donc n n'est pas premier.

2.2. Il s'agit de montrer que le sous-groupe H est distingué, donc de l'obtenir comme noyau d'un morphisme de groupe.

Pour cela on considère l'ensemble quotient G/H de toutes les classes d'équivalences xH, pour x dans G, de la relation $\mathscr{R}$ définie par $x\mathscr{R}y \Leftrightarrow x^{-1}y \in \text{H}$.

On sait que ces classes d'équivalences sont toutes équipotentes à H, et qu'elles forment une partition de G, donc card $G/H = \dfrac{\text{card } G}{\text{card } H} = p$.

Pour g dans G, on *définit une bijection* $\theta(g)$ de G/H sur G/H en posant $\theta(g)(xH) = gxH$.

L'application $\theta(g)$ est *injective* car $\theta(g)(xH) = \theta(g)(yH)$ équivaut à l'égalité des classes de gx et de gy, donc à $gx\mathcal{R}gy$, soit à $(gx)^{-1}gy = x^{-1}g^{-1}gy = x^{-1}y$ dans H, d'où en fait $x\mathcal{R}y$ et $xH = yH$.

L'application $\theta(g)$ *est surjective*, car si yH est dans G/H, il est clair que $\theta(g)(g^{-1}yH) = g(g^{-1}y)H = yH$.

Donc θ est définie sur G, à valeurs dans le groupe $\mathcal{S}$ des bijections de G/H, groupe pour le produit de composition, de cardinal $p!$ Avec un peu de bonne volonté, θ sera un morphisme de groupes, de noyau H et on aura gagné.

L'application θ est un *morphisme de groupe* : soient g et g' dans G : $\theta(g) \circ \theta(g')$ est l'application qui à xH de G/H associe l'image par $\theta(g)$ de la classe de $g'x$, soit $gg'xH$, ce qui est précisément $\theta(gg')(xH)$, d'où $\theta(g) \circ \theta(g') = \theta(gg')$.

On a $\text{Ker } \theta \subset H$, car si $\theta(g)$ est la bijection identité de G/H sur G/H, en particulier $\theta(g)(H) = \theta(g)(eH) = geH = gH = H$: c'est que $g \in H$, (tout ceci avec e élément neutre de G).

Mais alors, ce morphisme de groupe θ, de G dans le groupe des permutations de G/H, donne l'isomorphisme :

$$\theta(G) \approx G/\text{Ker } \theta, \text{ d'où } (\text{card } G) = (\text{card Ker } \theta)\ \text{card } (\theta(G)).$$

Or G/H ayant p éléments, le groupe de ses permutations a $p!$ éléments et card $(\theta(G))$ est un diviseur de $p!$, mais c'est aussi card G/card (Ker θ), donc un diviseur de card G, donc tout facteur premier de la décomposition de card $(\theta(G))$ divisera card G qui admet p pour plus petit diviseur premier : on n'a pas le choix, soit card $(\theta(G)) = 1$, soit card $(\theta(G))$ est divisible par p, en étant diviseur de $p!$, avec p premier, c'est-à-dire card $(\theta(G)) = p$.

Mais card $(\theta(G)) = 1$ donne Ker $\theta = G$, avec $\text{Ker } \theta \subset H \subset G$ d'où $H = G$ et $p = \dfrac{\text{card } G}{\text{card } H}$ est exclu.

Il reste card $(\theta(G)) = \dfrac{\text{card } G}{\text{card (Ker } \theta)} = p = \dfrac{\text{card } G}{\text{card (H)}}$ avec Ker θ sous-groupe de H, tournez cela comme vous voulez, c'est que card (Ker θ) = card (H) fini, d'où l'inclusion $\text{Ker } \theta \subset H$ qui devient une égalité. Mais alors H, noyau d'un morphisme de groupe, est bien sous-groupe distingué.

2.3. Soit I l'idéal engendré par $1 + X^2$ et 2X, donc

$$I = \{(1 + X^2)P + 2XQ \ ; \ P \text{ et } Q \text{ dans } \mathbb{Z}[X]\}.$$

Comme $2(1 + X^2) + 2X(-X) = 2$ est dans I, si I est principal, il ne peut être formé que des multiples de 1 ou de 2.

Mais $1 + X^2$ est non multiple de 2, donc 2 n'engendre pas l'idéal I, alors que si $I = \mathbb{Z}[X]$ est engendré par 1, on aurait P et Q dans $\mathbb{Z}[X]$ avec :

$1 = (1 + X^2)P(X) + 2XQ(X)$, d'où, pour $X = 1$,

$1 = 2(P(1) + Q(1))$: 1 serait nul ou multiple de 2 puisque $P(1) + Q(1)$ est dans $\mathbb{Z}$. Curieux !

Donc $\mathbb{Z}[X]$ n'est pas un anneau principal.

2.4. Pour m impair, $m = 2n + 1$ avec $n \geqslant 1$, on a

$$\begin{aligned} 2^{2n+1} + 1 &= 2^{2n+1} + 1^{2n+1} \\ &= (2 + 1)(2^{2n} - 2^{2n-1} + 2^{2n-2} + \ldots + (-1)^p 2^{2n-p} + \ldots + 1) \\ &= 3q, \text{ avec } a \textit{ priori } q \in \mathbb{Z}, \text{ mais comme :} \end{aligned}$$

$2^{2n+1} + 1 \geqslant 2^3 + 1 = 9$, $q \geqslant 2$, donc $2^{2n+1} + 1$ est non premier.

Il est clair que pour $m = 0$ et 1, on a $2^0 + 1 = 2$ et $2^1 + 1 = 3$ qui sont premiers.

Enfin si m, pair, est du type $m = 2^k(2p + 1)$, avec k et p non nuls, on a :

$$2^m + 1 = \left(2^{(2^k)}\right)^{2p+1} + 1^{2p+1}, \text{ et avec la même identité, on}$$

obtient l'égalité, $\left(\text{avec } a = 2^{(2^k)}\right)$,

$$2^m + 1 = (a + 1)(a^{2p} - a^{2p-1} + \ldots + (-1)^k a^{2p-k} + \ldots + 1),$$

avec $2^m + 1 = a^{2p+1} + 1 > a + 1$ car $p \geqslant 1$: la parenthèse est un entier $\geqslant 2$, donc $2^m + 1$ n'est pas premier.

Finalement, il est nécessaire que m soit dans l'ensemble :

$$\{2^k \ ; \ k \in \mathbb{N}\} \cup \{0\},$$

pour que $2^m + 1$ puisse être premier.

Les nombres $F_n = 2^{(2^n)} + 1$ sont les nombres de Fermat.

On sait qu'un diviseur de F_n, s'il existe, sera de la forme $k \cdot 2^m + 1$, avec k entier impair et $m \geqslant n + 2$, (Théorème d'Euler et Test de Pépin).

Par exemple F_{1945} est divisible par $5 \times 2^{1947} + 1$,

F_{3310} est divisible par $5 \times 2^{3313} + 1$ et

F_{6537} est divisible par $17 \times 2^{6539} + 1$.

On peut, avec ces nombres de Fermat, occuper des ordinateurs.

2.5. On peut aborder l'exercice en se donnant m, et en cherchant s'il existe alors $n \geqslant m$ tel que la somme donnée soit un entier.

Le cas $n = m$ revient à dire que $\dfrac{1}{m}$ est un entier : on a donc $n = m = 1$ solution.

Peut-on trouver $n > m$? Dans ce cas, parmi les i variant de m à n figurent des nombres pairs et on va évaluer la valuation modulo 2.

Posons $x = \displaystyle\sum_{k=m}^{n} \frac{1}{k} = \frac{\displaystyle\sum_{k=m}^{n} \prod_{\substack{j=m \\ j \neq k}}^{n} j}{\displaystyle\prod_{k=m}^{n} k}$,

et pour chaque entier j on note $\varphi(j)$ l'exposant de 2 dans la décomposition de j en produit de puissances de nombres premiers.

Soit $r = \sup \{\varphi(j) ; m \leqslant j \leqslant n\}$, on a $r \geqslant 1$, (présence de nombres pairs), et ce sup est atteint en un seul j : il est atteint, (nombre fini de valeurs), et supposons que l'on ait j_1 et j_2 distincts, par exemple $j_1 < j_2$, avec $\varphi(j_1) = \varphi(j_2) = r$. On peut alors écrire :

$j_1 = 2^r a_1, j_2 = 2^r a_2$, avec a_1 et a_2 impairs, et $a_1 < a_2$: entre a_1 et a_2 figurera forcément un nombre pair, ne serait-ce que $2p_1 + 2$ si $a_1 = 2p_1 + 1$. Mais alors $j = 2^r(2p_1 + 2)$ est entre j_1 et j_2 donc entre m et n, avec $\varphi(j) \geqslant r + 1$: ceci contredit la définition de r.

On note alors l le seul élément entre m et n pour lequel $\varphi(l) = r$: pour tout $j \neq l$, entre m et n, on a $\varphi(j) < r$.

On note $\varphi\left(\displaystyle\prod_{k=m}^{n} k\right) = \sum_{k=m}^{n} \varphi(k) = s$, avec $s \geqslant r$, et si x est entier,

$\displaystyle\sum_{k=m}^{n} \prod_{\substack{j=m \\ j \neq k}}^{n} j$ est divisible par 2^s, donc *a fortiori* par 2^{s-r+1} puisque $r \geqslant 1$.

Or, $\varphi\left(\prod_{\substack{j=m \\ j\neq k}}^{n} j\right) = s - \varphi(k)$, donc, si $k \neq l$, comme $\varphi(k) \leqslant r-1$,

$s - \varphi(k) \geqslant s - r + 1$: chaque nombre $\prod_{\substack{j=m \\ j\neq k}}^{n} j$, pour $k \neq l$, est divisible par 2^{s-r+1}.

Quant à $\prod_{\substack{j=m \\ j\neq l}}^{n} j$, lui, il n'est divisible que par 2^{s-r} puisque l'exposant de 2 dans ce numérateur est $s - \varphi(l) = s - r$.

Finalement, le numérateur de x n'est divisible que par 2^{s-r} et x n'est pas entier.

La seule solution est $n = m = 1$.

2.6. Soit f un morphisme de $\mathbb{Q}$, groupe additif, dans $\mathbb{Z}$, groupe additif. Pour p dans $\mathbb{Z}$ et q dans $\mathbb{N}^*$, on a :

$$q \cdot \frac{p}{q} = \underbrace{\frac{p}{q} + \frac{p}{q} + \ldots + \frac{p}{q}}_{q \text{ fois}} = p$$

donc $f(p) = qf\left(\frac{p}{q}\right)$, puisque f est un morphisme additif. Mais alors $\frac{1}{q} f(p) = f\left(\frac{p}{q}\right)$ est dans $\mathbb{Z}$, et ceci, pour p fixé et q variant dans $\mathbb{N}^*$, n'est possible que pour $f(p) = 0$, (sinon l'entier $f(p)$ serait divisible par tout entier q), mais alors $f\left(\frac{p}{q}\right) = 0$.

Finalement, seul $f \equiv 0$, est un morphisme de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

2.7. Soient x et y d'ordres respectifs α et β dans G, groupe abélien, et m le p.p.c.m. de α et β.

On a $(xy)^m = x^m y^m$, (G est abélien)

$= 1$, (m multiple de α et β),

en notant 1 l'élément neutre du groupe multiplicatif G, donc l'ordre de xy divise $m = \alpha \vee \beta$.

On n'a pas mieux : par exemple dans le groupe G des rotations d'un plan vectoriel euclidien, la rotation x d'angle $\frac{\pi}{6}$ est d'ordre 12 ; la rotation y d'angle $\frac{\pi}{3}$ est d'ordre 6, le p.p.c.m. est 12, et la rotation xy, d'angle $\frac{\pi}{2}$ est d'ordre 4.

Si α et β sont premiers entre eux, alors l'ordre de xy est effectivement le p.p.c.m., égal ici à $\alpha\beta$.

En effet supposons que $(xy)^n = x^n y^n = 1$ avec x^n ou y^n différent de 1. Alors $z = x^n = (y^n)^{-1} = (y^{-1})^n$ est un élément à la fois dans le groupe cyclique engendré par x et dans celui engendré par y, de plus $z \neq 1$. Cet élément z a alors un ordre qui divise α et β, premiers entre eux, ce serait 1, mais $z^1 = z = 1$ est exclu.

Donc $(xy)^n = 1 \Rightarrow x^n = 1$ et $y^n = 1$, d'où n multiple de α et de β donc du p.p.c.m. de α et β.

Si G n'est pas abélien, le résultat du départ ne s'applique plus, ni le suivant.

Dans le groupe S_3 des permutations de $\{1, 2, 3\}$ la transposition $\tau : \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ est d'ordre 2, la permutation $\sigma : \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ est d'ordre 3, alors que $\sigma\tau : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ est une transposition d'ordre 2, différent ici de 2×3, (2 et 3 premiers entre eux).

Puis, avec la transposition $\tau' : \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, on a $\tau'\tau = \sigma$ d'ordre 3 qui ne divise pas 2, p.p.c.m. de 2 et de 2.

2.8. D'abord p et q existent : $p = 3$ et $q = 7$ conviennent.

De plus $p = 2$ est exclu donc p, premier est impair.

On peut diviser a, b et c par leur p.g.c.d., δ, ce qui revient à simplifier $a^p + b^p + c^p = 0$ par δ^p, et, en posant $a = \delta a', b = \delta b', c = \delta c'$, si on justifie que p divise $a'b'c'$, il divisera abc.

Supposons donc a, b et c premiers entre eux pour simplifier l'écriture : du fait de la relation ils sont premiers deux à deux car si r divise a et b par exemple, r premier, l'égalité $-c^p = a^p + b^p$ montre que r divise c.

Nos trois nombres sont donc deux à deux premiers entre eux.

Puis $q - 1 = 2p$, or dans le corps $K = \mathbb{Z}/q\mathbb{Z}$ tout élément non nul x vérifie l'égalité $x^{q-1} = 1$, (petit Théorème de Fermat, vient de K*

groupe multiplicatif de cardinal $q-1$), et avec $x = 0$, tout élément cette fois est tel que $x^{q-1} \in \{0, 1\}$.

Comme $(a^p)^2 = a^{q-1}$, il en résulte que $a^p \equiv 0, 1$ ou -1, modulo q. Il en est de même pour b^p et c^p.

Puis, l'égalité $-c^p = a^p + b^p$, avec p impair, conduit à l'identité :

$$-c^p = (a+b)(a^{p-1} - a^{p-2}b + \ldots + (-1)^i a^{p-i-1}b^i + \ldots + (-1)^{p-1}b^{p-1})$$

$$= (a+b)s, \text{ en notant } s = \sum_{i=0}^{p-1} (-1)^i a^{p-1-i}b^i.$$

Procédons par l'absurde en supposant que p ne divise pas abc.

Alors $a+b$ et s sont premiers entre eux, car si r, nombre premier, divise $a+b$ et s, on aurait $b = -a$ (modulo r), donc, modulo r, $s = \sum_{i=0}^{p-1} (-1)^i a^{p-1-i}(-a)^i$ soit $s = pa^{p-1} = 0$ modulo r, et si r, premier, divisait a, comme il divise $a+b$, il diviserait b, ce qui contredit $a \wedge b = 1$. Donc r divise p premier, c'est que $r = p$. Mais alors, p divise $a+b$ et s, donc aussi $-c^p$, donc aussi c, ce qui contredit l'hypothèse faite : p ne divise pas abc.

Donc on a $-c^p = (a+b)s$ avec $a+b$ et s premiers entre eux : en utilisant une décomposition en facteurs premiers de c, on élève à la puissance p et on « répartit » entre $a+b$ et s, premiers entre eux, c'est que $a+b$ d'une part, (et s d'autre part), sont du type x^p. Il existe donc $\gamma \in \mathbb{Z}$ tel que $a+b = \gamma^p$, et de même α et β dans $\mathbb{Z}$ tels que $b+c = \alpha^p$ et $c+a = \beta^p$ par symétrie.

Par ailleurs on a vu que a^p, b^p et c^p sont congrus à 0, 1 ou -1 modulo q, avec q premier $\geqslant 7$. Il en résulte que l'on a les trois congruences distinctes, car, deux égales à 1, par exemple $a^p \equiv 1(q)$ et $b^p \equiv 1(q)$, donneraient $-c^p \equiv 2(q)$ soit $c^p \equiv -2(q)$ et -2 non congru à 0, 1 ou -1 modulo q puisque $q \geqslant 7$.

De même a^p et b^p congrus à -1 donnerait $c^p \equiv 2(q)$, exclu, et $a^p \equiv b^p \equiv 0(q)$ donne $c^p \equiv 0(q)$ mais alors q, premier, diviserait a, b et c, que l'on a supposés premiers entre eux.

Donc, à une permutation près, on peut supposer que $a^p \equiv 1(q)$, $b^p \equiv -1(q)$ et $c^p \equiv 0(q)$.

Mais alors q divise c, et ne divise ni a, ni b, donc également, q ne divise ni $a+c$, ni $b+c$.

Comme $a+c = \beta^p$ et $b+c = \alpha^p$ sont congrus à 0, 1 ou – 1 modulo q, il reste $a+c$ et $b+c$ congrus à 1 ou – 1 modulo q, soit a et b congrus à 1 ou – 1 modulo q car $c \equiv 0(q)$, mais $b^p \equiv -1$ et $a^p \equiv 1$ impliquent $a \equiv 1(q)$ et $b \equiv -1(q)$.

Il est alors temps de se rappeler, qu'on avait signalé que $s = \sum_{i=0}^{p-1} a^{p-1-i}(-b)^i$ est du type x^p, donc congru à 1, – 1 ou 0 modulo q, ce qui ici donne 1, – 1 ou $0 = \sum_{i=0}^{p-1} 1 \cdot 1 = p$, modulo q, mais $q = 2p+1$ donne $2p \equiv -1(q)$ et ce qui précède donnerait $2p \equiv 0, 2$ ou $-2(q)$: il y a incompatibilité car $q \geqslant 7$.

On a finalement trouvé une absurdité : l'hypothèse p ne divise pas abc est à rejeter.

2.9. On note G multiplicativement, et e son élément neutre. Soit a dans $G - \{e\}$, son ordre divise $2p$, c'est donc 2, p ou $2p$. Si l'ordre est $2p$, G est cyclique engendré par a et a^2 est d'ordre p.

Si a est d'ordre p, c'est terminé.

Il resterait le cas de G tel que tout élément $a \neq e$ soit d'ordre 2. Soit a un tel élément, il engendre le sous-groupe $H_a = \{a, e\}$, distinct de G, donc il existe b, d'ordre 2, dans $G \backslash H_a$.

Alors $ab = e$ est exclu, sinon $b = a^{-1} = a \in H_a$. Puis $(ab)^2 = a(ba)b = e$, (ordre 2) implique :

$a^2(ba)b^2 = aeb$ soit $ba = ab$, et les éléments $\{e, a, b, ab = ba\}$ forment un sous-groupe H à 4 éléments de G : d'abord $ab = a$, $(\Rightarrow b = e)$ est exclu, puis on a un sous-groupe, de table :

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

puisque a et b commutent.

Mais alors 4 = card H divise $2p$, donc 2 divise p. Si $p = 2$, en fait vu l'hypothèse tout élément de $G - \{e\}$ est d'ordre 2, on a le résultat ; et si p premier est différent de 2, c'est que cette hypothèse, (tout élément d'ordre 2) est à exclure.

Dans tous les cas on a un élément d'ordre p.

2.10. Il faut donc justifier l'existence d'un élément d'ordre pq dans G. On sait que l'ordre d'un élément divise le cardinal, pq, de G, (Théorème de Lagrange), donc tout élément de $G - \{e\}$ est d'ordre p, q, ou pq.

Si tous les éléments de $G - \{e\}$ sont du même ordre, p par exemple, soit a d'ordre p, H_a le sous-groupe engendré est tel que tout a^r, $1 \leqslant r < p$, engendre aussi H_a car $a^r \neq e$, donc a^r engendre un sous-groupe de H_a, non réduit à $\{e\}$, son ordre qui divise p premier ne peut être que p.

Soit $b \notin H_a$, (il y en a dans $G \backslash H_a$), le sous-groupe engendré par a et b est alors :

$$L = \{a^r b^s \, ; \, 1 \leqslant r \leqslant p, \quad 1 \leqslant s \leqslant p\},$$

car G est abélien.

Ce sous-groupe est de cardinal p^2, car avec r, s, r', s' entre 1 et p, $(a^r b^s = a^{r'} b^{s'}) \Leftrightarrow (a^{r-r'} = b^{s'-s})$, et $r \neq r'$ (donc aussi $s' \neq s$) donnerait un générateur à la fois de H_a et de H_b, qui seraient confondus, d'où b dans H_a, ce qui est exclu.

Mais alors p^2 divise pq : c'est absurde.

On dispose donc de a d'ordre p, et de b d'ordre q, dans G, mais alors $(ab)^p = a^p b^p = b^p \neq e$, ($p$ non multiple de q) et aussi $(ab)^q = a^q b^q = a^q \neq e$.

L'élément ab, distinct de e (sinon $a = b^{-1}$ et a et b auraient même ordre q, premier), ne peut être que d'ordre pq = card G : le groupe est monogène.

2.11. Rappelons que si $G_1, G_2, \ldots, G_n$ sont n groupes multiplicatifs, on appelle produit direct de ces groupes, l'ensemble

$G = \{(x_1, \ldots, x_n) \, ; \, x_i \in G_i, \, 1 \leqslant i \leqslant n\}$, (produit cartésien), pour la loi de groupe (vérification facile) :

$(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n)$, l'élément neutre étant le n · uplet $(e_1, \ldots, e_n)$, avec e_i neutre de G_i.

Par ailleurs, si $n \geqslant 3$, il est bien clair qu'alors G est isomorphe au produit direct de G_1 et du produit direct $H = G_2 \times G_3 \times \ldots \times G_n$.

On va donc justifier que U_p ne peut pas être isomorphe à un produit direct $G \times H$ de deux groupes non triviaux.

Supposons qu'il existe un isomorphisme φ de U_p sur $G \times H$. Soit A et B les sous-groupes de U_p, respectivement égaux à $\varphi^{-1}(G \times \{e_H\})$ et $\varphi^{-1}(\{e_G\} \times H)$.

Si $x \in A \cap B$, c'est que $\varphi(x) \in G \times \{e_H\} \cap \{e_G\} \times H = \{(e_G, e_H)\}$, donc que $x = 1$, $(e_G \times e_H)$ étant élément neutre du groupe produit $G \times H$; donc $A \cap B = \{1\}$.

Puis, G n'étant pas réduit à $\{e_G\}$, A n'est pas réduit à $\{1\}$, et B non plus.

D'autre part un élément de U_p est du type :

$$u = \left(\exp \frac{2i\pi}{p^{\alpha_1}}\right)^{q_1} \left(\exp \frac{2i\pi}{p^{\alpha_2}}\right)^{q_2} \ldots \left(\exp \frac{2i\pi}{p^{\alpha_n}}\right)^{q_n}$$

avec $\alpha_1, \ldots, \alpha_n$ dans $\mathbb{N}$, $q_1, \ldots, q_n$ dans $\mathbb{Z}$.

C'est encore :

$$u = \exp\left(2i\pi\left(\frac{q_1}{p^{\alpha_1}} + \ldots + \frac{q_n}{p^{\alpha_n}}\right)\right), \text{ ce qui, en posant}$$

$\alpha = \sup\{\alpha_1, \ldots, \alpha_n\}$, se mettra sous la forme $u = \exp \dfrac{2iq\pi}{p^{\alpha}}$

avec $q = \sum_{k=1}^{n} q_k p^{\alpha - \alpha_k}$ dans $\mathbb{Z}$, et même, si q est divisible par p on simplifie, donc on peut imposer q non divisible par p, et comme on a supposé p premier, c'est que q et p sont premiers entre eux.

On a donc, si G et H sont non triviaux, l'existence de $a = \exp \dfrac{2iq\pi}{p^{\alpha}}$ dans $A - \{1\}$, avec $p \wedge q = 1$, $\alpha \in \mathbb{N}$, et de $b = \exp \dfrac{2ir\pi}{p^{\beta}}$ dans $B - \{1\}$, avec $r \wedge p = 1$, $\beta \in \mathbb{N}$.

Supposons par exemple $\alpha \geqslant \beta$, avec $\beta > 0$,

$(\beta = 0 \Rightarrow b = \exp 2ir\pi = 1)$.

Alors $c = a^{p^{\alpha-\beta}} = \exp \dfrac{2iq\pi}{p^{\beta}}$ avec $q \wedge p = 1$ et $\beta > 0$, donc $c \neq 1$, et c, puissance de a, est dans A, (sous-groupe), donc $c \in A - \{1\}$.

Comme q et p, (p premier), sont premiers entre eux, il en est de même de q et p^β donc, (Bézout), il existe u et v dans $\mathbb{Z}$ tels que $uq + vp^\beta = 1$, d'où

$$\exp \frac{2i\pi}{p^\beta} = \exp 2i\pi \left(\frac{uq + vp^\beta}{p^\beta} \right) = \left(\exp \frac{2iq\pi}{p^\beta} \right)^u \exp (2iv\pi)$$

$$= c^u \in A, \text{ et c'est} \neq 1, \left(\frac{1}{p^\beta} \text{ non entier} \right).$$

Mais on a aussi r et p^β premiers entre eux, donc il existe s et t dans $\mathbb{Z}$ tels que $rs + tp^\beta = 1$, donc là encore :

$$\exp \frac{2i\pi}{p^\beta} = \exp 2i\pi \left(\frac{rs + tp^\beta}{p^\beta} \right) = \left(\exp \frac{2ir\pi}{p^\beta} \right)^s \exp (2it\pi)$$

$$= b^s, \text{ élément de B}, \neq 1, \left(\text{encore } \frac{1}{p^\beta} \text{ non entier} \right).$$

Mais alors $\exp \dfrac{2i\pi}{p^\beta} \in A \cap B$, cet élément étant différent de 1, alors que $A \cap B = \{1\}$: c'est absurde.

Donc U_p n'est pas isomorphe à un produit direct.

2.12. Soit I l'idéal $(a) + (b)$, supposé principal, et x un générateur de cet idéal. Comme a et b sont dans I, il existe α et β dans A tels que $a = \alpha x$ et $b = \beta x$.

Mais alors $y = \alpha\beta x = \alpha \cdot b \in (b)$, et aussi $y = \beta \cdot (\alpha x) = \beta \cdot a \in (a)$, puisque A est commutatif, donc l'idéal principal engendré par y est dans $(a) \cap (b)$.

Inversement, si z est dans l'idéal $(a) \cap (b)$, il existe u et v dans l'anneau tels que $z = au = bv$.

Puisque $(x) = (a) + (b)$, on a aussi r et s dans A tels que :

$$x = ra + sb = r\alpha x + s\beta x = (r\alpha + s\beta)x, \text{ puis :}$$

$$z = au = \alpha ux = \alpha u(r\alpha + s\beta)x$$

$$= \alpha ur\alpha x + us(\alpha\beta x)$$

$$= (\alpha r)(\alpha xu) + (us)y.$$

Mais comme $z = au = bv = \alpha xu = \beta xv$, on a encore

$$z = (\alpha r)(\beta x v) + (us)y = (rv)\cdot(\alpha\beta x) + (us)y$$
$$= (rv)y + (us)y = (rv + us)y,$$

et finalement on a l'autre inclusion $(a) \cap (b) \subset (y)$, d'où l'égalité et le caractère principal de $(a) \cap (b)$.

2.13. L'entier $q-1$ sera divisible par $2p$, avec p nombre premier impair si et seulement si il l'est par 2 et par p.

Comme q, premier, divise $2^p - 1$, impair, $q-1$ est pair donc divisible par 2. Il reste à justifier la divisibilité de $q-1$ par p.

Dans le corps $K = \mathbb{Z}/q\mathbb{Z}$, ($q$ premier impair), l'élément classe de 2, encore noté 2, engendre un sous-groupe multiplicatif de $K - \{1\}$, donc son ordre divise $q-1$.

Or $2^p = 1$ dans $\mathbb{Z}/q\mathbb{Z}$, donc cet ordre divise p, ce n'est pas 1, ($2 \neq 1$ dans $\mathbb{Z}/q\mathbb{Z}$), cet ordre est p.

Finalement p divise $q-1$, d'où $q \equiv 1(2p)$.

Il convient de noter l'importance du Théorème de Lagrange, (l'ordre d'un sous-groupe divise l'ordre du groupe).

2.14. L'ensemble N des éléments nilpotents de A est non vide, (0 est nilpotent), stable par soustraction, car si a et b sont nilpotents d'ordres α et β respectivement, pour $n \geqslant \alpha + \beta$, on a

$$(a-b)^n = \sum_{k=0}^{n} C_n^k (-1)^k a^{n-k} b^k, \text{ la formule du binôme de Newton}$$

étant valable car l'anneau est commutatif.

Mais alors, si $k \geqslant \beta$, $b^k = 0$, alors que $k < \beta$, soit $-k > -\beta$, donne $n - k > \alpha + \beta - \beta = \alpha$, donc $a^{n-k} = 0$.

Finalement $a-b$ est nilpotent, d'où N sous-groupe additif.

C'est une partie permise, car avec a dans N, nilpotent d'ordre α, et x dans A, on a : $(ax)^\alpha = a^\alpha x^\alpha = 0$, donc $ax \in N$, d'où N idéal.

Dans l'anneau non commutatif $\mathcal{M}_2(\mathbb{R})$, les matrices $a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ et $b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ sont nilpotentes d'ordre 2, mais $a+b = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, régulière, n'est pas nilpotente, donc N n'est pas un idéal.

Dans $\mathbb{Z}/n\mathbb{Z}$, on aura a nilpotent si et seulement si il existe k entier tel que $a^k \equiv 0(n)$, mais ceci équivaut à a multiple du produit des facteurs premiers figurant dans la décomposition de n.

Plus précisément, soit $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ la décomposition en produit de facteurs premiers de n. Alors une puissance de a sera multiple de $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ si et seulement si chaque p_i divise a.

En prenant alors a compris entre 0 et n, on a :

si chaque $\alpha_i = 1$, seul $a = p_1 p_2 \dots p_k = n$ convient, mais $a \equiv 0(n) \Rightarrow$ seul 0 est nilpotent ;

s'il existe des $\alpha_i > 1$, les éléments nilpotents sont associés aux $a \leqslant n$, a multiple de $p_1 p_2 \dots p_k$.

Si $q = \dfrac{n}{p_1 p_2 \dots p_k} = \prod_{i=1}^{k} p_i^{(\alpha_i - 1)}$, chaque classe dans $\mathbb{Z}/n\mathbb{Z}$ d'un élément $a = m p_1 p_2 \dots p_k$, avec $1 \leqslant m \leqslant q$, est un élément nilpotent, et ces éléments distincts compris entre 1 et n donnent des classes distinctes dans $\mathbb{Z}/n\mathbb{Z}$.

2.15. Les coefficients du binôme se trouvent en calculant $(1+x)^n = \sum_{k=0}^{n} C_n^k x^k$, et, comme on veut évaluer le nombre de ces coefficients impairs, c'est-à-dire congrus à 1 modulo 2, on se place dans $K[x]$, avec $K = \mathbb{Z}/2\mathbb{Z}$, où, en notant α_k la classe de C_n^k, on a :

$$(1+x)^n = \sum_{k=0}^{n} \alpha_k x^k,$$

et on cherche le cardinal d_n des k tels que $\alpha_k = 1$, (les autres étant nuls).

L'énoncé suggère de décomposer n en base 2.

On a déjà, dans $K[x]$, $(1+x)^2 = 1 + x^2$, donc

$(1+x)^{2^2} = (1+x^2)^2 = 1 + x^4$, et, par récurrence sur p,

$(1+x)^{2^p} = 1 + x^{2^p}$, d'où $d_{2^p} = 2$.

Si on décompose n en base 2, en $n = \sum_{r=0}^{s} \beta_r 2^r$, avec $\beta_r = 0$ ou 1, on a :

$$(1+x)^n = \prod_{\substack{r=0 \\ r \text{ tel que } \beta_r = 1}}^{s} (1+x)^{2^r} = \prod_{\substack{r=0 \\ r \text{ tel que } \beta_r = 1}}^{s} (1+x^{2^r}).$$

On obtient, si on développe, et si $m = \text{card}\,\{r, \beta_r = 1\}$, une somme de 2^m monômes tous distincts, de coefficient 1, obtenus en prenant dans chaque facteur, 1 ou x^{2^r}.

Comme les valeurs de r sont distinctes, en notant $r_1, r_2, ..., r_m$ les m valeurs, (supposées ordonnées), et en posant, pour $1 \leqslant i \leqslant m$, $\varepsilon_i = 0$, (resp. 1), si dans le $i^{\text{ième}}$ facteur on choisit 1, $\left(\text{resp. } x^{2^{r_i}}\right)$, on obtient

$$(1+x)^n = \sum_{(\varepsilon_1, \varepsilon_2, ..., \varepsilon_m) \in \{0,1\}^m} x^{\varepsilon_1 2^{r_1} + ... + \varepsilon_m 2^{r_m}},$$

et les puissances $\varepsilon_1 2^{r_1} + ... + \varepsilon_m 2^{r_m}$ sont distinctes, pour des m-uplets différents, l'écriture en base 2 d'un entier étant unique.

Finalement, on a 2^m coefficients du binôme C_n^k, $0 \leqslant k \leqslant n$, impairs, avec m = nombre de chiffres non nuls dans la décomposition de n en base 2.

2.16. D'abord un tel groupe existe, celui des racines quinzièmes de l'unité par exemple.

Puis, G_a contient $e^a = e$, il est non vide, et si x et y sont dans G_a, avec $x = u^a$ et $y = v^a$, comme G est commutatif on a $xy^{-1} = (uv^{-1})^a$ dans G_a, qui est donc un sous-groupe.

Qui dit « premiers entre eux » déclenche... Bézout. Il existe donc p et q entiers relatifs tels que $pa + qb = 1$, donc pour tout x de G on a :

$$x = x^{pa+qb} = (x^a)^p (x^b)^q, \text{ avec } x^a \text{ dans } G_a, \text{ stable par « puissance »,}$$

donc $u = (x^a)^p$ dans G_a, et de même, $v = (x^b)^q$ dans G_b, d'où l'existence d'une écriture $x = uv$.

Si on a aussi $x = u'v' = uv$, c'est que $u^{-1}u' = vv'^{-1}$ est dans $G_a \cap G_b$. Notons alors z un élément de $G_a \cap G_b$. Il s'écrit $z = s^a = t^b$, donc $z^b = s^{ab} = s^n = e$ et $z^a = t^{ab} = t^n = e$, mais avec les mêmes p et q, on a :

$$z = z^1 = z^{ap+bq} = (z^a)^p (z^b)^q = e.$$

Donc $G_a \cap G_b = \{e\}$ et deux écritures $uv = u'v'$ de x quelconque conduisent à $u^{-1}u' = vv'^{-1} = e$ d'où $u = u'$ et $v = v'$.

Posons $\varphi(x) = x^2$, comme G est commutatif, on a :

$\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$ donc φ est un morphisme de groupe.

Comme n est supposé impair, avec $n = 2p+1$, en posant $\psi(y) = y^{p+1}$, on aura $(\varphi \circ \psi)(y) = (y^{p+1})^2 = y^{2p+2}$

$$= y^n \cdot y = y,$$

vu l'hypothèse sur G, mais aussi :

$$(\psi \circ \varphi)(x) = (x^2)^{p+1} = x^{2p+2} = x^n \cdot x = x.$$

Donc $\varphi \circ \psi = \psi \circ \varphi = \mathrm{id}_G$, d'où φ automorphisme d'automorphisme réciproque ψ.

Plus généralement, avec k premier à n, p et q tels que $pk + qn = 1$, si on pose $\varphi(x) = x^k$ et $\psi(x) = x^p$, on aura φ et ψ morphismes, et :

$$\varphi(\psi(x)) = (x^p)^k = x^{1-qn} = x \cdot (x^n)^{-q} \text{ avec } x^n = e,$$

donc $\varphi \circ \psi = \mathrm{id}_G$ et c'est aussi $\psi \circ \varphi$ donc φ et ψ sont des automorphismes réciproques l'un de l'autre.

2.17. Avec $p = 4q+1$, l'ensemble S n'est pas vide, car avec $x = 1$ et $y = q$, $z = 1$ (ou $y = 1, z = q$), on a des points de S.

De plus S est fini car l'égalité $x^2 + 4yz = p$, avec p premier, exclut la possibilité d'avoir y ou z nul, et, comme on a des entiers, on a $x \leqslant \sqrt{p}$ d'une part, puis $4yz \leqslant p \Rightarrow y \leqslant \dfrac{p}{4z} \leqslant \dfrac{p}{4}$ car $z \geqslant 1$, et de même $z \leqslant \dfrac{p}{4}$.

La manière de définir φ est cohérente, le seul problème venant de l'inégalité $y - z < 2y$, or l'inégalité $2y \leqslant y - z \Leftrightarrow y + z \leqslant 0$, avec y et z dans $\mathbb{N}$, elle n'est possible que si $y = z = 0$ d'où $x^2 = p$ avec p premier et x entier : c'est exclu. Donc pour les points de S on a forcément $y - z < 2y$ et après, on ne peut pas avoir $x = y - z$, sinon

$(y-z)^2 + 4yz = (y+z)^2 = p$ premier : non ; ni $x = 2y$, car alors on aurait, sur S, $4y^2 + 4yz = 4y(y+z) = p$, avec $p \equiv 1(4)$: non.

On place alors x par rapport à $y - z$ et $2y$ d'où la « partition » de S utilisée pour définir φ, (les guillemets car des parties peuvent être vides).

On doit vérifier que $\varphi(S) \subset S$. Il est clair que $\varphi(S) \subset \mathbb{N}^3$. Dans le deuxième cas par exemple, on vérifie que

$$(2y-x)^2 + 4y(z+x-y) = 4y^2 - 4xy + x^2 + 4yz + 4xy - 4y^2$$

$$= x^2 + 4yz = p.$$

On procèderait de même dans les autres cas, d'où $\varphi(S) \subset S$.

Puis $\varphi^2 = \mathrm{id}_S$. Supposons (x, y, z) dans S avec $x < y - z$.

Soit $(X, Y, Z) = \varphi(x, y, z) = (x + 2z, z, y - z - x)$. On a :

$2Y - X = 2z - 2z - x < 0$, ($x = 0$ est exclu, sinon $4yz = p$, p premier : c'est difficile, d'autant que $p \equiv 1(4)$), d'où $2Y < X$, donc $\varphi(X, Y, Z) = (X - 2Y, Z - Y + X, Y)$, soit :

$$\varphi^2(x, y, z) = (x + 2z - 2z, y - z - x - z + x + 2z, z) = (x, y, z).$$

Je suppose que dans les deux autres cas il en est de même. Je vous avouerai que je ne l'ai pas vérifié.

D'où $\varphi^2 = \mathrm{id}_S$.

Point fixe. Peut-on avoir $x < y - z$ et $\varphi(x, y, z) = (x, y, z)$, soit entre autres, $x + 2z = x$? Non, car $z = 0$ conduit à $x^2 = p$, p premier, c'est exclu.

Peut-on avoir $2y < x$ et (x, y, z) point fixe ? On devrait avoir $x - 2y = x$ d'où $y = 0$ et la même impossibilité.

Enfin, avec $y - z < x < 2y$, on aura un point fixe si de plus :

$2y - x = x$, d'où $y = x$;

$y = y$, c'est possible ;

$z + x - y = z$, c'est encore $x = y$.

Pour être dans S, il faut de plus que $x^2 + 4xz = 4q + 1 = p$, soit $x(x + 4z) = p$, premier, d'où $x = 1$ et $x + 4z = p$, (car $x = p$ et $x + 4z = 1$, donnerait $x = p = 1$ et $z = 0$: exclu), d'où

$$z = \frac{p - x}{4} = \frac{4q + 1 - 1}{4} = q$$: *on a un seul point fixe*, si ce point $\left(1, 1, \frac{p - 1}{4}\right)$ vérifie la double inégalité $y - z < x < 2y$ soit $1 - \frac{p - 1}{4} < 1$: vrai ; et $1 < 2$: vrai.

On considère alors l'action du groupe $G = \{\mathrm{id}_S, \varphi\}$ sur S, en notant a le point fixe. L'orbite de a est de cardinal 1, les autres sont de cardinal 2, ($\forall x \neq a$, $\varphi(x) \neq x$ et $\varphi^2(x) = \mathrm{id}_S(x)$), s'il y a k orbites on a $2k + 1$ éléments dans S, (équation aux classes).

Il en résulte aussi que toute involution sur S aura au moins un point fixe, et ceci est vrai sur tout ensemble de cardinal impair.

Or $\psi : (x, y, z) \rightsquigarrow (x, z, y)$ est une involution sur S, (rôles symétriques de y et z dans la définition de S), donc ψ admet un point fixe (u, v, w), tel que $\psi(u, v, w) = (u, v, w)$, d'où $v = w$, et l'égalité $u^2 + 4v^2 = p = u^2 + (2v)^2$: l'équation $x^2 + y^2 = p$ a bien une solution.

2.18. Si p divise m et q divise n, le produit pq divise mn. Puis si r divise mn, si p est un nombre premier divisant r, d'exposant α dans la décomposition de r en produit de facteurs premiers, p divise m, ou n, mais pas les deux puisqu'ils sont premiers. Si par exemple p divise m, on a p^{α} divise m, et finalement r s'écrit sous la forme $r = uv$ avec u divise m et v divise n.

Si on note S_n l'ensemble des diviseurs de n, on a donc :

$$S_{mn} = \{uv\ ;\ u \in S_m, v \in S_n\},$$

lorsque m et n sont premiers entre eux.

$$\text{Donc } \sigma_{mn} = \sum_{(u,v) \in S_m \times S_n} uv = \sum_{u \in S_m} u \left(\sum_{v \in S_n} v \right)$$

$$= \sigma_n \sum_{u \in S_m} u = \sigma_n \sigma_m = \sigma_m \sigma_n.$$

2.19. Si on note $A = \sum_{M \in G} M$, cette somme est stable si on permute les éléments du groupe fini G, or pour M_0 fixé dans G, l'ensemble des M_0M, lorsque M parcourt G, redonne G, (on translate à gauche dans un groupe), donc $M_0A = A$.

Mais alors, (pas de jaloux) :

$$\sum_{M_0 \in G} M_0 A = pA = \left(\sum_{M_0 \in G} M_0 \right) A = A^2, \text{ et } \textit{a fortiori} \text{ en notant}$$

$U = \frac{1}{p} \sum_{M \in G} M = \frac{1}{p} A$, on a :

$$U^2 = \frac{1}{p^2} A^2 = \frac{1}{p^2} pA = \frac{1}{p} A = U,$$

donc U est un projecteur.

Si A est de trace nulle, U est de trace nulle, donc ce projecteur est nul, (valeurs propres 1 et 0, un projecteur est diagonalisable, donc sa trace est la dimension de l'image).

2.20. Avoir $u = \frac{p}{q}$ et $u' = \frac{p'}{q'}$, rationnels écrits sous forme irréductible, tels que $u^2 + v^2 = 1$, implique que $q'^2p^2 + q^2p'^2 = q^2q'^2$, d'où des entiers $a = q'p$, $b = qp'$ et $c = qq'$ tels que $a^2 + b^2 = c^2$.

Réciproquement, avec a, b et c entiers tels que : $a^2 + b^2 = c^2$, si c est non nul, ($c = 0$ impliquant $a = b = 0$), les rationnels $u = \pm \frac{a}{c}$ et $v = \pm \frac{b}{c}$ vérifiant l'égalité $u^2 + v^2 = 1$.

Or, avec a, b et c entiers, $a^2 + b^2 = c^2$ équivaut à

$$a^2 = c^2 - b^2 = (c-b)(c+b).$$

Pour b quelconque et $c = b+1$, cette égalité s'écrit $a^2 = 2b+1$.

Mais alors, partant de a entier impair, $a = 2n+1$, on aura $a^2 = 2(2n^2+2n)+1$, donc on peut poser : $b = 2n^2+2n$ et $c = 2n^2+2n+1$, d'où $u = \pm \dfrac{2n+1}{2n^2+2n+1}$, $v = \pm \dfrac{2n^2+2n}{2n^2+2n+1}$, tels que $u^2 + v^2 = 1$, u et v dans $\mathbb{Q}$, et il suffit de vérifier que, pour n variant, on a une infinité de valeurs distinctes.

Le numérateur de la dérivée de $f : x \longrightarrow \dfrac{2x+1}{2x^2+2x+1}$ est, sauf erreur, $-4x^2 - 4x$, donc négatif pour x positif. Cette fonction de x est strictement monotone pour $x \geqslant 0$, donc les n de $\mathbb{N}$ distincts donnent des $f(n)$ distincts : on a bien une infinité de points de $\mathbb{Q}^2$ sur le cercle.

2.21. Soit E de cardinal n. Une relation binaire $\mathscr{R}$ est déterminée par la partie $\mathscr{P}(\mathscr{R})$ de $E \times E$ formée des couples (x, y) tels que $x\mathscr{R}y$, (en particulier il y a 2^{n^2} relations binaires), et dire que $\mathscr{R}$ est réflexive donc que $x\mathscr{R}x$ pour tout x, équivaut à dire que la diagonale $\Delta = \{(x, x), x \in E\}$ est dans $\mathscr{P}(\mathscr{R})$. Comme il reste $n^2 - n$ couples possibles à adjoindre à Δ, on a 2^{n^2-n} relations binaires réflexives.

2.22. Un tel exercice ne compte pas : vous devez en faire un autre. En effet, pour tout k vérifiant $2 \leqslant k \leqslant n+1$, $x_k = k + (n+1)!$ est divisible par k, ce qui donne bien n entiers consécutifs non premiers.

2.23. Comme $21 = 3 \times 7$, l'exercice équivaut à justifier que $2^{(4^n)} + 5$ est divisible par 3 et par 7.

Dans le groupe multiplicatif $\mathbb{Z}/3\mathbb{Z} - \{\bar{0}\}$, $\bar{2}$ est d'ordre 2, donc 4^n étant pair, on a $\bar{2}^{(4^n)} = \bar{1}$, d'où $2^{(4^n)} + 5 \equiv (1+5)(3)$, soit encore $\equiv 0(3)$.

Pour la divisibilité par 7, on doit justifier que $2^{(4^n)}$ est congru à 2 modulo 7, ou encore, que dans le groupe multiplicatif $\mathbb{Z}/7\mathbb{Z} - \{0\}$, on a : $\bar{2}^{(4^n)} = \bar{2}$, soit $\bar{2}^{(4^n-1)} = \bar{1}$, ce qui revient à justifier que l'ordre de $\bar{2}$ divise $4^n - 1$. Comme $2^3 = 8$, on a $\bar{2}^3 = \bar{1}$: l'ordre de $\bar{2}$ est 3, or $4 \equiv 1(3)$, donc $4^n \equiv 1(3)$ et $4^n - 1$ est bien divisible par 3.

2.24. On cherche à quoi est congru 3^{1993}, modulo 100, ce qui revient à chercher le plus petit entier p tel que $3^p \equiv 1 \mod (100)$, puis à diviser 1993 par p pour ne considérer que le reste r et 3^r modulo 100.

Comme $3^p = 100k + 1 = 10 \cdot (10k) + 1$, si p convient on a $3^p \equiv 1$ modulo 10, donc p est multiple du plus petit q tel que $3^q \equiv 1(10)$.

On a $3 \equiv 3(10)$, $3^2 \equiv 9(10)$, $3^3 \equiv 7(10)$, $3^4 \equiv 1(10)$, donc p est du type $4k$, et alors $3^p = (3^4)^k = (81)^k$.

On a
$$3^4 = 81^1 \equiv 81 \mod 100,$$
$$3^8 = 81^2 \equiv 61 \mod 100,$$
$$3^{12} = 81^3 \equiv 41 \mod 100,$$
$$3^{16} = 81^4 \equiv 21 \mod 100,$$
$$3^{20} = 81^5 \equiv 1 \mod 100,$$

tous ces calculs se faisant de tête car, par exemple, $61 = 60 + 1$ et $81 = 80 + 1$ donc $61 \times 81 = 4\,800 + 60 + 80 + 1 \equiv 40 + 1 \mod 100$...

Puis $1993 = 20 \times 99 + 13$, donc $3^{1993} = (3^{20})^{99} \times 3^{13}$ est congru à 3^{13} modulo 100, avec $3^{13} = 3^{12} \times 3$ et 3^{12} congru à 41 modulo 100, donc 3^{13} congru à $3 \times 41 = 123$ modulo 100 et finalement $3^{1993} \equiv 23$ modulo 100.

Remarque. Si on veut les trois derniers chiffres, on cherche d'abord le plus petit entier n tel que $3^n \equiv 1 \mod 1\,000$, ce qui implique $3^n \equiv 1 \mod 100$, donc n est du type $k \cdot 20$. On cherche alors à quoi est congru 3^{20}, modulo 1 000, pour trouver le plus petit k tel que $(3^{20})^k \equiv 1 \mod 1\,000$...

2.25. Avoir un élément x inversible dans $\mathbb{Z}/n\mathbb{Z}$, c'est-à-dire avoir l'existence de y tel que $xy = 1$, avec x représenté par l'entier q, revient à dire qu'il existe u, représentant y, tel que $qu \equiv 1 \mod n$, ce qui équivaut à l'existence de v dans $\mathbb{Z}$ tel que $qu + nv = 1$, donc (Bézout à la rescousse) que q et n sont premiers entre eux.

Si $n = p^m$, avec p nombre premier, on est donc ramené à compter le nombre d'entiers n, compris entre 1 et p^m, premiers à p, c'est-à-dire non du type kp, avec $1 \leqslant k \leqslant p^{m-1}$. Il y a donc $p^m - p^{m-1}$ éléments inversibles dans $\mathbb{Z}/p^m\mathbb{Z}$, si p est premier.

On conçoit que l'on peut aborder ensuite le cas de $n = p_1^{m_1} p_2^{m_2}$, avec p_1 et p_2 premiers : il faut évaluer les entiers non multiples de p_1, ni de p_2.

Or il y a $\dfrac{n}{p_1}$ multiples de p_1 inférieurs à n ; $\dfrac{n}{p_2}$ multiples de p_2 inférieurs à n, et $\dfrac{n}{p_1 p_2}$ multiples à la fois de p_1 et de p_2 : il reste donc $n - \dfrac{n}{p_1} - \dfrac{n}{p_2} + \dfrac{n}{p_1 p_2}$ éléments inversibles dans $\mathbb{Z}/p_1^{m_1} p_2^{m_2}\mathbb{Z}$, avec p_1 et p_2 premiers, et $n = p_1^{m_1} p_2^{m_2}$.

2.26. On décompose x et y en produits de puissances de nombres premiers sous la forme $x = \prod_{p \in \mathscr{P}_x} p^{\alpha_p}$ et $y = \prod_{q \in \mathscr{P}_y} q^{\beta_q}$, $\mathscr{P}_x$ et $\mathscr{P}_y$ désignant les nombres premiers figurant, (en nombre fini) dans ces décompositions, les α_p et β_q étant entiers non nuls, ceci si x et y sont non nuls.

L'égalité $x^y = y^x$ étant impossible si $x = 0$ et $y \neq 0$, cette écriture de x et y est licite, et $x^y = y^x$ s'écrit :

$$\prod_{p \in \mathscr{P}_x} p^{y\alpha_p} = \prod_{q \in \mathscr{P}_y} q^{x\beta_q},$$

avec x et y non nuls. Mais alors les ensembles $\mathscr{P}_x$ et $\mathscr{P}_y$ sont les mêmes, et en écrivant $y = \prod_{p \in \mathscr{P}_x} p^{\beta_p}$, on a les égalités $y\alpha_p = x\beta_p$, pour tout facteur premier p.

Comme $x \neq y$, supposons par exemple $x < y$, l'égalité entre entiers : $y\alpha_p = x\beta_p$ implique $\beta_p > \alpha_p$ donc p^{α_p} divise p^{β_p}, et ce pour tout facteur premier p de $\mathscr{P}_x = \mathscr{P}_y$, finalement x divise y.

Posons $y = kx$ avec k entier $\neq 1$ et $\neq 0$. On doit avoir $x^{kx} = (kx)^x$ ou encore $x^{x(k-1)} = k^x$, soit encore $x(k-1)\ln x = x\ln k$, avec $x \neq 0$, donc x et k sont tels que $(k-1)\ln x - \ln k = 0$.

Étudions, pour x fixé, la fonction $k \rightsquigarrow f(k) = (k-1)\ln x - \ln k$, on a $f'(k) = \ln x - \frac{1}{k}$.

Mais pour x entier $\geqslant 3$, $\ln x > 1$, et comme k est entier > 1, $\frac{1}{k} < 1$, donc $f'(k) > 0$ si $k > 1$: la fonction f est croissante et $f(1) = 0$: pour $k > 1$ elle ne s'annule pas.

S'il y a des solutions, ce ne peut être qu'avec $x = 1$ ou 2.

Pour $x = 1$, on doit avoir $-\ln k = 0$, donc $k = 1$ et $y = 1 = x$, c'est exclu.

Pour $x = 2$, on doit avoir $(k-1)\ln 2 - \ln k = 0$, qui admet $k = 2$ pour solution, unique car avec cette fois $f(k) = (k-1)\ln 2 - \ln k$ et $f'(k) = \ln 2 - \frac{1}{k}$, qui s'annule en $k = \frac{1}{\ln 2}$, on a pour variations :

k	1		$\frac{1}{\ln 2}$		$+\infty$
$f'(k)$		$-$	0	$+$	
$f(k)$	0	↘	0	↗	$+\infty$

donc f admet un seul zéro > 1, c'est $k = 2$, d'où $y = 4$.

Finalement les couples solutions sont (2, 4) et (4, 2).

2.27. Comme p_0 divise p_1 et p_{-1}, $\frac{p_1 p_{-1}}{p_0^2}$ est un entier, r, avec $r = \prod_{i=1}^{q} \frac{(N_i - 1)(N_i + 1)}{N_i^2} = \prod_{i=1}^{q} \left(1 - \frac{1}{N_i^2}\right)$, et, si pour tout i, $|N_i| > 1$, chaque facteur $1 - \frac{1}{N_i^2}$ étant dans $]0, 1[$, r ne serait pas entier. Donc il existe i tel que $|N_i| = 1$.

On suppose désormais les N_i dans $\mathbb{N}^*$, donc $\geqslant 1$, on a alors l'existence de i tel que $N_i = 1$, on peut supposer l'indexation telle que $N_1 = 1$.

Supposons justifiée l'hypothèse de récurrence $\mathscr{H}_r$ suivante, avec $1 \leqslant r \leqslant q$, $\mathscr{H}_r$: on a r entiers N_i valant 1, 2, ..., r.

$\mathscr{H}_1$ est vérifiée, on suppose $\mathscr{H}_r$ vérifiée avec $r < q$, et l'indexation telle que $N_1 = 1, N_2 = 2, ..., N_r = r$. Les N_i étant distincts, si $i > r$ on aura $N_i > r$.

On a alors p_{-r-1} divisible par p_0, ce qui s'écrit encore :

$$s = \frac{p_{-r-1}}{p_0} = \prod_{i=1}^{r} \frac{(i-r-1)}{i} \prod_{i=r+1}^{q} \frac{N_i - r - 1}{N_i}, \text{ entier, avec :}$$

$$s = \frac{(-r)(-(r-1))...(-1)}{r!} \prod_{i=r+1}^{q} \left(1 - \frac{r+1}{N_i}\right) = (-1)^r \prod_{i=r+1}^{q} \left(1 - \frac{r+1}{N_i}\right)$$

entier.

Si alors, pour chaque $i \geqslant r+1$, on avait $N_i > r+1$, les $1 - \frac{r+1}{N_i}$ seraient dans]0, 1[, leur produit aussi, et s ne serait pas entier relatif : c'est exclu.

Il existe donc $i_0 \geqslant r+1$ avec $N_{i_0} \leqslant r+1$, et comme les entiers non nuls, N_j sont tous distincts, $\geqslant 1$, et que 1, 2, ..., r sont déjà pris, on a $N_{i_0} = r+1$ d'où $\mathscr{H}_{r+1}$.

Par récurrence $\mathscr{H}_q$ est vraie, d'où le résultat.

2.28. On va en fait s'inspirer de l'algorithme d'Euclide.

Si on divise a par b, on a q_0 et r_0, $0 \leqslant r_0 < b$, tels que $a = q_0 b + r_0$, et soit $r_0 = 0$, auquel cas $a \wedge b = b$, soit $r_0 > 0$ et dans ce cas $a \wedge b = b \wedge r_0$. On divise b par r_0 ...

En fait on introduit une suite double, (r_n, q_n), avec :

$$a = q_0 b + r_0 \quad , \quad 0 < r_0 < b ;$$

$$b = q_1 r_0 + r_1 \quad , \quad 0 < r_1 < r_0 ;$$

$$r_0 = q_2 r_1 + r_2 \quad , \quad 0 < r_2 < r_1 ;$$

- -

$$r_{n-2} = q_n r_{n-1} + r_n \quad , \quad 0 < r_n < r_{n-1} ;$$

$$r_{n-1} = q_{n+1} r_n$$

et $a \wedge b = r_n$. Le processus s'arrête car la suite des r_k est strictement décroissante : au bout de b divisions au plus on a un reste r_{n+1} nul.

À chaque couple (a, b) d'entiers non nuls, on associe donc un entier n, et une suite de quotients $q_0, q_1, \ldots, q_n$.

Nous allons justifier, par récurrence sur n, que :

$$r_n = a \wedge b = a \begin{vmatrix} -q_1 & 1 & 0 & \ldots & 0 & 0 \\ -1 & -q_2 & 1 & \ldots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & & -q_{n-1} & 1 \\ 0 & 0 & 0 & & -1 & -q_n \end{vmatrix} + b \begin{vmatrix} -q_0 & 1 & 0 & \ldots & 0 & 0 \\ -1 & -q_1 & 1 & \ldots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & & -q_{n-1} & 1 \\ 0 & 0 & 0 & & -1 & -q_n \end{vmatrix}.$$

Si $n = 1$, on a : $a = q_0 b + r_0$ et $b = q_1 r_0 + r_1$, donc :

$aq_1 = q_0 q_1 b + q_1 r_0 = q_0 q_1 b + b - r_1$ d'où

$r_1 = a \wedge b = (q_0 q_1 + 1)b - aq_1$

$$= a|-q_1| + b \begin{vmatrix} -q_0 & 1 \\ -1 & -q_1 \end{vmatrix}.$$

Si on suppose le résultat vrai pour tout couple d'entiers, dont l'entier associé est $\leqslant n$; soient alors a et b conduisant à $n+1$ et une suite $q_0, q_1, \ldots, q_{n+1}$ de quotients.

En fait $a \wedge b = b \wedge r_0$, et, les opérations étant décalées d'un cran, pour le couple (b, r_0) on a l'entier n et les quotients $q'_0 = q_1$, $q'_1 = q_2$, $\ldots$, $q'_n = q_{n+1}$, donc, en appliquant l'hypothèse de récurrence au couple (b, r_0), on a :

$a \wedge b = r_{n+1} = b \wedge r_0$

$$= b \begin{vmatrix} -q_2 & 1 & & \\ -1 & -q_3 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix} + r_0 \begin{vmatrix} -q_1 & 1 & & \\ -1 & -q_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix},$$

soit, avec $r_0 = a - q_0 b$,

$$r_{n+1} = a \begin{vmatrix} -q_1 & 1 & & 0 \\ -1 & -q_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix} + b \begin{vmatrix} -q_2 & 1 & & 0 \\ -1 & -q_3 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix}$$

$$- q_0 b \begin{vmatrix} -q_1 & 1 & & 0 \\ -1 & -q_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix}$$

$$= a \begin{vmatrix} -q_1 & 1 & & 0 \\ -1 & -q_2 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix} + b \begin{vmatrix} -q_0 & 1 & & 0 \\ -1 & -q_1 & \ddots & \\ & \ddots & \ddots & 1 \\ 0 & & -1 & -q_{n+1} \end{vmatrix},$$

(si on développe par rapport à la première colonne) : c'est bien la forme voulue à l'ordre $n+1$.

2.29. Soit q un diviseur premier de p non premier, on a $2 \leqslant q \leqslant p-1$, donc q divise $(p-1)!$.

Mais alors, si p divise $1 + (p-1)!$, *a fortiori* q diviserait $1 + (p-1)!$, donc il diviserait 1, avec $q \geqslant 2$ c'est assez difficile.

2.30. On a $N = (p-1)!^2 \sum_{k=1}^{p-1} \frac{1}{k^2} = \sum_{k=1}^{p-1} \left(\frac{(p-1)!}{k} \right)^2$: c'est un entier, comme somme de carrés d'entiers.

On considère le corps $\mathbb{Z}/p\mathbb{Z}$, (p entier premier), et, en notant $\bar{r}$ la classe d'équivalence de l'entier r, montrer que p divise N revient à montrer la nullité de $\overline{N}$.

Pour $1 \leqslant k \leqslant p-1$, on a $\bar{k} \neq 0$ dans $\mathbb{Z}/p\mathbb{Z}$, donc il existe un inverse de $\bar{k}$ dans ce corps, et $(\bar{k})^{-1}$ est représenté par un (et un seul) entier k' compris entre 1 et $p-1$: on a donc une bijection θ de $\{1, ..., p-1\}$ sur lui-même, tel que $k' = \theta(k)$ soit tel que $kk' \equiv 1$ modulo p : on a un

entier r_k tel que $kk' = k\theta(k) = 1 + r_k p$, d'où $\frac{1}{k} = k' - \frac{r_k p}{k}$ et $\frac{1}{k^2} = (\theta(k))^2 + \frac{p}{k^2}(r_k^2 p - 2r_k kk')$, ceci avec $k' = \theta(k)$.

On a une relation du genre $\frac{1}{k^2} = (\theta(k))^2 + \frac{p}{k^2}s_k$ avec s_k entier, d'où $\sum_{k=1}^{p-1} \frac{1}{k^2} = \sum_{k=1}^{p-1} (\theta(k))^2 + p \cdot \sum_{k=1}^{p-1} \frac{s_k}{k^2}$.

Les $\theta(k)$ redonnant $\{1, 2, ..., p-1\}$, la somme des carrés vaut $\frac{(p-1)p(2p-1)}{6}$, et, en multipliant par $(p-1)!^2$, on obtient

$$N = ((p-1)!)^2 \sum_{k=1}^{p-1} \frac{1}{k^2}$$

$$= p \cdot \frac{(p-1)(2p-1)}{6}((p-1)!)^2 + p \cdot \sum_{k=1}^{p-1} s_k \left(\frac{(p-1)!}{k}\right)^2 :$$

c'est un entier qui contient p en facteur, ($p \geqslant 5$, donc le 6 en dénominateur ne simplifie pas p, en fait 2 et 3 figurent en facteur dans $(p-1)!$).

On a bien N divisible par p.

2.31. On peut essayer de démontrer que :

soit $xy = yx$, pour tout couple (x, y),

soit $xy = -yx$, pour tout couple.

Pour cela, on fixe x_0 dans A, et on introduit les parties :

$A_+(x_0) = \{y \in A \; ; \; yx_0 = x_0 y\}$ et,

$A_-(x_0) = \{y \in A \; ; \; yx_0 = -x_0 y\}$.

Ce sont des parties non vides de A, (toutes deux contiennent 0), stables par addition, (distributivité), et passage à l'opposé car si $yx_0 = x_0 y$, on a $-(yx_0) = -(x_0 y)$, soit $(-y)(x_0) = x_0(-y)$; et de même l'égalité $yx_0 = -x_0 y$ donne $-(yx_0) = x_0 y$ soit $(-y)(x_0) = -(x_0)(-y)$.

Comme l'hypothèse permet de dire que tout y de A est dans l'un des deux sous-groupes additifs $A_+(x_0)$ ou $A_-(x_0)$, et qu'un groupe n'est jamais réunion de deux sous-groupes sans que l'un contienne l'autre, on a $A_+(x_0) \subset A_-(x_0) = A$, (ou $A_-(x_0) \subset A_+(x_0) = A$).

Dans le premier cas, $yx_0 = -x_0 y$, pour tout y de A, dans le deuxième cas $yx_0 = x_0 y$ pour tout y, et il ne reste plus qu'à voir si on peut, lorsque x_0 varie, avoir les deux types d'inclusion ou non.

Soit donc $E_- = \{x \in A\ ;\ A_+(x) \subset A_-(x)\}$ et,

$E_+ = \{x \in A\ ;\ A_-(x) \subset A_+(x)\}$, ce qui revient à dire que $E_- = \{x \in A\ ;\ A_-(x) = A\}$ et $E_+ = \{x \in A\ ;\ A_+(x) = A\}$.

Ces parties de E sont non vides, (toutes deux contiennent 0), stables par addition et passage à l'opposé. En effet, si x et x' sont dans E_+, alors pour tout y de A, y est dans $A_+(x)$ et $A_+(x')$ donc on a $yx = xy$ et $yx' = x'y$ d'où par addition : $yx + yx' = y(x + x') = xy + x'y = (x + x')y$, d'où $x + x'$ dans E_+.

Mais de même, pour x dans E_+, l'égalité $yx = xy$, valable pour y quelconque de A, donne $-(yx) = y(-x) = -(xy) = (-x)y$, d'où $-x$ dans E_+.

Les vérifications se font sans problème pour E_-, et on se retrouve là encore, avec deux sous-groupes du groupe additif A, de réunion A : l'un des deux contient l'autre.

Si $E_- \subset E_+$, c'est que $E_+ = A$, donc tout x de A est tel que $A_+(x) = A$, d'où pour tout y de A, $yx = xy$ et A est commutatif.

Si $E_+ \subset E_-$, on obtient un anneau anti-commutatif, où pour tout couple (x, y), $xy = -yx$.

2.32. a) On a $C_n^k C_{n-k}^{p-k} = \dfrac{n!}{k!(n-k)!}\dfrac{(n-k)!}{(p-k)!(n-p)!}$

$$= \frac{n!}{p!(n-p)!}\frac{p!}{k!(p-k)!},$$

donc la somme cherchée devient :

$$\sum_{k=0}^{p} (-1)^k C_n^k C_{n-k}^{p-k} = \sum_{k=0}^{p} C_n^p (-1)^k C_p^k = C_n^p (1-1)^p = 0, \text{ si } p \geqslant 1$$

car pour $p = 0$ il reste $(-1)^0 C_n^0 C_n^0 = 1$.

b) Le produit $C_n^k A_{n-k}$ est le nombre d'éléments du groupe symétrique ayant exactement k points fixes, car ces permutations sont obtenues en choisissant les k points fixes, ceci de C_n^k façons différentes, et pour chaque choix il reste à permuter les $n-k$ éléments restant, sans point fixe, ce qui se fait de A_{n-k} façons distinctes.

En faisant une partition de $\mathscr{S}_n$, (de cardinal $n!$), suivant le nombre de points fixes, on obtient $n! = \sum_{k=0}^{n} C_n^k A_{n-k}$.

c) La formule du b) donnant A_n en fonction des A_j, pour $j \leqslant n-1$, on peut procéder par récurrence.

On a $A_1 = 0$, (il n'y a que l'identité dans S_1), et

$1!\left(\frac{(-1)^0}{0!} + \frac{(-1)}{1!}\right) = 0$ est vérifiée.

Par contre on est amené, dans b, à poser $A_0 = 1$ pour considérer l'identité, ayant n points fixes, et avec cette convention, on a $A_0 = 0! \frac{(-1)^0}{0!} = 1$.

Si vous y tenez $A_2 = 1 = 2!\left(1 - 1 + \frac{1}{2}\right)$.

Supposons que $A_k = k! \sum_{j=0}^{k} \frac{(-1)^j}{j!}$ soit vérifiée pour $k \leqslant n-1$, alors :

$$A_n = n! - \sum_{k=1}^{n} C_n^k \left(\sum_{j=0}^{n-k} (n-k)! \frac{(-1)^j}{j!} \right)$$

$$= n! - \sum_{k=1}^{n} \sum_{j=0}^{n-k} (-1)^j \frac{n!}{k!(n-k)!} \frac{(n-k)!}{j!}$$

$$= n! - \sum_{k=1}^{n} \sum_{j=0}^{n-k} (-1)^j C_n^k C_{n-k}^j (n-k-j)!.$$

On pose $j = p - k$, p variant de k à n, d'où :

$$A_n = n! - \sum_{k=1}^{n} \sum_{p=k}^{n} (-1)^{p-k} C_n^k C_{n-k}^{p-k} (n-p)!,$$

et que faire de sérieux si ce n'est intervertir les sommations, d'où :

$$A_n = n! - \sum_{p=1}^{n} (n-p)! \left(\sum_{k=1}^{p} (-1)^{p-k} C_n^k C_{n-k}^{p-k} \right)$$

$$= n! - \sum_{p=1}^{n} (n-p)! \left((-1)^p \cdot \underbrace{\sum_{k=1}^{p} (-1)^k C_n^k C_{n-k}^{p-k}}_{= -(-1)^0 C_n^0 C_n^p \text{ d'après a)}} \right)$$

donc :

$$A_n = n! - \sum_{p=1}^{n} (n-p)! (-1)^{p+1} \frac{n!}{p!(n-p)!}$$

$$= n! \left(1 + \sum_{p=1}^{n} \frac{(-1)^p}{p!} \right) = n! \sum_{p=0}^{n} \frac{(-1)^p}{p!},$$

ce qui est bien le résultat cherché.

2.33. L'ensemble, non vide, E, des $a+b\sqrt{2}$, avec a et b dans $\mathbb{Q}$ est stable pour la soustraction de $\mathbb{R}$, c'est donc un sous-groupe additif.

On a stabilité pour le produit car, avec a, b, a', b' dans $\mathbb{Q}$:

$(a+b\sqrt{2})(a'+b'\sqrt{2}) = aa' + 2bb' + \sqrt{2}(ab'+ba')$ est dans E, donc E est sous-anneau de $\mathbb{R}$.

Supposons a et b de $\mathbb{Q}$ tels que $a+b\sqrt{2} = 0$. Si $b \neq 0$, on aurait $\sqrt{2} = -ab^{-1}$ dans $\mathbb{Q}$, et avec $\sqrt{2} = \frac{p}{q}$ irréductible, l'égalité $2q^2 = p^2$ conduit à 2 divise p, d'où $p = 2p'$ pair, et $2q^2 = 4p'^2$ à son tour donnera q pair, ce qui est incompatible avec l'hypothèse $\frac{p}{q}$ irréductible.

Donc $a+b\sqrt{2} = 0 \Rightarrow b = 0$ et $a = 0$, la réciproque est évidente.

Soit alors $a+b\sqrt{2} \neq 0$, (donc $(a,b) \neq (0,0)$). On a :

$(a+b\sqrt{2})(a-b\sqrt{2}) = a^2 - 2b^2$, non nul, car $a^2 - 2b^2 = 0$ avec $a \neq 0$ (ou $b \neq 0$) implique $b \neq 0$, (ou $a \neq 0$), d'où $2 = \frac{a^2}{b^2}$ et $\sqrt{2} = \left|\frac{a}{b}\right|$ dans $\mathbb{Q}$.

Donc $\frac{a-b\sqrt{2}}{a^2-2b^2}$ est, dans E, inverse de $a+b\sqrt{2}$, d'où E sous-corps de $\mathbb{R}$.

Soit f un automorphisme de E.

On a $f(x+y) = f(x)+f(y)$, pour tout (x,y) de E^2, d'où $f(2x) = 2f(x)$, et par une récurrence immédiate, pour n dans $\mathbb{N}$ et x dans E, l'égalité $f(n \cdot x) = nf(x)$.

Comme $f(0) = 0$, (prendre $y = 0$ dans $f(x+y)$), on a aussi :

$$f(nx+(-n)x) = 0 = f(nx)+f((-n)x) = nf(x)+f((-n)x),$$

donc $f((-n)x) = (-n)f(x)$ et l'égalité $f(p \cdot x) = pf(x)$ valable cette fois pour tout $(p,x) \in \mathbb{Z} \times E$.

Puis, (morphisme d'anneau), $f(1^2) = f(1) = (f(1))^2$ donc $f(1) = 0$ ou 1, mais f automorphisme, donc $f(1) = 0$ est exclu, il reste $f(1) = 1$ et $f(p) = p$ pour tout p de $\mathbb{Z}$, ($x = 1$ dans ce qui précède).

En écrivant $q \cdot \frac{1}{q} = 1$, on en déduit que pour q entier, $1 = q \cdot f\left(\frac{1}{q}\right)$, d'où $f\left(\frac{1}{q}\right) = \frac{1}{q}$ et $f\left(\frac{p}{q}\right) = \frac{p}{q}$, donc sur les rationnels f est l'identité.

On a $(f(\sqrt{2}))^2 = f((\sqrt{2})^2) = f(2) = 2$, donc $f(\sqrt{2}) = \varepsilon\sqrt{2}$ avec $\varepsilon = 1$ ou -1, et alors, avec $x = a + b\sqrt{2}$ dans E, a et b dans $\mathbb{Q}$, on a :

$$\begin{aligned} f(a+b\sqrt{2}) &= f(a) + f(b\cdot\sqrt{2}) \\ &= f(a) + f(b)\cdot f(\sqrt{2}) = a + b\varepsilon\sqrt{2}. \end{aligned}$$

On vérifie enfin que les deux applications f_+ et f_- définies par :

$$f_+(a+b\sqrt{2}) = a + b\sqrt{2} \text{ et,}$$

$$f_-(a+b\sqrt{2}) = a - b\sqrt{2},$$

sont bijectives ; et ce sont des morphismes de corps car :

$$\begin{aligned} f_\varepsilon((a+b\sqrt{2})(a'+b'\sqrt{2})) &= f(aa' + 2bb' + (ab' + ba')\sqrt{2}) \\ &= aa' + 2bb' + \varepsilon(ab' + ba')\sqrt{2}, \end{aligned}$$

alors que :

$$\begin{aligned} f_\varepsilon(a+b\sqrt{2})f_\varepsilon(a'+b'\sqrt{2}) &= (a+\varepsilon b\sqrt{2})(a'+\varepsilon b'\sqrt{2}) \\ &= aa' + 2\varepsilon^2 bb' + \varepsilon(ab' + ba')\sqrt{2} \end{aligned}$$

avec $\varepsilon^2 = 1$ d'où l'égalité. On a exactement deux automorphismes de corps.

2.34. a) Si $\frac{p}{q}$, irréductible, est zéro de $X^3 - 2$, on aura $p^3 = 2q^3$, d'où p pair, et avec $p = 2p'$, on a $4p'^3 = q^3$, d'où q pair, mais alors $\frac{p}{q}$ n'est pas irréductible. Donc $X^3 - 2$ n'a pas de racine rationnelle.

Or, si P est un diviseur, (non constant), de $X^3 - 2$ dans $\mathbb{Q}[X]$, il existe $Q \in \mathbb{Q}[X]$ tel que $PQ = X^3 - 2$, donc l'un des deux polynômes est de degré 1 et admet un zéro dans $\mathbb{Q}$: c'est exclu, d'où $X^3 - 2$ irréductible sur $\mathbb{Q}[X]$.

b) $A = \{a + b\alpha + c\alpha^2 \,;\, (a, b, c) \in \mathbb{Q}^3\}$ est non vide, stable par différence donc A est sous-groupe additif de $\mathbb{C}$. Comme $\alpha^3 = 2 \in \mathbb{Q} \subset A$, et $\alpha^4 = 2\alpha \in A$, A est stable par produit : c'est un sous-anneau (commutatif) de $\mathbb{C}$.

Puis 1, α et α^2 sont linéairement indépendants sur $\mathbb{Q}$, car l'existence d'un triplet $(a, b, c) \neq (0, 0, 0)$ tel que $a + b\alpha + c\alpha^2 = 0$ se traduit par

l'existence d'un polynôme $P(X) = a + bX + cX^2$ de $\mathbb{Q}[X]$ annulé par α, donc le reste R(X) de la division de $X^3 - 2$ par P(X) est un polynôme de degré 1, si P est de degré 2, annulé par α ; et si P est de degré 1, on a $P \in \mathbb{Q}[X]$, de degré 1, annulé par α.

Dans les deux cas α, zéro d'un polynôme de $\mathbb{Q}[X]$, de degré 1, est dans $\mathbb{Q}$, ce qui est faux.

Donc $u = a + b\alpha + c\alpha^2$, est un élément non nul de A si et seulement si $(a, b, c) \neq (0, 0, 0)$.

Soit $u = a + b\alpha + c\alpha^2$ non nul dans A, et, pour $z = x + y\alpha + z\alpha^2$ dans A isomorphe à l'espace vectoriel $\mathbb{Q}^3$ sur $\mathbb{Q}$, on pose :

$$f_u(z) = uz = (ax + 2bz + 2cy) + \alpha(bx + ay + 2cz) + \alpha^2(cx + by + az).$$

Vu la décomposition de uz dans la base $\{1, \alpha, \alpha^2\}$ de A sur $\mathbb{Q}$, on a f_u linéaire. Elle est injective, car $uz = 0$ avec $u \neq 0$ donne $z = 0$, tout étant dans $A \subset \mathbb{C}$, corps. Donc f_u est surjective, et il existe en particulier u' dans A tel que $f_u(u') = 1 = uu'$, d'où $u' = u^{-1}$, inverse de u dans $\mathbb{C}$, qui est dans A. On a $A - \{0\}$ sous-groupe multiplicatif de $\mathbb{C} - \{0\}$, donc A est un sous-corps de $\mathbb{C}$.

2.35. a) Comme G opère sur E et que l'on considère card (E), on pense à l'équation aux classes. Rappelons ce dont il s'agit.

Pour x dans E, $G_x = \{g\ ;\ g \in G, g \cdot x = x\}$ est un sous-groupe de G, (le groupe d'isotropie de x, ou le stabilisateur de x) car $1 \cdot x = x$ donc $1 \in G_x$, et si $g \in G_x$, on a $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$ mais c'est aussi $(g^{-1}g) \cdot x = 1 \cdot x = x$, donc $g^{-1} \in G_x$, et on vérifie facilement la stabilité par produit de G_x.

Puis on a $(g \cdot x = g' \cdot x) \Leftrightarrow (g'^{-1}g \cdot x = x) \Leftrightarrow g'^{-1}g \in G_x$ soit encore équivalent à $g \in g'G_x$: il y a exactement card G_x éléments de G qui donnent chaque image dans l'orbite de x, qui est l'ensemble $O_x = \{gx\ ;\ g \in G\}$.

On a donc $\dfrac{\text{card G}}{\text{card } G_x}$ éléments dans l'orbite de x.

Par ailleurs, les orbites forment une partition de E, car chaque x de E est égal à $1 \cdot x$ donc est dans son orbite, (comme les choses sont bien faites), et si $x' \in O_x$, comme il existe g dans G tel que $x' = g \cdot x$, soit

$x = g^{-1} \cdot x'$, tout élément $h \cdot x = h \cdot (g^{-1} \cdot x')$ de l'orbite O_x est dans $O_{x'}$, et réciproquement, donc $O_x \neq O_y$ implique $O_x \cap O_y = \emptyset$.

On a donc card (E) = $\sum_{\text{orbites}}$ card (orbite).

Ici, $x \in E^G \Leftrightarrow O_x = \{x\}$, orbite de cardinal 1.

Il y a donc card (E^G) orbites à un élément, et les autres orbites sont de cardinal $\frac{\text{card } G}{\text{card } G_x}$, entier du type p^r, avec $r \geqslant 1$.

On a donc card (E) = card (E^G) + somme d'entiers multiples de p, d'où card (E) $\equiv$ card (E^G) (mod p).

b) Soit $E = \{(x_1, ..., x_p) \in H^p, x_1 x_2 ... x_p = 1\}$, H groupe fini ayant n éléments.

Un p-uplet est dans E, si on se donne $x_1, x_2, ..., x_{p-1}$ quelconques, (d'où n^{p-1} choix), et que x_p est choisi de façon que $(x_1 ... x_{p-1})x_p = 1$, d'où $x_p = (x_{p-1})^{-1} ... (x_1)^{-1}$ obtenu de manière unique. On a n^{p-1} éléments dans E.

Ce sont des $p \cdot$ uplets, et on veut faire agir $G = \mathbb{Z}/p\mathbb{Z}$, additif, sur E. En notant $(\bar{0}, \bar{1}, ..., \overline{p-1})$ les éléments de G, on peut poser $\bar{k} \cdot (x_1, x_2, ..., x_p) = (x_{k+1}, ..., x_p, x_1, x_2, ..., x_k)$, à condition que le produit $x_{k+1} x_{k+2} ... x_p x_1 x_2 ... x_k$ soit égal à 1, ce qui s'obtient en remarquant que :

$$x_1 x_2 ... x_p = 1 \Rightarrow (x_1 ... x_p)x_1 = x_1,$$

$$\Rightarrow x_1^{-1}(x_1 x_2 ... x_p x_1) = x_1^{-1} x_1 = 1,$$

soit encore $x_2 x_3 ... x_p x_1 = 1$, et on itère ce calcul.

On vérifie que G opère ainsi sur E, et on applique le a), en cherchant $E^G = \{X \in E ; k \cdot X = X, k = \bar{0}, \bar{1}, ..., \overline{p-1}\}$, soit encore l'ensemble des X de E tels que :

$$(x_1, x_2, ..., x_p) = (x_2, x_3, ..., x_p, x_1) = (x_3, x_4, ..., x_p, x_1, x_2) = ...$$

$$= (x_p, x_1, x_2, ..., x_{p-1}),$$

ce qui équivaut à $x_i = x$, pour $i = 1, ..., p$, avec $x^p = 1$, (et voici les éléments d'ordre p : tout vient à point à qui sait attendre !).

D'après le a) le cardinal de l'ensemble des x de H, avec $x^p = 1$, (p est premier) est de cardinal congru au cardinal de E, modulo p.

Or card $E = n^{p-1}$, avec p qui divise n et $p - 1 \geqslant 1$, (p premier), d'où le cardinal de l'ensemble des x de H tels que $x^p = 1$ est congru à 0 modulo p. Cet ensemble, qui contient 1, n'est pas réduit à 1, donc il existe $x \in H - \{1\}$, tel que $x^p = 1$, x est bien d'ordre p, car p est premier.

c) Soit H un groupe abélien d'ordre n, et m un entier tel que pour tout x de H, $x^m = 1$. On sait, d'après le b) que si p, premier, divise n, il existe x d'ordre p, et comme $x^m = 1$, m est multiple de p.

Comme m est multiple de chaque nombre premier p divisant n, si α = sup des exposants des nombres premiers divisant n, m^α sera multiple de n.

2.36. a) On fait agir G sur lui-même par automorphismes intérieurs.

Comme dans 2.35, en notant, pour x dans G, G_x le sous-groupe stabilisateur de x, $G_x = \{g \in G, g^{-1}xg = x\}$, l'orbite O_x de x est de cardinal $\dfrac{\text{card } G}{\text{card } G_x}$, et l'équation aux classes devient ici :

$$\text{card } G = \sum_{x \in K} \frac{\text{card } G}{\text{card } G_x},$$

en notant K un ensemble de représentants des orbites, (donc en bijection avec les orbites).

Si on suppose que, pour tout x, $\bar{x} \cap H \neq \emptyset$, $\bar{x}$ orbite de x, on peut choisir les représentants dans H, donc on a une partie K de H telle que, après simplification par card G, on ait

$$1 = \sum_{x \in K} \frac{1}{\text{card } G_x}.$$

On fait maintenant agir H sur lui-même par automorphismes intérieurs, de H, et on note, pour x dans H,

$\bar{\bar{x}} = \{h^{-1}xh, h \in H\}$, l'orbite de x dans cette action.

Il est clair que $\bar{\bar{x}} \subset \bar{x} = \{g^{-1}xg, g \in G\}$.

Soient x et x' distincts dans K, s'ils étaient dans la même orbite par action de H, on aurait $h \in H$ tel que $x' = h^{-1}xh$, or $h \in G \Rightarrow \bar{x}' = \bar{x}$ ce qui est exclu.

Comme les x de K correspondent à des orbites $\bar{\bar{x}}$ disjointes, un système de représentants des orbites dans H, peut être choisi du type $K \cup L$, avec $L \subset H$ et $K \cap L = \emptyset$.

L'équation aux classes conduit alors à l'égalité :

$$1 = \sum_{x \in K \cup L} \frac{1}{\operatorname{card} H_x},$$

avec $H_x = \{h \in H ; h^{-1}xh = x\}$ d'où $H_x \subset G_x$ car $H \subset G$, et

$$\operatorname{card} H_x \leqslant \operatorname{card} G_x \Rightarrow \frac{1}{\operatorname{card} H_x} \geqslant \frac{1}{\operatorname{card} G_x}.$$

Mais alors, on a :

$$1 = \sum_{x \in K} \frac{1}{\operatorname{card} H_x} + \sum_{x \in L} \frac{1}{\operatorname{card} H_x} \geqslant \underbrace{\sum_{x \in K} \frac{1}{\operatorname{card} G_x}}_{=1} + \sum_{x \in L} \frac{1}{\operatorname{card} H_x}$$

$$\geqslant 1 + \sum_{x \in L} \frac{1}{\operatorname{card} H_x}.$$

On a donc $L = \emptyset$ et, $\forall x \in K$, $\operatorname{card} H_x = \operatorname{card} G_x$, d'où, (parties finies et $H_x \subset G_x$), l'égalité $H_x = G_x$.

Mais parmi les orbites, il y a celle de e, neutre, et comme $e \in H$, on peut imposer d'avoir choisi e comme représentant de cette orbite, dans le choix des éléments de K, d'où $H_e = G_e$, mais $H_e = \{h \in H ; h^{-1}eh = e\}$: c'est H, et de même $G_e = G$, on arrive finalement à $G = H$, ce qui est exclu.

Donc il existe x dans G tel que $\bar{x} \cap H = \emptyset$.

b) L'expression $g^{-1}xg$ fait penser à des matrices semblables par exemple.

Prenons $G = GL_n(\mathbb{C})$, toute matrice est semblable à une matrice triangulaire supérieure, régulière ici, or H = {matrices triangulaires supérieures, régulières} est bien sous-groupe multiplicatif de G, avec $H \subsetneq G$, et cependant, $\forall X \in GL_n(\mathbb{C})$, $\exists P \in GL_n(\mathbb{C})$ avec $P^{-1}XP \in H$, soit $\overline{X} \cap H \neq \emptyset$.

2.37. On a d'abord $2^{(2^{6n+2})} = 2^{\left(4 \cdot (2^6)^n\right)} = 2^{4 \cdot (64)^n}$ ou encore $2^{(2^{6n+2})} = (16)^{64^n}$. Notons a ce nombre, comme $16 \equiv (-3)(19)$, on obtient $a \equiv (-3)^{64^n}(19)$.

Comme 64^n est pair, si $n > 0$, $(-3)^{64^n} = (3)^{64^n}$, et, 19 étant premier, par le petit Théorème de Fermat, on obtient $3^{18} \equiv 1(19)$. Comme

$64 = 3 \times 18 + 10$, on aura $3^{64} \equiv 3^{10}(19)$. On peut alors chercher à quoi est congru 3^{10}. On a successivement $3^2 \equiv 9(19)$, $3^3 \equiv 8(19)$, d'où, par produit $3^5 \equiv 72(19)$ donc $\equiv 15(19)$ ou encore $3^5 \equiv -4(19)$, d'où au carré, $3^{10} \equiv 16(19)$, donc $3^{10} \equiv -3(19)$.

Pour $n \geqslant 1$, $3^{(64^n)} = (3^{64})^{64^{n-1}}$, avec $3^{64} \equiv (-3)(19)$ d'après ce qui précède, donc :

$$(-3)^{64^n} \equiv (-3)^{64^{n-1}}(19), \text{ si } n \geqslant 1.$$

Par itération, on obtient finalement :

$a \equiv (-3)^{64^0}(19) \equiv (-3)(19)$, d'où $a + 3 \equiv 0(19)$, ce que l'on voulait, le cas $n = 0$ étant également traité.

2.38. Si r n'est pas premier, en écrivant $r = pq$ avec p et q tous deux strictement supérieurs à 1, on obtient une identité :

$$\begin{aligned} a^r - 1 &= (a^p)^q - 1^q \\ &= (a^p - 1)\left(\sum_{k=0}^{q-1} a^{pk}\right). \end{aligned}$$

Or $p > 1$ et $a \geqslant 2 \Rightarrow a^p - 1 > 1$. Puis $q \geqslant 2$ donc $\sum_{k=0}^{q-1} a^{pk} \geqslant 1 + a^p > 1$:

il en résulte que $a^r - 1$ n'est pas premier.

Puis, avec r premier, comme $a^r - 1 = (a-1)(1 + a + \ldots + a^{r-1})$, si $a > 2$, comme $r - 1 \geqslant 1$, on décomposerait là encore $a^r - 1$ en un produit de deux entiers $\geqslant 2$, c'est exclu. Donc $a = 2$.

2.39. L'utilisation d'une calculette ou d'un ordinateur montre que, pour $k = 2$ et n variant de 1 à 100, on obtient pour images les entiers sauf les carrés. Pour $k = 3$, on n'obtient pas les cubes.

Ceci conduit à justifier que $f(\mathbb{N}) = \mathbb{N} - \{m^k, m \in \mathbb{N}^*\}$, ce qui se fera en utilisant les encadrements liés à la partie entière.

On fixe donc k. D'abord $f(0) = 0 + E(0) = 0$.

Puis si n augmente, $(n + n^{1/k})^{1/k}$ augmente, la partie entière aussi, donc $f(n)$ augmente strictement, (car n lui croît strictement).

On veut justifier que :

$$f(\mathbb{N}) = \{0, \ , 2, 3, ..., 2^k - 1, \ , 2^k + 1, ..., 3^k - 1, \ , 3^k + 1, ..., ...\},$$

et, si ce résultat est correct, l'entier $m^k - 1$ apparaît comme la $(m^k - 1 - (m-1))^{\text{ième}}$ image non nulle, obtenue en croissant, les entiers $1^k, 2^k, ..., (m-1)^k$ n'étant pas dans l'image, et 0 étant à part car $f(0) = 0$.

On suppose donc $m \geqslant 1$.

On doit donc justifier que $f(m^k - m) = m^k - 1$, et pour y parvenir on va encadrer la partie entière en remarquant que :

$$\mathrm{E}(x) \leqslant x < 1 + \mathrm{E}(x) \Leftrightarrow x - 1 < \mathrm{E}(x) \leqslant x.$$

On a donc :

$$f(m^k - m) = m^k - m + \mathrm{E}((m^k - m + (m^k - m)^{1/k})^{1/k})$$

$$\leqslant m^k - m + (m^k - m + (m^k - m)^{1/k})^{1/k},$$

or $(m^k - m)^{1/k} < (m^k - 0)^{1/k} = m$, et il vient :

$$f(m^k - m) < m^k - m + (m^k - m + m)^{1/k} = m^k,$$

d'où, puisque f est à valeurs entières, $f(m^k - m) \leqslant m^k - 1$.

Nous allons prouver que $f(m^k - m) > m^k - 2$, en prouvant qu'un minorant de $f(m^k - m)$ est déjà supérieur strictement à $m^k - 2$, et on utilise $\mathrm{E}(x) > x - 1$ pour cela. On a :

$$f(m^k - m) > m^k - m + (m^k - m + (m^k - m)^{1/k})^{1/k} - 1,$$

et on va justifier que :

$$m^k - m + (m^k - m + (m^k - m)^{1/k})^{1/k} - 1 \geqslant m^k - 2,$$

soit encore que :

$$(m^k - m + (m^k - m)^{1/k})^{1/k} \geqslant m - 1.$$

Comme $m \geqslant 1$, on a une inégalité entre nombres positifs, elle est équivalente à celle obtenue en élevant à la puissance $k^{\text{ième}}$, donc on va prouver que la fonction g définie par :

$$g(m) = m^k - m + (m^k - m)^{1/k} - (m-1)^k,$$

est à valeurs positives si $m \geqslant 1$.

On la considère comme fonction d'une variable réelle, on dérive, on obtient :

$$g'(m) = km^{k-1} - 1 + \frac{1}{k}(m^k - m)^{(1/k)-1}(km^{k-1} - 1) - k(m-1)^{k-1}$$

$$= [k(m^{k-1} - (m-1)^{k-1}) - 1] + (m^k - m)^{(1/k)-1}\left(m^{k-1} - \frac{1}{k}\right).$$

Comme $k \geqslant 2$ et $m \geqslant 1$, on a déjà $(m^k - m)^{(1/k)-1}\left(m^{k-1} - \frac{1}{k}\right) \geqslant 0$;

puis en posant $u(m) = k(m^{k-1} - (m-1)^{k-1}) - 1$, on a :

$$u'(m) = k(k-1)(m^{k-2} - (m-1)^{k-2}) \geqslant 0,$$

(toujours $k \geqslant 2$), donc u croît et $u(1) = k - 1 \geqslant 1$.

Finalement, $g'(m) \geqslant 1$ sur $[1, +\infty[$, la fonction g croît strictement et $g(1) = 0$: on a bien g à valeurs positives et, tout compte fait, l'entier $f(m^k - m)$ est $\geqslant m^k - 1$.

L'autre inégalité ayant été justifiée, on vient de prouver que, pour tout $m \geqslant 1$, $f(m^k - m) = m^k - 1$.

Mais alors, la stricte monotonie de f permet de dire que l'on a l'inclusion :

$$f([m^k - m, (m+1)^k - (m+1)[) \subset [m^k - 1, (m+1)^k - 1[.$$

Or $[m^k - m, (m+1)^k - (m+1)[$ contient exactement :

$(m+1)^k - (m+1) - (m^k - m) = (m+1)^k - m^k - 1$ entiers, alors que l'intervalle $[m^k - 1, (m+1)^k - 1[$, lui, est de cardinal $(m+1)^k - m^k$: il y a un entier en plus.

On va prouver que m^k n'est pas dans l'image de $\mathbb{N}$: comme on a $m^k - 1 \leqslant m^k$, et $m^k < (m+1)^k - 1$, ce sera l'élément de $[m^k - 1, (m+1)^k - 1[$ non image d'un entier.

Comme $f(m^k - m) = m^k - 1$, si m^k avait un antécédent, il serait supérieur à $m^k - m + 1$. Prouvons donc que $f(m^k - m + 1) > m^k$ pour conclure cet exercice déjà long. Or, $(E(x) > x - 1)$, on a :

$$f(m^k - m + 1) > m^k - m + 1 + (m^k - m + 1 + (m^k - m + 1)^{1/k})^{1/k} - 1$$

et on va justifier que :

$$m^k - m + (m^k - m + 1 + (m^k - m + 1)^{1/k})^{1/k} \geqslant m^k,$$

ce qui équivaut à :

$$(m^k - m + 1 + (m^k - m + 1)^{1/k})^{1/k} \geqslant m,$$

donc, comme il s'agit de nombres positifs, c'est encore l'inégalité

$$m^k - m + 1 + (m^k - m + 1)^{1/k} \geqslant m^k,$$

qu'il s'agit de justifier, ou bien :

$$(m^k - m + 1)^{1/k} \geqslant m - 1,$$

soit, $(m - 1 \geqslant 0)$,

$$m^k - m + 1 \geqslant (m-1)^k.$$

Si on pose $h(m) = m^k - m - (m-1)^k + 1$, on a :

$$h'(m) = km^{k-1} - k(m-1)^{k-1} - 1,$$

$$h''(m) = k(k-1)(m^{k-2} - (m-1)^{k-2}) \geqslant 0,$$

pour $m \geqslant 1$ et $k \geqslant 2$.

La fonction h' croît, $h'(1) = k - 1 \geqslant 1$, donc h croît strictement, et $h(1) = 1$, je pense qu'on a gagné, et justifié que

$$f(\mathbb{N}) = \mathbb{N} - \{m^k ; m \in \mathbb{N}^*\}.$$

2.40. Comme $\mathbb{R}$ est en particulier un anneau pour la somme et le produit des réels, l'ensemble des applications de $[-1, 1]$ dans $\mathbb{R}$, pour les lois + et · définies par :

$$(f+g)(x) = f(x) + g(x) \text{ et } (f \cdot g)(x) = f(x)g(x),$$

est un anneau. On vérifie que $\mathscr{A}$ en est un sous-anneau, car $\mathscr{A}$ est non vide, la fonction polynôme nulle est dans $\mathscr{A}$,

puis si $f : x \rightsquigarrow P(x) + \sqrt{1-x^2}Q(x)$, et $g : x \rightsquigarrow R(x) + \sqrt{1-x^2}S(x)$ sont dans $\mathscr{A}$, on a :

$f - g : x \rightsquigarrow P(x) - R(x) + \sqrt{1-x^2}(Q(x) - S(x))$, et :

$$f \cdot g : x \rightsquigarrow (P(x)R(x)) + (1-x^2)Q(x)S(x) + \sqrt{1-x^2}(P(x)S(x) + Q(x)R(x)),$$

qui sont du type voulu pour être dans $\mathscr{A}$.

Recherche des éléments inversibles

Avoir $f = P + \sqrt{1-x^2}Q$ inversible, c'est trouver deux polynômes R et S tels que, pour tout x de $[-1, 1]$, on ait la relation (1) :

$$(P(x)R(x) + (1-x^2)Q(x)S(x) - 1) + \sqrt{1-x^2}(P(x)S(x) + Q(x)R(x)) = 0.$$

Or, une relation du genre $U(x) + \sqrt{1-x^2}V(x) = 0$, avec U et V polynômes, conduit à $U = V = 0$. En effet, si l'un des deux polynômes est nul, l'autre l'est immédiatement.

On les suppose non nuls tous les deux. Si D est leur p.g.c.d., en écrivant $U = DU_1$ et $V = DV_1$, après simplification par D, on obtient l'égalité $U_1(x) + \sqrt{1-x^2}V_1(x) = 0$.

Pour $x = 1$ et -1 on a donc $U_1(1) = U_1(-1) = 0$, donc $1-x^2$ se factorise dans U_1, et en écrivant $U_1(x) = (1-x^2)U_2(x)$, après simplification, dans $(1-x^2)U_2(x) + \sqrt{1-x^2}V_1(x) = 0$, par $\sqrt{1-x^2}$, on obtient l'égalité :

$$\sqrt{1-x^2}U_2(x) + V_1(x) = 0,$$

qui conduit à 1 et -1 zéros de V_1, d'où V_1 également divisible par $(1-x^2)$: contredit V_1 et U_1 premiers entre eux.

Donc l'égalité (1) équivaut au système (I) :

$$\text{(I)} \begin{cases} P(x)R(x) + (1-x^2)Q(x)S(x) - 1 = 0 \\ P(x)S(x) + Q(x)R(x) = 0. \end{cases}$$

Supposons que l'on ait des solutions autres que celles auxquelles on s'attend, (à savoir $k \cdot \frac{1}{k}$, avec $k \in \mathbb{R}^*$), donc avec Q et S polynômes non nuls.

Alors ces polynômes ont des degrés, q et s, et des coefficients directeurs non nuls, c_q et c_s, donc, l'expression :

$(1-x^2)Q(x)S(x) - 1$

est un polynôme de degré $2+q+s$, de coefficient directeur $-c_qc_s$, et la première égalité ne peut être vérifiée que si PR est de même degré et de coefficient directeur opposé.

En notant p et r les degrés de P et R, et c_q, c_r leurs coefficients directeurs, ceci conduit à l'égalité :

$c_pc_r - c_qc_s = 0$, qui, comme $c_qc_s \neq 0$, exige $c_pc_r \neq 0$.

De même, le coefficient de plus haut degré de PS + QR devant être nul, PS et QR doivent être de mêmes degrés, et on doit avoir l'égalité $c_pc_s + c_qc_r = 0$.

En considérant les deux relations :

$$\begin{cases} c_pc_r - c_qc_s = 0 \\ c_pc_s + c_qc_r = 0, \end{cases}$$

comme un système linéaire homogène en c_p et c_q comme inconnues, son déterminant vaut $(c_r)^2 + (c_s)^2 \neq 0$ puisque $c_qc_s \neq 0$ a impliqué $c_pc_r \neq 0$, mais alors on devrait avoir $c_p = c_q = 0$: absurde.

Donc Q ou S est nul.

Supposons $Q = 0$, (symétrie des rôles), dans le système (I) il reste les égalités :

$$\begin{cases} P(x)R(x) = 1 \\ P(x)S(x) = 0. \end{cases}$$

Comme P est non nul, S est le polynôme nul, puis $P(x)$ est une constante k, non nulle, et $R(x) = \frac{1}{k}$: les éléments inversibles de $\mathscr{A}$ sont du type k, $k \in \mathbb{R}^*$.

L'élément x est irréductible dans l'anneau $\mathscr{A}$

En effet, supposons que x soit un produit de deux éléments $P + \sqrt{1-x^2}Q$ et $R + \sqrt{1-x^2}S$ de $\mathscr{A}$. L'égalité :

$$PR + (1-x^2)QS + \sqrt{1-x^2}(QR + PS) = x$$

conduit, comme dans la recherche des éléments inversibles, au système (II) :

$$(II) \begin{cases} PR - x + (1-x^2)QS = 0, \\ QR + PS = 0, \end{cases}$$

et, là encore, si Q et S sont non nuls, de degrés q et s, $(1-x^2)QS - x$ est de degré $2 + q + s$, de coefficient directeur $-c_q c_s$, avec les notations précédentes.

Le même raisonnement s'applique, P et Q ne peuvent être nuls, et en notant c_p et c_q leurs coefficients directeurs, non nuls, on est conduit au système :

$$\begin{cases} c_p c_r - c_q c_s = 0, \\ c_q c_r + c_p c_s = 0, \end{cases}$$

qui, avec c_p et c_q non nuls, conduit à $c_r = c_s = 0$, (système homogène de Cramer), ce qui est absurde.

On a donc, par exemple, $Q = 0$, le système (II) se réduit à :

$PR = x$ et $PS = 0$, d'où $P \neq 0 \Rightarrow S = 0$, et $PR = x$, on peut choisir, par exemple $P(x) = kx$, $(k \in \mathbb{R}^*)$, et $R = \frac{1}{k}$.

Mais écrire $x = \frac{1}{k} \cdot kx$, c'est décomposer x avec un élément inversible de l'anneau $\mathscr{A}$ comme facteur, ce qui, dans les anneaux, n'est pas du jeu. Cela compte pour du beurre, et x est irréductible.

2.41. Soit $\mathscr{U} = \{\text{suites d'entiers naturels}\}$. Cet ensemble est de cardinal infini car, pour tout n de $\mathbb{N}$ on peut définir la suite $a^{(n)}$, qui à n associe 1 et à $p \neq n$ associe 0 : on a une injection de $\mathbb{N}$ dans $\mathscr{U}$, d'où $\mathscr{U}$ de cardinal supérieur ou égal à celui de $\mathbb{N}$.

Si $\mathscr{U}$ est équipotent à $\mathbb{N}$, on indexe les éléments de $\mathscr{U}$ par $\mathbb{N}$, donc on les note $u^{(n)}$, $n \in \mathbb{N}$, et, par le procédé *de la suite diagonale* on construit une suite v en posant, pour tout p de $\mathbb{N}$, $v_p = u_p^{(p)} + 1$ par exemple.

Comme $v \in \mathscr{U}$, il existe un n tel que $v = u^{(n)}$, mais alors le $n^{\text{ième}}$ terme de v est $u_n^{(n)}$ d'une part, et c'est $v_n = u_n^{(n)} + 1$: c'est impossible. Donc $\mathscr{U}$ n'est pas dénombrable.

2.42. On note le groupe multiplicativement.

a) Pour x et y dans G, on a $(xy)(xy) = e$. On multiplie à gauche par x, à droite par y, et compte tenu de l'associativité on a :

$$x^2(yx)y^2 = xy,$$

soit comme $x^2 = y^2 = e$, élément neutre, $yx = xy$: le groupe est commutatif.

b) Soit x dans $H \cap aH$, il existe y dans H tel que $x = ay$. Alors $xy = a(y^2) = ae = a$, avec x et y dans H sous-groupe : on aurait a dans H ce qui est exclu. Donc $H \cap aH = \emptyset$.

Soit alors $K = H \cup aH$, c'est une partie non vide de G, (car $e \in H$).

Puis, si x et y sont dans K, comme dans G, $y^{-1} = y$ puisque $y^2 = e$, si on prouve que xy est dans K, ce sera aussi xy^{-1} dans K et on aura justifié que K est sous-groupe.

Si x et y sont tous les deux dans H, sous-groupe, on a xy dans H donc dans K.

Si x et y sont tous les deux dans aH, en écrivant $x = ah$ et $y = ak$, avec h et k dans H, on obtient, G étant commutatif, $xy = a^2hk = hk$ dans H, (sous-groupe), donc dans K.

Enfin, si x est dans H et y dans K, avec $y = ah$, (h dans H), on a $xy = x(ah) = a(xh)$, (associativité et commutativité), avec xh dans H, stable par produit, donc xy dans aH, et *a fortiori* dans K.

On a finalement la stabilité de K par produit, ce qui achève la justification de K sous-groupe.

CHAPITRE III

Polynômes

Il s'agit d'une structure très riche où se mêlent algèbre et analyse lorsque le corps de base s'y prête.

Du point de vue algébrique, on a déjà une structure d'espace vectoriel dénombrable strict, et pour les questions se ramenant à des bases, le choix d'une base adaptée est primordial. En plus de la base canonique, penser à toute famille de polynômes en nombre voulu, et de degrés échelonnés, (ou de valuations échelonnées), (voir 3.1).

A ce propos, partant d'un polynôme P de degré n, ne pas oublier que les $n+1$ polynômes dérivés $P^{(k)}(X)$, $0 \leqslant k \leqslant n$, qui se définissent algébriquement, sont de degrés échelonnés, et que l'on a droit, sur un corps K quelconque, à la formule de Taylor à l'ordre n = degré du polynôme, formule exacte en fait. Donc $P(X+a)$ peut faire penser à Taylor, (devrais-je dire doit faire penser...).

Mais K[X] est aussi un anneau factoriel et des raisonnements faisant intervenir les décompositions en produits de puissances de polynômes irréductibles sont à faire quand la divisibilité est en cause. Ne pas oublier en particulier **Bézout** ! Voir 3.21.

En liaison avec ces facteurs irréductibles interviennent les zéros d'un polynôme, dont l'existence dépend du corps K, (et du polynôme), mais dont le nombre ne dépasse pas le degré.

On dispose alors des relations entre zéros et coefficients d'un polynôme.

On trouve, comme base « adaptée » à cette notion de zéros, de valeurs prises en des points distincts, les polynômes **interpolateurs de Lagrange**, $\prod_{\substack{j=1 \\ j \neq k}}^{n+1} \frac{(X-a_j)}{a_k-a_j}$, pour des a_r tous distincts, polynômes en nombre $n+1$, tous de degré n, et qui forment une base de $K_n[X]$. Voir 3.22 par exemple, ou 3.17.

L'analyse intervient, lorsque $K = \mathbb{R}$, par l'étude des fonctions polynômes, de leurs variations et de leurs zéros. Ne pas oublier qu'un polynôme de $\mathbb{R}[X]$ de degré impair s'annule toujours, (il varie entre $+\infty$ et $-\infty$).

Un cas particulier est celui des familles $(P_n)_{n \in \mathbb{N}}$ de polynômes, où les P'_n sont reliés aux P_{n-1} par des relations simples, et où par récurrence on peut étudier les variations et les zéros de ces polynômes, en ayant une *démarche dynamique*, c'est-à-dire en revenant aux données pour voir en quoi les résultats trouvés peuvent les modifier, et donner ainsi d'autres conséquences. Voir 3.3.

Il faut aussi savoir penser « fractions rationnelles » et dérivées logarithmiques, lorsque P et P' sont en cause par exemple, (voir 3.24).

Ne pas oublier les fonctions symétriques des racines même si les calculs où elles interviennent peuvent être laborieux, (voir 3.30).

Lorsque le corps de base est $\mathbb{R}$, la structure polynomiale s'enrichit des apports de l'analyse. Ainsi, les fonctions polynômes étant de classe C^∞, on pourra recourir aux équations différentielles pour traiter les questions, (3.7 par exemple).

Énoncés

3.1. Pour tout P de $\mathbb{C}[X]$, on pose $L(P)(z) = e^{-z} \sum_{n=0}^{+\infty} \frac{P(n)}{n!} z^n$.

Montrer que L est un isomorphisme de $\mathbb{C}[X]$ sur lui-même.

3.2. Soit les applications f et g de $\mathbb{C}$ dans $\mathbb{C}$ définies par $f(z) = z^2 + z + 1$ et $g(z) = z^2 - z + 1$ respectivement, et A une partie finie, non vide, de $\mathbb{C}$ telle que $f(A) \subset A$ et $g(A) \subset A$.

Montrer que $A = \{i, -i\}$.

Trouver les polynômes P de $\mathbb{C}[X]$ tels que :

$P(X^2 + X + 1) = P(X)P(X + 1)$.

3.3. Soit $P_n(X) = \sum_{k=0}^{n} \frac{X^k}{k!}$. Montrer que P_n admet au plus une racine réelle. Préciser selon la parité de n. Soit a_{2k+1} l'unique racine réelle de P_{2k+1}. Déterminer $\lim_{k \to +\infty} a_{2k+1}$.

3.4. Soit P dans $\mathbb{Q}[X]$, de degré trois, ayant α dans $\mathbb{C}$ pour racine multiple. Montrer que α est dans $\mathbb{Q}$. Généralisation ?

3.5. Trouver les polynômes P de $\mathbb{C}[X]$ tels qu'il existe p et q dans $\mathbb{N}^*$ tels que $(P')^p$ divise P^q.

3.6. Soit P dans $\mathbb{C}_n[X]$, de racines, distinctes ou non, $u_1, u_2, \ldots, u_n$, (les racines multiples sont donc répétées).

On note, pour p dans $\mathbb{N}$, $S_p = (u_1)^p + \ldots + (u_n)^p$.

Soit l dans $\mathbb{N}^*$ et Q le quotient de la division euclidienne de $X^{l+1}P'$ par P. Montrer que :

$$Q = \sum_{p=0}^{d^\circ Q} S_p X^{l-p}, \text{ et préciser le degré de Q.}$$

3.7. Soit $P \in \mathbb{R}[X]$ tel que, $\forall x \in \mathbb{R}$, $P(x) \geqslant 0$. Si n est le degré de P on pose $Q = P + P' + P'' + \ldots + P^{(n)}$.

Montrer que, $\forall x \in \mathbb{R}$, $Q(x) \geqslant 0$.

3.8. Soit $a_1, ..., a_n$ des entiers relatifs distincts. On pose :

$$P(X) = -1 + \prod_{i=1}^{n} (X - a_i).$$

Montrer que si l'on a $P(X) = Q(X)R(X)$ avec Q et R dans $\mathbb{Z}[X]$, on a : Q ou R de degré n.

3.9. Soit (P, Q) un couple de polynômes de $\mathbb{R}[X]$, simplement scindés sur $\mathbb{R}$ et tels qu'entre deux racines de l'un, il y ait toujours au moins une racine de l'autre. Montrer que pour tout (λ, μ) de $\mathbb{R}^2$, le polynôme $\lambda P + \mu Q$ est scindé.

3.10. Soit une matrice carrée complexe d'ordre n sur $\mathbb{C}$. Montrer l'équivalence de : M est nilpotente, et de : trace de $M^k = 0$ pour $k = 1, 2, ..., n$.

3.11. Montrer qu'il existe a dans $\mathbb{R}\backslash\{-2\}$, tel qu'il existe $(\alpha, \beta, \gamma, \delta)$ dans $\mathbb{R}^4$, tel que pour tout polynôme P de $\mathbb{R}_4[X]$ on ait :

$$\alpha P(-2) + \beta P'(-2) + \gamma P(-1) + \delta P\left(\frac{1}{2}\right) = P'(a).$$

3.12. Soit P dans $\mathbb{Z}[X]$, de coefficient directeur 1 et a un zéro de P dans $\mathbb{Q}$. Montrer que a est dans $\mathbb{Z}$.

3.13. Soit $A = \sum_{j=0}^{2n} a_j X^j$ dans $\mathbb{R}_{2n}[X]$. On considère l'application $\delta(A)$ de $\mathbb{R}_{2n}[X]$ dans lui-même définie par : $P \rightsquigarrow \sum_{j=0}^{2n} \frac{a_j}{j!} P^{(j)}$. Montrer que les propriétés suivantes sont équivalentes :

(i) $\forall P \in \mathbb{R}_{2n}[X], P(\mathbb{R}) \subset \mathbb{R}_+ \Rightarrow \delta(A)(P)(\mathbb{R}) \subset \mathbb{R}_+$;

(ii) $\forall P \in \mathbb{R}_{2n}[X], P(\mathbb{R}) \subset \mathbb{R}_+ \Rightarrow \delta(A)(P)(0) \in \mathbb{R}_+$;

(iii) la matrice de terme général $\alpha_{ij} = a_{i+j}$, avec $0 \leqslant i, j \leqslant n$, est associée à une forme quadratique positive.

3.14. On pose $(\Delta P)(X) = P(X+1) - P(X)$ pour tout polynôme P réel de degré au plus n. Calculer Δ^p pour tout p.

3.15. Calculer le déterminant de la matrice $(a_{i,j})_{0 \leqslant i,j \leqslant n}$ telle que $a_{0,j} = a^j$ et $a_{i,j} = (j+1)^{i-1}$ si $i > 0$.

3.16. Montrer qu'il existe un polynôme réel T_n tel que, pour tout x réel non nul, on ait $T_n\left(x + \frac{1}{x}\right) = x^n + \frac{1}{x^n}$.

Décomposer en éléments simples la fraction rationnelle $\frac{1}{T_n}$.

3.17. Soit E l'ensemble des $(n+1)$ · uplets de complexes distincts. Pour $z = (z_0, z_1, ..., z_n)$ de E et P de $\mathbb{C}_n[X]$, on pose $N_Z(P) = \sum_{k=0}^{n} |P(z_k)|$. Montrer que N_Z est une norme sur $\mathbb{C}_n[X]$, espace vectoriel des polynômes de degré n au plus.

Pour Z et Z' dans E, comparer N_Z et $N_{Z'}$, et trouver $c > 0$ tel que $N_Z \leqslant cN_{Z'}$.

3.18. Soit $P \in \mathbb{R}[X]$ un polynôme admettant n racines réelles simples strictement supérieures à 1. On pose :

$$Q(x) = (X^2+1)P(X)P'(X) + X(P^2(X) + P'^2(X)).$$

Montrer que Q admet au moins $2n-1$ racines réelles distinctes.

3.19. Soit $P = X^3 + aX^2 + bX + c$ un polynôme unitaire de degré trois à coefficients réels. Trouver une condition sur a, b et c pour que toutes ses racines aient une partie réelle négative.

3.20. a) Montrer que le $n^{\text{ième}}$ polynôme cyclotomique, $\varphi_n(X) = \prod \left(X - \exp \frac{2ik\pi}{n}\right)$, où k décrit l'ensemble des entiers inférieurs ou égaux à n et premiers avec n, est à coefficients entiers.

b) Que peut-on dire d'un nombre premier p divisant $\varphi_n(a)$, où a est entier, mais aucun $\varphi_d(a)$, où d décrit l'ensemble des diviseurs stricts de n ?

c) En déduire qu'il existe une infinité de nombres premiers de la forme $\lambda n + 1$, λ entier.

3.21. Soit un entier $n \geqslant 3$. Montrer qu'il n'existe pas de polynômes P, Q, R à coefficients complexes, non tous trois proportionnels, tels que $P^n + Q^n = R^n$.

3.22. Soit P un polynôme complexe de degré n. On suppose qu'il existe k dans $\mathbb{Z}$ tel que $P(k)$, $P(k+1)$, ..., $P(k+n)$ soient dans $\mathbb{Z}$. Montrer que pour tout i de $\mathbb{Z}$, $P(i)$ est dans $\mathbb{Z}$.

3.23. Soit P dans $\mathbb{Z}[X]$, non nul, et a une racine irrationnelle de P.

a) Montrer qu'il existe c et r dans $\mathbb{R}$, $c > 0$, tels que, pour tout couple (p, q) de $\mathbb{Z} \times \mathbb{N}^*$, on ait $\left|a - \frac{p}{q}\right| \geqslant \frac{c}{q^r}$.

b) Montrer qu'il existe un réel $d > 0$ tel que, pour une infinité de couples (p, q) de $\mathbb{Z} \times \mathbb{N}^*$, on ait $\left|a - \frac{p}{q}\right| \geqslant \frac{d}{q^2}$.

c) Montrer que l'ordre de a, comme racine de P, est inférieur ou égal à $\frac{n}{2}$, n étant le degré de P.

3.24. Soit P dans $\mathbb{C}[X]$ dont les racines ont des parties imaginaires strictement positives. Montrer que P' vérifie la même propriété.

3.25. Soient P et Q deux polynômes non constants de $\mathbb{C}[X]$ tels que l'ensemble des racines de P (resp. $P - 1$) soit égal à l'ensemble des racines de Q, (resp. $Q - 1$). Montrer que $P = Q$. On pourra, si P de degré d, possède m racines distinctes, et si $P - 1$ possède n racines distinctes, montrer que $d \leqslant m + n - 1$.

3.26. Soit les polynômes complexes de degré 2, $P = ax^2 + bx + c$ et $Q = a'x^2 + b'x + c'$. On considère la matrice :

$$A = \begin{pmatrix} 0 & a & 0 & a' \\ a & b & a' & b' \\ b & c & b' & c' \\ c & 0 & c' & 0 \end{pmatrix}.$$

Étudier le rang de A selon le nombre de racines communes des deux polynômes.

3.27. Soit n dans $\mathbb{N}^*$, et le polynôme $P(X) = 1 + X + ... + X^{n-1}$. Quels sont les entiers m tels que l'ensemble des racines de P soit invariant par $z \rightsquigarrow z^m$.

3.28. a) Soit $R(z)$ une fraction rationnelle à coefficients complexes ayant z_0 pour zéro d'ordre k.

Montrer que pour $r > 0$, assez petit, il existe au moins $2k$ points du type $z_k = z_0 + re^{i\theta_k}$ tels que Im $(R(z_k)) = 0$.

b) Soit P et Q dans $\mathbb{R}[X]$ tels que, pour tout (λ, μ) de $\mathbb{R}^2$, $\lambda P + \mu Q$ ait tout ses zéros réels. Montrer que les zéros de P et Q sont intercalés.

3.29. Soit s et p deux nombres complexes. Condition pour que les deux racines du polynôme $X^2 - sX + p$ aient même argument.

3.30. Soit $A \in \mathcal{M}_n(\mathbb{C})$. On définit une suite A_k de matrices en posant $A_0 = A$ et, pour $k \geqslant 1$,

$$A_k = A\left(A_{k-1} - \frac{1}{k} \text{ trace } (A_{k-1})I_n\right).$$

Montrer que $A_n = 0$.

Solutions

3.1. Justifions d'abord l'existence de L(P), évidente si P est nul. Pour P non nul, de degré q, avec $P(X) = \sum_{k=0}^{q} a_k X^k$, on a :

$$u_n = \frac{P(n)z^n}{n!} = \sum_{k=0}^{q} a_k \frac{n^k z^n}{n!}, \text{ et chacune des } q+1 \text{ séries entières,}$$

de terme général $v_{n,k} = \frac{n^k z^n}{n!}$, ($k$ paramètre fixé), a un rayon de convergence infini, car pour z non nul, $\left|\frac{v_{n+1,k}}{v_{n,k}}\right| = \left(\frac{n+1}{n}\right)^k \frac{|z|}{n+1}$ tend vers 0 si n tend vers l'infini, donc pour tout z complexe, la fonction L(P), de $\mathbb{C}$ dans $\mathbb{C}$ existe.

Est-elle polynomiale ? Pour le savoir, on peut remarquer que L(P) dépend linéairement de P, et considérer des polynômes $(P_k)_{k \in \mathbb{N}}$, de degrés échelonnés pour avoir une base de $\mathbb{C}[X]$, adaptée à la situation.

D'abord $P_0(X) = 1$, conduit à $L(1)(z) = e^{-z} \sum_{n=0}^{+\infty} \frac{z^n}{n!} = 1$; puis, pour $k \geqslant 1$, prenons $P_k(x) = x(x-1) \ldots (x-k+1)$, (donc $P_1(x) = x$).

On a $P_k(0) = P_k(1) = \ldots = P_k(k-1) = 0$, et pour $n \geqslant k$,

$$P_k(n) = n(n-1) \ldots (n-k+1).$$

Mais alors $\sum_{n=0}^{+\infty} \frac{P_k(n)}{n!} z^n = \sum_{n=k}^{+\infty} \frac{n(n-1) \ldots (n-k+1)z^{n-k}}{n!} \cdot z^k$

$$= z^k (e^z)^{(k)} = z^k e^z,$$

(les séries entières se dérivent terme à terme sur leur domaine de convergence), et

$$L(P_k)(z) = e^{-z} z^k e^z = z^k.$$

L'image par L, linéaire, de la base des P_k de $\mathbb{C}[X]$ étant la base canonique de $\mathbb{C}[X]$, on peut conclure à l'aspect isomorphisme de L de $\mathbb{C}[X]$ sur lui-même.

3.2. Si A est finie, non vide, l'ensemble des modules de ses éléments admet une borne supérieure atteinte : soit z_0 dans A un élément de module maximum.

La stabilité de A par f et g donne $|f(z_0)| \leqslant |z_0|$ et $|g(z_0)| \leqslant |z_0|$. De plus $f(z_0) - g(z_0) = 2z_0$, d'où, par inégalité triangulaire :

$2|z_0| = |f(z_0) - g(z_0)| \leqslant |f(z_0)| + |g(z_0)| \leqslant 2|z_0|$: on n'a que des égalités : $|z_0| = |f(z_0)| = |g(z_0)|$.

Or $z_0 = 0$ est exclu, ($f(0) = 1$ serait dans A avec $|1| > 0 = |z_0|$), donc les complexes $f(z_0)$ et $-g(z_0)$, non nuls, sont positivement liés pour qu'il y ait égalité dans l'inégalité triangulaire. Comme de plus ils sont alors de même module, (égal à $|z_0|$), ils sont égaux : on a $z_0^2 + z_0 + 1 = -(z_0^2 - z_0 + 1)$ soit $1 + z_0^2 = 0$, d'où $z_0 = i$ ou $-i$. Or $f(i) = i$, $g(i) = -i$, alors que $f(-i) = -i$ et $g(-i) = i$: finalement i et $-i$ sont dans A, et tout autre élément $z = a + ib$ de A est de module inférieur ou égal à 1.

Avec $z = a + ib$, on a :

$$f(z) = (a^2 - b^2 + a + 1) + ib(2a + 1) \text{ et}$$

$$g(z) = (a^2 - b^2 - a + 1) + ib(2a - 1).$$

Comme $|z| \leqslant 1$, on a $|b| \leqslant 1$, donc $1 - b^2 \geqslant 0$, et en posant $a' = a^2 + a + 1 - b^2$ et $a'' = a^2 - a + 1 - b^2$, si $a > 0$, $a' > a$; si $a < 0$, $a'' = |a| + a^2 + 1 - b^2 > |a|$: on voit s'amorcer une croissance des modules des parties réelles ; mais le cas $a = 0$ donne quoi ?

En fait, si $a = 0$, $z = ib$ avec soit $|b| = 1$, et $z = i$ ou $-i$ que l'on sait être dans A, soit $|b| < 1$. On suppose $|b| < 1$.

Mais alors $f(z) = (1 - b^2) + ib$ est dans A avec une partie réelle $1 - b^2$ non nulle et dans tous les cas, on peut partir de $z_1 = a_1 + ib_1$ dans A, supposé différent de $\{i, -i\}$ avec $|a_1| \neq 0$.

En posant, pour $a_1 > 0$, $z_2 = f(z)$, et pour $a_1 < 0$, $z_2 = g(z)$, on a z_2 dans A avec $z_2 = a_2 + ib_2$ et $a_2 \geqslant a_1^2 + |a_1| > 0$.

En posant $z_{n+1} = a_{n+1} + ib_{n+1} = f(z_n)$, pour $n \geqslant 2$, on a une suite d'éléments de A, de parties réelles positives cette fois, avec $a_{n+1} = a_n^2 + a_n + 1 - b_n^2 \geqslant a_n^2 + a_n > 0$.

Mais en définissant une suite $(u_n)_{n \geqslant 2}$ de nombres positifs, par la donnée de $u_2 = a_2 > 0$, et la relation de récurrence $u_{n+1} = u_n^2 + u_n$, l'hypothèse $a_n \geqslant u_n$ implique $a_n^2 + a_n \geqslant u_n^2 + u_n$ d'où *a fortiori* $a_{n+1} \geqslant a_n^2 + a_n \geqslant u_n^2 + u_n = u_{n+1}$. Mais la suite croissante des u_n

diverge vers $+\infty$, (une convergence vers l donnerait $l = l^2 + l$, soit $l = 0$, avec $l \geqslant u_2 > 0$: impossible), donc les a_n divergent vers $+\infty$, alors que $|z_n|^2 = a_n^2 + b_n^2 \leqslant 1$: gênant !

Il est donc absurde de supposer l'existence de z dans A, différent de i ou de $-i$.

Soit alors $P \in \mathbb{C}[X]$ tel que $P(X^2 + X + 1) = P(X)P(X+1)$. Cela ne donne rien sur le degré mais... on est sur $\mathbb{C}$, où tout polynôme est scindé. Soit donc $A = \{a_1, a_2, ..., a_n\}$ l'ensemble des zéros, distincts de P, (peu importe leur multiplicité), si P est non constant.

Comme $P(a_k) = 0$, on a $P(a_k^2 + a_k + 1) = 0$, donc $f(a_k) \in A$.

Comme $P((a_k - 1) + 1) = 0$, on a $P((a_k - 1)^2 + (a_k - 1) + 1) = 0$, soit encore $P(a_k^2 - a_k + 1) = P(g(a_k)) = 0$, donc $g(a_k) \in A$, et vu le début de l'exercice, $A = \{i, -i\}$ et P est du type $P(X) = \lambda(X+i)^r(X-i)^s$. Comme on n'a pas travaillé par équivalences, on vérifie la relation de départ. On doit avoir :

$$\lambda(X^2 + X + 1 + i)^r(X^2 + X + 1 - i)^s = \lambda^2(X + 1 + i)^r(X + 1 - i)^s(X + i)^r(X - i)^s$$

d'où $\lambda = 0$ ou 1, et, comme $X^2 + X + 1 + i = (X + i)(X + 1 - i)$ et

$$X^2 + X + 1 - i = (X - i)(X + 1 + i)$$

pour $\lambda = 1$, l'identité à vérifier devient :

$$(X+i)^r(X+1-i)^r(X-i)^s(X+1+i)^s = (X+1+i)^r(X+1-i)^s(X+i)^r(X-i)^s$$

ce qui exige $r = s$.

Finalement, les solutions sont les polynômes $P(X) = (X^2 + 1)^r$, $r \in \mathbb{N}$, ou $P = 0$. Pour $r = 0$, on retrouve $P = 1$, seul polynôme constant, non nul, solution.

3.3. Comme $P'_n = P_{n-1}$, pour $n \geqslant 1$, la connaissance du signe de P_{n-1} donnera les variations de P_n et, on peut l'espérer, son signe.

On a $P_0(x) = 1, > 0$ sur $\mathbb{R}$, et $P_1(x) = x + 1$ admet un seul zéro, a_1, P_1 étant < 0 si $x < a_1$ et > 0 si $x > a_1$.

On suppose que P_{2n} reste > 0 sur $\mathbb{R}$, et que P_{2n+1} admet un seul zéro, a_{2n+1}, simple, en étant < 0 si $x < a_{2n+1}$ et > 0 après. C'est l'hypothèse de récurrence, vérifiée si $n = 0$.

Tableau de variations de P_{2n+2}, *avec* $P'_{2n+2} = P_{2n+1}$, *puis de* P_{2n+3}.

x	$-\infty$		a_{2n+1}		$+\infty$
P'_{2n+2}		$-$	0	$+$	
P_{2n+2}	$+\infty$	↘		↗	$+\infty$

On a $P_{2n+2}(a_{2n+1}) = \dfrac{(a_{2n+1})^{2n+2}}{(2n+2)!} + P_{2n+1}(a_{2n+1}) = \dfrac{(a_{2n+1})^{2n+2}}{(2n+2)!}$.

Or $P_n(0) = 1$ est vrai pour tout n, donc $a_{2n+1} \neq 0$: on a un minimum pour P_{2n+2}, strictement positif donc P_{2n+2} reste > 0 sur $\mathbb{R}$.

Mais alors, la fonction P_{2n+3}, strictement monotone et variant de $-\infty$ à $+\infty$ s'annule une seule fois en a_{2n+3}, en étant d'abord < 0 puis > 0 : la propriété est récurrente.

Soit par ailleurs a fixé, on a $\lim\limits_{n \to +\infty} P_{2n+1}(a) = e^a > 0$, donc $\exists n_0$, $\forall n \geqslant n_0$, $P_{2n+1}(a) \geqslant \dfrac{1}{2} e^a$, mais alors vu les variations de P_{2n+1} on a : $a_{2n+1} < a$, et finalement on a :

$$\forall a \in \mathbb{R},\ \exists n_0,\ \forall n \geqslant n_0,\ a_{2n+1} < a,$$

ce qui traduit $\lim\limits_{n \to +\infty} a_{2n+1} = -\infty$.

3.4. Dans l'anneau $\mathbb{Q}[X]$, divisons P par P' : il existe un couple unique de polynômes de $\mathbb{Q}[X]$, Q et R, tels que :

$$P = P'Q + R, \text{ avec } R = 0 \text{ ou } d^\circ R \leqslant 1.$$

De plus $P(\alpha) = P'(\alpha) = 0$, implique $R(\alpha) = 0$.

Si $R = 0$, sur $\mathbb{C}$, P' admet deux zéros distincts, ou un double.

Dans le premier cas, on aurait α et β distincts, zéros de P' et de P, donc zéros doubles de P qui n'est que de degré trois : c'est exclu.

Le deuxième cas conduit à $P(\alpha) = P'(\alpha) = P''(\alpha) = 0$, mais P'' est de degré 1, dans $\mathbb{Q}[X]$, donc du type $ax + b$ avec $a \neq 0$ d'où $\alpha = -\dfrac{b}{a}$ dans $\mathbb{Q}$.

Si R est non nul, avec $R(\alpha) = 0$ car α est zéro multiple de P, donc il annule P', on a R de degré un, dans $\mathbb{Q}[X]$, donc du type $aX + b$, avec $a \neq 0$, là encore $\alpha = -\dfrac{b}{a}$ est dans $\mathbb{Q}$.

Tout ceci se généralise sur un corps K quelconque et une clôture algébrique K' de K, en utilisant les développements de Taylor, (c'est de l'algèbre pour les polynômes).

3.5. Les seuls polynômes irréductibles de $\mathbb{C}[X]$ étant de degré 1, si $z_1, ..., z_r$ sont les zéros distincts de P, de multiplicités respectives $\alpha_1, ..., \alpha_r$, et si P est de degré n, de coefficient directeur a, on aura $\alpha_1 + \alpha_2 + ... + \alpha_r = n$ et $P = a \prod_{j=1}^{r} (X - z_j)^{\alpha_j}$.

On suppose P tel qu'il existe p et q dans $\mathbb{N}^*$, avec $(P')^p$ qui divise P^q. Les polynômes constants donnent $P' = 0$: ils sont à écarter, donc $p \geqslant 1$, (d'ailleurs, c'est ce que signifie $p \in \mathbb{N}^*$, suis-je bête).

On a :

$$P' = a \sum_{j=1}^{r} \alpha_j (X - z_j)^{\alpha_j - 1} \prod_{\substack{k=1 \\ k \neq j}}^{r} (X - z_k)^{\alpha_k}$$

$$= a \sum_{j=1}^{r} \alpha_j \underbrace{\left(\prod_{k=1}^{r} (X - z_k)^{\alpha_k - 1} \right)}_{\text{constant en } j} \prod_{\substack{k=1 \\ k \neq j}}^{r} (X - z_k)$$

$$= \left(na \prod_{k=1}^{r} (X - z_k)^{\alpha_k - 1} \right) \underbrace{\sum_{j=1}^{r} \frac{\alpha_j}{n} \prod_{\substack{k=1 \\ k \neq j}}^{r} (X - z_k)}_{\text{noté } Q} .$$

On a $Q(z_j) = \frac{\alpha_j}{n} \prod_{\substack{k=1 \\ k \neq j}}^{r} (z_j - z_k) \neq 0$, donc aucun facteur irréductible divisant P ne divise Q : ces polynômes sont premiers entre eux.

Si on suppose que P'^p divise P^q, on devrait avoir Q qui divise P^q, donc un facteur irréductible de Q devrait diviser P : c'est exclu, c'est que Q est une constante, et vu le coefficient directeur na de P', c'est que $Q = 1$. Mais alors, P', de degré $n - 1 = \left(\sum_{j=1}^{r} \alpha_j \right) - 1$, est égal à $na \prod_{k=1}^{r} (X - z_k)^{\alpha_k - 1}$, qui est de degré $\left(\sum_{k=1}^{r} \alpha_k \right) - r$, donc $r = 1$, et P est

du type $P = a(X-z_1)^{\alpha}$, d'où $P' = \alpha a(X-z_1)^{\alpha-1}$, donc pour un p donné, $P'^p = (\alpha a)^p (X-z_1)^{p(\alpha-1)}$ divisera $P^q = a^q(X-z_1)^{\alpha q}$ si et seulement si q vérifie l'inégalité $p(\alpha-1) \leqslant q\alpha$, ce qui, pour un $\alpha \geqslant 1$ donné, détermine un q_0 tel que les solutions soient les q tels que $q \geqslant q_0$.

Les polynômes cherchés sont donc tous ceux du type :

$P(X) = a(X-z_1)^{\alpha}$, $\alpha \in \mathbb{N}^*$.

3.6. Le polynôme P étant de degré n, le polynôme $X^{l+1}P'$ est de degré $n+l$, son quotient Q par P est de degré $n+l-n = l$, et si on note R le reste, le couple (Q, R) est unique à vérifier la relation :

$$X^{l+1}P' = PQ + R, \text{ avec } R = 0 \text{ ou } d^\circ R < d^\circ P,$$

donc Q est en fait la partie entière de la fraction rationnelle $\dfrac{X^{l+1}P'}{P}$, notée $E\left(\dfrac{X^{l+1}P'}{P}\right)$.

Comme $\dfrac{P'}{P} = \displaystyle\sum_{i=1}^{n} \frac{1}{X-u_i}$, on a :

$$Q = E\left(\sum_{i=1}^{n} \frac{X^{l+1}}{X-u_i}\right)$$

$$= E\left(\sum_{i=1}^{n} \frac{X^{l+1}-u_i^{l+1}}{X-u_i}\right), \text{ puisque les } \frac{u_i^{l+1}}{X-u_i} \text{ sont de partie}$$

entière nulle, et que l'application partie entière est additive.

Comme $X^{l+1} - u_i^{l+1} = (X-u_i)\displaystyle\sum_{k=0}^{l} X^{l-k}u_i^k$,

on obtient $Q = \displaystyle\sum_{i=1}^{n}\left(\sum_{k=0}^{l} u_i^k X^{l-k}\right)$

$$= \sum_{k=0}^{l}\left(\sum_{i=1}^{n} u_i^k\right)X^{l-k} = \sum_{k=0}^{l} S_k X^{l-k},$$

d'où le résultat cherché.

3.7. Des polynômes, cela se dérive, et avoir $Q = P + P' + ... + P^{(n)}$, incite à calculer $Q' = P' + P'' + ... + P^{(n)} + 0$, d'où l'on constate que $Q' - Q = -P(x)$.

L'équation différentielle sans second membre $y' - y = 0$, a pour solution $y = \lambda e^x$, et la méthode de variation des constantes conduit à intégrer $\lambda' = -P(x)e^{-x}$.

Mais, comme Q est solution de cette équation, avec la fonction $\lambda(x)$ telle que $Q(x) = \lambda(x)e^x$, c'est-à-dire $\lambda(x) = Q(x)e^{-x}$, on a encore :

$(Q(x)e^{-x})' = -P(x)e^{-x}$, d'où avec x_0 fixé,

$$Q(x)e^{-x} - Q(x_0)e^{-x_0} = -\int_{x_0}^{x} P(t)e^{-t}dt = \int_{x}^{x_0} P(t)e^{-t}dt,$$

et cette relation est valable pour tout couple (x, x_0) : on fait tendre x_0 vers $+\infty$, comme P et Q sont des polynômes, il vient :

$$Q(x)e^{-x} = \int_{x}^{+\infty} P(t)e^{-t}dt \text{ soit } Q(x) = e^x \int_{x}^{+\infty} P(t)e^{-t}dt,$$

ce qui donne bien $Q(x) \geqslant 0$.

3.8. Supposons que l'on ait une décomposition $P = QR$ avec Q et R dans $\mathbb{Z}[X]$. Alors $Q(a_i)$ et $R(a_i)$ sont dans $\mathbb{Z}$, et tels que $Q(a_i)R(a_i) = P(a_i) = -1$: on n'a pas le choix, l'un des entiers vaut 1, l'autre -1, donc $(R + Q)(a_i) = 0$.

Mais alors si Q et R sont de degrés $< n$, $R + Q$ est de degré $k < n$, ce polynôme s'annule n fois : il est identiquement nul, d'où $R = -Q$ et $P = -Q^2$.

Mais le coefficient directeur de $-Q^2$ est négatif alors que P est unitaire : c'est exclu.

On a donc Q ou R de degré n.

3.9. Soient $a_1, a_2, ..., a_n$ et $b_1, b_2, ..., b_q$, les zéros réels distincts de P et Q, respectivement, indexés en croissant.

Si α et β sont les coefficients directeurs, non nuls, de P et Q, $\forall(\lambda, \mu) \in \mathbb{R}^2$, $\lambda P + \mu Q = (\lambda\alpha)\dfrac{P}{\alpha} + (\mu\beta)\dfrac{Q}{\beta}$, avec $\lambda' = \lambda\alpha$ et $\mu' = \mu\beta$ qui décrivent $\mathbb{R}$ lorsque λ et μ sont quelconques. Donc on peut supposer P et Q unitaires.

On peut aussi supposer λ et μ tous deux non nuls, (si $\lambda = 0$, μQ est scindé...).

Supposons $a_1 \leqslant b_1$, entre a_1 et a_2, seul figure b_1, (si $a_1 \leqslant b_1 < b_2 \leqslant a_2$, il y aurait un zéro de P entre b_1 et b_2, lequel ?) : on a donc une répartition du type $a_1 \leqslant b_1 \leqslant a_2 \leqslant b_2 \leqslant a_3 \ldots$, avec bien sûr les a_i distincts, ainsi que les b_j, l'hypothèse $a_1 \leqslant b_1$ ne nuisant pas à la généralité de la solution.

En fait si un a_i est un b_j, on peut le « supprimer », car alors $x - a_i = x - b_j$ est en facteur dans P et Q donc dans $\lambda P + \mu Q$, et ce polynôme sera scindé si et seulement si $\dfrac{\lambda P + \mu Q}{x - a_i}$ l'est.

Enfin, si $a_1 < b_1 < a_2 = b_2 < a_3 \ldots$, supprimer a_2 et b_2 dans chaque suite de zéros ne modifie pas l'imbrication des deux suites : on peut donc supposer les a_i et les b_j tous différents, et si $a_1 < b_1$, on a les inégalités

① : $a_1 < b_1 < a_2 < b_2 < \ldots < a_n < b_n$, ou

② : $a_1 < b_1 < a_2 < b_2 < \ldots < a_n < b_n < a_{n+1}$.

Comme les zéros sont simples, les polynômes changent de signe en chacun de leurs zéros, donc $Q(a_i)Q(a_{i+1}) < 0$, (et $P(b_i)P(b_{i+1}) < 0$).

Mais alors $(\lambda P + \mu Q)(a_i) = \mu Q(a_i)$, d'où $\lambda P + \mu Q$ de signes contraires en a_i et a_{i+1} : le polynôme $\lambda P + \mu Q$ s'annule sur chaque $]a_i, a_{i+1}[$, (n'oubliez pas l'hypothèse $\mu \neq 0$).

Dans le cas ①, $\lambda P + \mu Q$ est de degré n au plus, et a déjà $n - 1$ zéros distincts, dans le cas ②, il est de degré $n + 1$ et admet n zéros réels distincts : dans chaque cas il ne reste, après factorisation, qu'un zéro réel donc $\lambda P + \mu Q$ est scindé sur $\mathbb{R}$.

En fait, avec $\lambda\mu \neq 0$, et les a_i et les b_j tous distincts, $\lambda P + \mu Q$ est simplement scindé.

En effet ni les a_i, ni les b_j n'annulent alors $\lambda P + \mu Q$, donc $\lambda P + \mu Q = 0 \Leftrightarrow \dfrac{Q}{P} = -\dfrac{\lambda}{\mu}$. Or la fraction rationnelle $\dfrac{Q}{P}$ admet $a_1, \ldots, a_n$, (ou $a_1, \ldots, a_n, a_{n+1}$) pour pôles.

Dans le cas de $d°P = d°Q = n$, $\lim\limits_{x \to \pm\infty} \dfrac{Q}{P} = 1$, (les polynômes sont unitaires), donc sur $]a_n, +\infty[$, $\dfrac{Q}{P}$ croît de $-\infty$ à 1 ; sur chaque

$]a_i, a_{i+1}[$, $\frac{Q}{P}$ croît de $-\infty$ à $+\infty$, et sur $]-\infty, a_1[$, $\frac{Q}{P}$ croît de 1 à $+\infty$, (pôles en a_i, avec changement de signe de, la fraction s'annulant en chaque b_i).

Il en résulte que $\frac{Q(x)}{P(x)} = -\frac{\lambda}{\mu}$ est une valeur prise n fois sauf... si $\frac{-\lambda}{\mu} = 1$, mais alors $\lambda + \mu = 0$, $\lambda P + \mu Q$ n'est plus que de degré $n-1$, et on a $\frac{-\lambda}{\mu}$ prise $n-1$ fois, (sur chaque $]a_i, a_{i+1}[$).

Si $d°P = n+1 = d°Q+1$, là, pas de problème, la limite en $+\infty$ et $-\infty$ de $\frac{Q}{P}$ est nulle et $\frac{Q(x)}{P(x)} = \frac{-\lambda}{\mu}$ est obtenue pour $n+1$ valeurs de x.

3.10. En introduisant $E = \mathbb{C}^n$, et u l'endomorphisme de E, de matrice M dans une base de E, on sait, (Théorème de Dunford) que u s'écrit de manière unique $u = d + v$ avec d diagonalisable et v nilpotent, donc u est nilpotent si et seulement si d est nul, soit si et seulement si u n'admet que 0 pour valeur propre.

On peut aussi trigonaliser M, et le moindre soupçon de $\lambda_j \neq 0$ sur la diagonale donnera un λ_j^k sur la diagonale de M^k, alors qu'une diagonale nulle impliquera la nullité de M^n, les termes non nuls « remontant d'un cran » quand on passe de M^k à M^{k+1}, avec M triangulaire.

On suppose donc que, pour $k = 1, 2, ..., n$, trace $M^k = 0$, et on veut justifier que 0 est seule valeur propre. Il y a de nombreuses solutions. En voici une, où Taylor Lagrange interviendra.

On procède par l'absurde en supposant que le polynôme caractéristique unitaire de M, se décompose sur $\mathbb{C}$ en :

$$P(X) = X^{n-r} \prod_{j=1}^{r} (X - \lambda_j), \text{ avec } r \geqslant 1 \text{ et } \lambda_1, ..., \lambda_r \text{ non nuls.}$$

Posons $Q(x) = \prod_{j=1}^{r} (X - \lambda_j)$.

Par Taylor Lagrange, on a pour chaque λ_j :

$$Q(x + \lambda_j) = \sum_{k=0}^{r} \lambda_j^k \frac{Q^{(k)}(x)}{k!},$$

d'où, pour ne pas faire de jaloux parmi les λ_j, en sommant :

$$\sum_{j=1}^{r} Q(x+\lambda_j) = \sum_{k=0}^{r} \left(\sum_{j=1}^{r} \lambda_j^k \right) \frac{Q^{(k)}(x)}{k!}.$$

Mais, M étant semblable à une matrice triangulaire de diagonale $(\lambda_1, ..., \lambda_r, 0, 0, ..., 0)$, on a $\sum_{j=0}^{r} \lambda_j^k = \text{trace } M^k$, pour tout $k \geqslant 1$, soit ici une somme nulle.

Il reste donc l'égalité $\sum_{j=1}^{r} Q(x+\lambda_j) = rQ(x)$. Or, pour $x = 0$, chaque $Q(\lambda_j)$ étant nul, on obtient $rQ(0) = 0$, d'où 0 racine de Q, ce qui est exclu.

L'hypothèse de départ est absurde et 0 est bien seule valeur propre de M.

La réciproque est évidente : si M est nilpotent, les λ_j sont tous nuls, donc les traces des matrices M^k sont nulles.

3.11. La relation à vérifier :

$$① \quad \alpha P(-2) + \beta P'(-2) + \gamma P(-1) + \delta P\left(\frac{1}{2}\right) = P'(a),$$

dépend linéairement de P, donc elle sera vérifiée pour tout P de $\mathbb{R}_4[X]$ si et seulement si elle l'est pour les 5 vecteurs d'une base de $\mathbb{R}_4[X]$, et on va essayer de bien choisir cette base, en prenant des vecteurs P tels que trois des quatre conditions $P(-2) = 0$, $P'(-2) = 0$, $P(-1) = 0$ et $P\left(\frac{1}{2}\right) = 0$ soient vérifiées, cela simplifierait tout.

Posons $P_1(X) = (X+2)(X+1)\left(X-\frac{1}{2}\right)$

$$P_2(X) = (X+2)^2\left(X-\frac{1}{2}\right)$$

$$P_3(X) = (X+2)^2(X+1)$$

$$P_4(X) = (X+2)^2(X+1)\left(X-\frac{1}{2}\right)$$

et $P_5(X) = (X+1)\left(X-\frac{1}{2}\right)(X-b)$

en choisissant b tel que $P'_5(-2) = 0$, si c'est possible. Or :

$$P'_5(X) = \left(X-\frac{1}{2}\right)(X-b) + (X+1)(X-b) + (X+1)\left(X-\frac{1}{2}\right),$$

on doit avoir :

$$0 = \left(-\frac{5}{2}\right)(-2-b) - (-2-b) - \left(-\frac{5}{2}\right), \text{ d'où l'on tire } b = -\frac{19}{7},$$

sauf erreur.

On a 5 polynômes indépendants, car si on a :

$\lambda_1 P_1 + \lambda_2 P_2 + \lambda_3 P_3 + \lambda_4 P_4 + \lambda_5 P_5 = P = 0$, avec $P(-2) = 0$ il reste $\lambda_5 P_5(-2) = 0$ avec $P_5(-2) \neq 0$ d'où $\lambda_5 = 0$;

puis $P(-1) = 0 = \lambda_2 P_2(-1)$ avec $P_2(-1) \neq 0 \Rightarrow \lambda_2 = 0$;

avec $P\left(\frac{1}{2}\right) = 0$ on a $\lambda_3 = 0$, et $P'(-2) = 0$ donne $\lambda_1 = 0$; d'où finalement $\lambda_4 = 0$: on a une base de $\mathbb{R}_4[X]$.

On aura alors ① vérifiée si elle l'est pour les P_j, $1 \leqslant j \leqslant 5$, d'où les conditions :

$$\begin{cases} \beta P'_1(-2) = P'_1(a) \\ \gamma P_2(-1) = P'_2(a) \\ \delta P_3\left(\frac{1}{2}\right) = P'_3(a) \\ 0 = P'_4(a) \\ \alpha P_5(-2) = P'_5(a), \end{cases}$$

que doivent vérifier α, β, γ, δ et a.

On doit prendre pour a un zéro réel, différent de -2, de P'_4, or $P_4\left(\frac{1}{2}\right) = P_4(-1) = 0$: par Rolle on sait qu'il existe a entre -1 et $\frac{1}{2}$, (donc différent de -2), tel que $P'(a) = 0$. En choisissant ainsi a, les autres relations déterminent α, β, γ et δ de manière unique, donc ① est vérifiée pour tout P de $\mathbb{R}_4[X]$.

Un calcul explicite donne $P'_4(X) = X(X+2)\left(4X+\frac{11}{2}\right)$, d'où $a = 0$ ou $a = -\frac{11}{8}$, sauf erreur.

3.12. C'est un exercice de tout repos ! D'abord, si $a = 0$, il est dans $\mathbb{Z}$. Sinon, en écrivant $a = \frac{p}{q}$, avec p dans $\mathbb{Z}^*$ et q dans $\mathbb{N}^*$, premiers entre eux, et si P, de degré n, s'écrit $X^n + \sum_{k=0}^{n-1} a_k X^k$, on aura :

$\frac{p^n}{q^n} = -\sum_{k=0}^{n-1} a_k \frac{p^k}{q^k}$, donc, en multipliant par q^{n-1}, chaque q^{n-1-k} est entier, les a_k sont entiers, donc $\frac{p^n}{q} = -\sum_{k=0}^{n-1} a_k p^k q^{n-1-k}$ est dans $\mathbb{Z}$.

Mais p et q étant premiers entre eux, c'est que $q = 1$, (sinon, aucun diviseur de q ne diviserait p^n), donc a est dans $\mathbb{Z}$.

3.13. Comme il est question du signe des valeurs prises par les fonctions polynômes, on va faire intervenir les zéros, réels ou complexes d'un polynôme P.

Soit $P \in \mathbb{R}_{2n}[X]$, de zéros réels les β_i, de multiplicités respectives s_i, les zéros complexes étant alors conjugués deux à deux, de même multiplicité, peuvent se noter α_j et $\overline{\alpha_j}$ de multiplicité chacun r_j. Le polynôme P se décompose alors en :

$$P(x) = \lambda \prod_j ((x-\alpha_j)(x-\overline{\alpha_j}))^{r_j} \prod_i (x-\beta_i)^{s_i}, \quad \text{avec } \lambda \text{ coefficient}$$

directeur de P, (et sans qu'il soit utile de préciser le nombre de zéros).

Si on suppose alors $P(\mathbb{R}) \subset \mathbb{R}_+$, d'abord le degré de P est pair, et λ est positif ou nul, donc s'écrit $\lambda = (\sqrt{\lambda})^2$, puis chaque s_i est pair, donc, en posant $s_i = 2\sigma_i$ et :

$$Q(x) = \sqrt{\lambda} \prod_j (x-\alpha_j)^{r_j} \prod_i (x-\beta_i)^{\sigma_i},$$

on aura $P(x) = Q(x)\overline{Q(x)}$, avec $Q \in \mathbb{C}_n[X]$.

La réciproque est évidente, donc on a déjà :

$$P \text{ tel que } P(\mathbb{R}) \subset \mathbb{R}_+ \Leftrightarrow \exists Q \in \mathbb{C}_n[X], P = Q\overline{Q}.$$

Passons à la justification de l'exercice. On a (i) $\Rightarrow$ (ii) sans problème.

On a (ii) $\Rightarrow$ (iii). Soit $B = (b_0, b_1, ..., b_n)$ un vecteur de $\mathbb{R}^{n+1}$, on veut prouver que $\phi(B) = \sum_{0 \leq i,j \leq n} a_{i+j} b_i b_j$ est positif.

Si on introduit $Q(x) = \sum_{i=0}^{n} b_i x^i$, on a un polynôme de $\mathbb{R}_n[X]$ donc de $\mathbb{C}_n[X]$, et $P = Q\overline{Q} = Q^2$ est tel que $P(\mathbb{R}) \subset \mathbb{R}_+$: d'après (ii) on a $\delta(A)(P)(0) \in \mathbb{R}^+$, soit encore $\sum_{k=0}^{2n} \frac{a_k}{k!} P^{(k)}(0) \in \mathbb{R}^+$.

Or $P(x) = \sum_{0 \leqslant i,j \leqslant n} b_i b_j x^{i+j}$, donc $P^{(k)}(0) = \sum_{\substack{i+j=k \\ 0 \leqslant i,j \leqslant n}} k! b_i b_j$.

En posant $b_i = 0$ si $n < i \leqslant 2n$, on pourra, pour k variant de 0 à $2n$, prendre i et j tels que $i+j = k$, sous la forme i et $k-i$, puisque si l'un de ces 2 entiers est supérieur à n, le b associé sera nul.

Donc, avec cette convention, $P^{(k)}(0) = \sum_{i=0}^{k} k! b_i b_{k-i}$ et :

$$\delta(A)(P)(0) = \sum_{k=0}^{2n} \frac{a_k}{k!} \sum_{i=0}^{k} k! b_i b_{k-i} = \sum_{k=0}^{2n} a_k \sum_{i=0}^{k} b_i b_{k-i}.$$

Que faire si ce n'est intervertir les sommations :

$$\delta(A)(P)(0) = \sum_{i=0}^{2n} \sum_{k=i}^{2n} a_k b_i b_{k-i},$$

et, comme pour i fixé, $k \geqslant i$ s'écrit $k = i+j$, on aura j variant de 0 à $2n-i$, d'où :

$$\delta(A)(P)(0) = \sum_{i=0}^{2n} \sum_{j=0}^{2n-i} a_{i+j} b_i b_j \text{ : on approche du résultat.}$$

Faisons le ménage : si $i > n$, $b_i = 0$: la première somme s'arrête à $i = n$, mais alors $2n - i \geqslant n$, et b_j étant nul si $j > n$, la deuxième somme s'arrête à n aussi d'où :

$$\delta(A)(P)(0) = \sum_{i=0}^{n} \sum_{j=0}^{n} a_{i+j} b_i b_j.$$

Comme $\delta(A)(P)(0) \geqslant 0$, on a bien $\phi(B)$ positif, pour tout vecteur B de $\mathbb{R}^{n+1}$, d'où la propriété (iii).

Enfin (iii) $\Rightarrow$ (i). Soit $P \in \mathbb{R}_{2n}[X]$, tel que $P(\mathbb{R}) \subset \mathbb{R}_+$, et a réel, on veut prouver que $\delta(A)(P)(a) \geqslant 0$. Le calcul précédent reliant la valeur prise par la forme quadratique à la valeur en 0 d'un polynôme, on va

d'abord translater la variable et se ramener en 0 en posant $R(x) = P(x+a)$.

On a $R(\mathbb{R}) \subset \mathbb{R}_+$, et $P^{(j)}(a) = R^{(j)}(0)$, donc :

$$\delta(A)(P)(a) = \delta(A)(R)(0).$$

En écrivant $R(x) = \overline{Q}(x)Q(x)$, et en posant $Q(x) = \sum_{j=0}^{n} b_j x^j$, (avec les b_j complexes, ce qui est possible car $R(\mathbb{R}) \subset \mathbb{R}_+$), les calculs faits pour prouver que (ii) $\Rightarrow$ (iii) se refont dans le domaine complexe, et $\tilde{\phi}$ étant cette fois la forme hermitienne définie par :

$$\tilde{\phi}(z_0, ..., z_n) = \sum_{0 \leqslant i,j \leqslant n} a_{i+j} \bar{z}_i z_j,$$

avec $B = (b_0, ..., b_n)$, on obtiendrait :

$$\tilde{\phi}(B) = \delta(A)(R)(0) = \delta(A)(P)(a).$$

Mais ϕ, de matrice symétrique réelle $(a_{i+j})_{0 \leqslant i,j \leqslant n}$ étant forme quadratique positive, n'a que des valeurs propres positives, et s'étend en $\tilde{\phi}$ hermitienne positive.

Finalement, $\tilde{\phi}(B)$ est positif, d'où $\delta(A)(P)(a) \geqslant 0$, ceci pour tout a de $\mathbb{R}$, on conclut bien à $\delta(A)(P)(\mathbb{R}) \subset \mathbb{R}_+$.

3.14. Sur l'espace vectoriel $E_n = \mathbb{R}_n[X]$ des polynômes à coefficients réels de degré n au plus, Δ est linéaire et un polynôme de degré $q \leqslant n$, aura pour image un polynôme de degré $q-1$.

Il en résulte que, pour $p > n$, $\Delta^p = 0$.

Pour $p \leqslant n$, on procède par récurrence en remarquant que :

$(\Delta P)(X) = Q(X) = P(X+1) - P(X)$, d'où :

$(\Delta^2 P)(X) = Q(X+1) - Q(X) = P(X+2) - 2P(X+1) + P(X)$.

Si on suppose que $(\Delta^p P)(X) = \sum_{i=0}^{p} C_p^i (-1)^{p-i} P(X+i)$, formule vraie pour $p = 1$ et 2, en notant $R(X)$ ce polynôme, et si $p < n$, on aura :

$$\begin{aligned}(\Delta^{p+1} P)(X) &= R(X+1) - R(X) \\ &= \sum_{i=0}^{p} C_p^i (-1)^{p-i} P(X+i+1) - \sum_{i=0}^{p} C_p^i (-1)^{p-i} P(X+i) \\ &= \sum_{j=1}^{p+1} C_p^{j-1} (-1)^{p-j+1} P(X+j) - \sum_{i=0}^{p} C_p^i (-1)^{p-i} P(X+i).\end{aligned}$$

Si on veut regrouper, pour k variant de 0 à $p+1$, les coefficients de $P(X+k)$, les termes associés à 0 et $p+1$ sont à part.

On a :

$$C_p^p(-1)^{p+1-(p+1)}P(X+p+1) = C_{p+1}^{p+1}(-1)^{p+1-(p+1)}P(X+p+1),$$

puis : $-C_p^0(-1)^{p-0}P(X+0) = C_{p+1}^0(-1)^{p+1-0}P(X+0)$.

Pour $1 \leqslant k \leqslant p$, le coefficient de $P(X+k)$ est :

$C_p^{k-1}(-1)^{p+1-k} - C_p^k(-1)^{p-k} = (-1)^{p+1-k}(C_p^{k-1} + C_p^k)$, ce qui, triangle de Pascal oblige, redonne $C_{p+1}^k(-1)^{p+1-k}$. Donc on a $(\Delta^{p+1}P)(X) = \sum_{j=0}^{p+1} C_{p+1}^j(-1)^{p-j}P(X+j)$, et la formule est récurrente.

3.15. On a un déterminant d'ordre $n+1$,

$$D = \begin{vmatrix} 1 & a & a^2 & & a^n \\ 1 & 1 & 1 & & 1 \\ 1 & 2 & 3 & & n+1 \\ 1 & 2^2 & 3^2 & \dots & (n+1)^2 \\ \hline 1 & 2^{n-1} & 3^{n-1} & \dots & (n+1)^{n-1} \end{vmatrix}$$

que l'on développe par rapport à la première ligne, vu son rôle particulier.

En notant $V(a_1, a_2, \dots, a_n)$ le déterminant de Vandermonde,

$$\begin{vmatrix} 1 & 1 & & 1 \\ a_1 & a_2 & \dots & a_n \\ \hline a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant j < i \leqslant n} (a_i - a_j), \text{ (calcul classique)}$$

on a $D = \sum_{j=0}^{n} (-1)^j a^j V(1, 2, \dots, j, j+2, \dots, n+1)$.

Il nous faut donc calculer $d_j = V(1, 2, \dots, j, j+2, \dots, n+1)$.

On trouve :

$$\begin{aligned} d_j &= [(2-1)(3-1)\ldots(j-1)(j+1)\ldots n] \\ &\quad \times [(3-2)\ldots(j-2)j(j+1)\ldots(n-1)] \times \ldots \\ &\quad \times [(j-(j-1))(j+2-(j-1))\ldots(n-j+2)] \\ &\quad \times (n-j+1)!(n-j-1)!(n-j-2)!\ldots 2! \\ &= \frac{n!}{j} \times \frac{(n-1)!}{j-1} \times \ldots \times \frac{(n-j+2)!}{2} \times (n-j+1)!(n-j-1)! \ldots 3!2! \\ &= \frac{\prod_{k=1}^{n} k!}{j!(n-j)!}, \end{aligned}$$

$$\text{donc } D = \sum_{j=0}^{n} (-a)^j \frac{n!}{j!(n-j)!} \prod_{k=1}^{n-1} k! = \left(\prod_{k=1}^{n-1} k!\right)\left(\sum_{j=0}^{n} C_n^j (-a)^j\right)$$

$$= (1-a)^n \prod_{k=1}^{n-1} k!$$

3.16. On peut procéder par récurrence, en remarquant que :

$$T_1(u) = u \text{ donne } T_1\left(x+\frac{1}{x}\right) = x+\frac{1}{x}.$$

On suppose la propriété vraie pour $j = 1, 2, \ldots, n-1$.

On a $\left(x+\frac{1}{x}\right)^n = x^n + \frac{1}{x^n} + \sum_{k=1}^{n-1} C_n^k x^k \cdot \frac{1}{x^{n-k}}$.

Si $n = 2p+1$, on a, en regroupant C_n^k et C_n^{n-k}, pour $1 \leqslant k \leqslant p$:

$$\begin{aligned} x^n + \frac{1}{x^n} &= \left(x+\frac{1}{x}\right)^n - \sum_{k=1}^{p} C_n^k \left(\frac{1}{x^{n-2k}} + x^{n-2k}\right) \\ &= \left(x+\frac{1}{x}\right)^n - \sum_{k=1}^{p} C_n^k T_{n-2k}\left(x+\frac{1}{x}\right), \end{aligned}$$

avec $n-2k$ variant entre 1 et $n-2$. Dans ce cas,

$$T_n(y) = T_{2p+1}(y) = y^n - \sum_{k=1}^{p} C_n^k T_{n-2k}(y) \text{ est solution.}$$

Si $n = 2p$, on groupera les termes 2 à 2, sauf $C_{2p}^{p} x^p \cdot \frac{1}{x^p}$, d'où :

$$\left(x + \frac{1}{x}\right)^{2p} = x^{2p} + \frac{1}{x^{2p}} + C_{2p}^{p} + \sum_{k=1}^{p-1} C_n^k \left(\frac{1}{x^{n-2k}} + x^{n-2k}\right),$$

d'où $T_{2p}(y) = y^{2p} - \sum_{k=1}^{p-1} C_n^k T_{n-2k}(y) - C_{2p}^{p}$.

On a bien existence d'un tel polynôme T_n, qui est de degré n, unitaire.

Pour z complexe tel que $z^n + \frac{1}{z^n} = 0$, soit $z^{2n} = -1$, on aura $T_n\left(z + \frac{1}{z}\right) = 0$.

Or $z^{2n} = -1$ équivaut à $z_k = e^{i(2k+1)\pi/2n}$, pour $k = 0, 1, ..., 2n-1$, et $\frac{1}{z_k} = \overline{z_k}$ d'où :

$$z_k + \frac{1}{z_k} = 2\cos\left(\frac{2k+1}{2n}\pi\right) = x_k, \text{ valeur réelle qui annule } T_n.$$

Pour $k = 0, 1, ..., n-1$, les angles $\theta_k = \frac{2k+1}{2n}\pi$ varient en croissant de $\frac{\pi}{2n}$ à $\pi - \frac{\pi}{2n}$, et donnent n valeurs distinctes des $\cos\theta_k$: on a les n zéros réels distincts de T_n, polynôme de degré n.

On a donc $\frac{1}{T_n(x)} = \sum_{k=0}^{n-1} \frac{\alpha_k}{x - 2\cos\frac{(2k+1)\pi}{2n}}$

avec $\alpha_k = \frac{1}{T'_n\left(2\cos\frac{(2k+1)\pi}{2n}\right)}$.

3.17. On peut se lancer dans la vérification des propriétés des normes, mais on peut aussi aller chercher les polynômes interpolateurs de Lagrange, les Q_j, avec :

$$Q_j(z) = \prod_{\substack{k=0 \\ k \neq j}}^{n} \frac{z - z_k}{z_j - z_k},$$

polynômes de degré n, en nombre $n+1$, qui forment une famille libre de $\mathbb{C}_n[X]$, car $\sum_{j=0}^{n} \lambda_j Q_j(z) = 0$, calculé en z_k donne $\lambda_k = 0$, ceci pour tout k. On a une base de $\mathbb{C}_n[X]$, et, pour $P = \sum_{j=0}^{n} \lambda_j Q_j$, décomposé dans cette base, on a $N_Z(P) = \sum_{k=0}^{n} \left| \left(\sum_{j=0}^{n} \lambda_j Q_j \right)(z_k) \right| = \sum_{k=0}^{n} |\lambda_k| = \|P\|_1$, norme usuelle cette fois sur un espace vectoriel de dimension $n+1$, rapporté à une base, puisque c'est la somme des modules des composantes scalaires.

Si vous y tenez, vous pouvez faire les vérifications !

Comme on est en dimension finie, toutes les normes sont équivalentes, donc si on se donne deux $(n+1)$ .uplets dans E, Z et Z', il existe une constante $c > 0$ telle que $N_Z \leqslant c N_{Z'}$.

En notant cette fois $(P_j)_{0 \leqslant j \leqslant n+1}$ les polynômes interpolateurs de Lagrange pour la famille Z', on doit avoir en particulier $N_Z(P_j) \leqslant c N_{Z'}(P_j)$, avec $N_{Z'}(P_j) = 1$, donc $c \geqslant c_0 = \sup \{N_Z(P_j) ; j = 0, ..., n\}$.

Or, avec cette constante c_0, et pour P décomposé en $\sum_{j=0}^{n} \lambda_j P_j$, on a :

$$N_Z(P) \leqslant \sum_{j=0}^{n} |\lambda_j| N_Z(P_j) \leqslant \sum_{j=0}^{n} |\lambda_j| c_0 = c_0 \sum_{j=0}^{n} |\lambda_j| \text{, soit :}$$

$$N_Z(P) \leqslant c_0 N_{Z'}(P) : c_0 = \sup \{N_Z(P_j) ; j = 0, ..., n\}$$

est la meilleure valeur de c convenant.

3.18. On peut considérer l'expression $(X^2+1)PP' + X(P^2 + P'^2)$ comme un polynôme en X du second degré, (P et P' devenant des coefficients), pour en chercher une éventuelle factorisation.

On a un discriminant Δ valant $(P^2 + P'^2)^2 - 4P^2P'^2 = (P^2 - P'^2)^2$, d'où des « zéros » : $\frac{-(P^2 + P'^2) \pm (P^2 - P'^2)}{2PP'}$ égaux à $-\frac{P'}{P}$ et à $-\frac{P}{P'}$, ce qui conduit à une factorisation de Q en $Q(X) = (XP + P')(XP' + P)$, et on va chercher les zéros de chacun des deux facteurs, avec intervention de la dérivée logarithmique de P.

On sait que P admet n zéros simples > 1, indexés en : $1 < x_1 < x_2 < \ldots < x_n$. Donc la décomposition en éléments simples de $\frac{P'}{P}$ sera du type :

$$\frac{P'(x)}{P(x)} = \sum_{i=1}^{n} \frac{1}{x - x_i} + f(x),$$

avec $f(x)$ fraction rationnelle définie pour $x > 1$.

On a donc $\lim\limits_{x \to x_i^-} \frac{P'(x)}{P(x)} = -\infty$ et $\lim\limits_{x \to x_i^+} \frac{P'(x)}{P(x)} = +\infty$.

Mais alors, sur chaque intervalle ouvert $]x_i, x_{i+1}[$, (pour $1 \leqslant i \leqslant n-1$, la fonction $x \rightsquigarrow P(x)\left(x + \frac{P'(x)}{P(x)}\right)$ va s'annuler car le facteur $x + \frac{P'(x)}{P(x)}$ a pour limites $-\infty$ et $+\infty$ en ces deux bornes, donc, continuité oblige, il s'annule en $\alpha_i \in]x_i, x_{i+1}[$.

Il en est de même de la fonction $x \rightsquigarrow xP(x)\left(\frac{P'(x)}{P(x)} + \frac{1}{x}\right)$ car $\frac{P'(x)}{P(x)} + \frac{1}{x}$ tend vers $+\infty$ en x_i^+ et $-\infty$ en x_{i+1}^-, d'où un $\beta_i \in]x_i, x_{i+1}[$ tel que $\beta_i P'(\beta_i) = -P(\beta_i)$.

Comme $\alpha_i P(\alpha_i) = -P'(\alpha_i)$, l'égalité $\alpha_i = \beta_i$ impliquerait $\frac{P'(\beta_i)}{P(\beta_i)} = -\frac{1}{\beta_i} = \frac{P'(\alpha_i)}{P(\alpha_i)} = -\alpha_i = -\beta_i$ donc $\beta_i^2 = 1$, avec $\beta_i > 1$: c'est exclu.

On dispose donc déjà de $2(n-1)$ racines réelles distinctes (et > 1), pour Q.

On en veut une de plus que l'on va chercher dans $]0, x_1[$. Si P admet des zéros dans $[0, 1]$, soit x_0 le zéro le plus près de x_1, supposé de multiplicité α, on rajoute $\frac{\alpha}{x - x_0}$ dans la décomposition de $\frac{P'}{P}$, et on récupère deux zéros α_0 et β_0 dans $]x_0, x_1[$, par le raisonnement précédent, avec cependant la possibilité d'avoir $\alpha_0 = \beta_0 = 1$ cette fois, donc en fait au moins un zéro de plus pour Q.

Si P ne s'annule pas sur $[0, 1]$, on a $\lim\limits_{x \to 0^+} \frac{P'(x)}{P(x)} + \frac{1}{x}$ qui vaut $+\infty$, (la fraction rationnelle f est cette fois définie sur $[0, +\infty[$, et

$\lim_{x \to x_1^-} \frac{P'(x)}{P(x)} + \frac{1}{x} = -\infty$, donc ce facteur $\frac{P'(x)}{P(x)} + \frac{1}{x}$ s'annule en un $\beta_0 \in]0, x_1[$, d'où un zéro de plus pour Q. On a au moins $2n-1$ zéros réels distincts, (et > 0), pour Q.

3.19. Le polynôme P, unitaire de degré impair admet un zéro réel et deux autres, réels ou imaginaires conjugués. On note x_1 la plus grande racine réelle, on peut alors noter $z_2 = x_2 + iy_2$ et $z_3 = x_3 + iy_3$ les deux autres racines, avec soit $y_2 = y_3 = 0$, (et $x_2 \leqslant x_1, x_3 \leqslant x_1$), soit $y_3 = -y_2$, non nul mais alors $x_3 = x_2$. On a donc $z_2 = x_2 + iy_2$ et $z_3 = x_3 - iy_2$ avec $y_2(x_2 - x_3) = 0$.

Supposons x_1, x_2 et x_3 négatifs.

Les relations entre coefficients et racines donnent :

① : $a = -x_1 - x_2 - x_3 - iy_2 + iy_2 = -(x_1 + x_2 + x_3) \geqslant 0$;

$b = x_1(x_2 + x_3) + z_2 z_3$ avec :

$z_2 z_3 = x_2 x_3 + y_2^2 + iy_2(x_3 - x_2) = x_2 x_3 + y_2^2$, d'où :

② : $b = x_1(x_2 + x_3) + x_2 x_3 + y_2^2 \geqslant 0$;

③ : $c = -x_1(x_2 x_3 + y_2^2) \geqslant 0$.

On peut tenter de voir si ces conditions $a \geqslant 0, b \geqslant 0, c \geqslant 0$ suffisent à donner trois zéros de parties réelles négatives.

Si P admet trois zéros réels, x_1, x_2 et x_3, on les indexe de façon que x_1 soit le plus grand des trois.

Sinon x_1 est le zéro réel, et $x_2 + iy_2$ et $x_2 - iy_2$ les zéros complexes conjugués.

Pour un zéro réel, l'égalité $x^3 + ax^2 + bx + c = 0$ conduit à :

$$x(x^2 + b) = -(ax^2 + c).$$

Avec a, b et c positifs, on a soit $x = 0$, soit $x \neq 0$ mais alors $x^2 + b > 0$, $ax^2 + c \geqslant 0$ implique $x \leqslant 0$.

Donc a, b et c positifs donnent, si les zéros de P *sont réels, trois zéros négatifs.*

On suppose maintenant que x_1 est seul zéro réel, ($\leqslant 0$), et que $y_2 \neq 0$.

La relation ①, valable, donne :

$$a + x_1 + 2x_2 = 0.$$

Avoir $x_2 \leqslant 0$, équivaut à $a + x_1 \geqslant 0$, soit à $x_1 \geqslant -a$, et comme sur $]x_1, +\infty[$, P est à valeurs positives, et sur $]-\infty, x_1[$, à valeurs négatives, on aura $-a \leqslant x_1$ si et seulement si $P(-a) = -a^3 + a(a^2) - ba + c \leqslant 0$.

Si aux conditions a, b, c positifs on ajoute $-ba + c \leqslant 0$, les trois zéros ont leurs parties réelles négatives.

Vérifions alors, pour avoir une équivalence, que si les trois parties réelles sont négatives on a $-ba + c \leqslant 0$.

En utilisant ①, ② et ③, on a

$$\begin{aligned} c - ba &= -x_1(x_2x_3 + y_2^2) + (x_1 + x_2 + x_3)[x_1(x_2 + x_3) + x_2x_3 + y_2^2] \\ &= (x_2x_3 + y_2^2)(-x_1 + x_1 + x_2 + x_3) + x_1(x_2 + x_3)(x_1 + x_2 + x_3) \\ &= (x_2x_3 + y_2^2)(x_2 + x_3) + x_1(x_2 + x_3)(x_1 + x_2 + x_3), \\ &\qquad \geqslant 0 \qquad \leqslant 0 \quad \leqslant 0 \quad \leqslant 0 \qquad \leqslant 0 \end{aligned}$$

il me semble que cela donne bien $c - ba \leqslant 0$.

Finalement, les trois zéros de P ont une partie réelle négative si et seulement si $a \geqslant 0, b \geqslant 0, c \geqslant 0$ et $ba - c \geqslant 0$.

3.20. a) Soit d un diviseur de n, si on note $\mathscr{D}_d$ l'ensemble des entiers k de $\{1, ..., n\}$, de p.g.c.d d avec n, (donc $k \wedge n = d$), les $\mathscr{D}_d$ forment une partition de $\{1, ..., n\}$ si d décrit l'ensemble des diviseurs de n.

De plus, $k \wedge n = d$ équivaut à l'existence de $p \leqslant \frac{n}{d}$ tel que $k = pd$, p étant premier à $\frac{n}{d}$, donc :

$$\mathscr{D}_d = \left\{ pd \,;\, 1 \leqslant p \leqslant \frac{n}{d}, p \wedge \frac{n}{d} = 1 \right\}.$$

On a alors $X^n - 1 = \prod_{d|n} \left(\prod_{k \in \mathscr{D}_d} \left(X - \exp \frac{2ik\pi}{n} \right) \right)$, avec

$$\begin{aligned} \prod_{k \in \mathscr{D}_d} \left(X - \exp \frac{2ik\pi}{n} \right) &= \prod_{p \leqslant \frac{n}{d}, p \wedge \frac{n}{d} = 1} \left(X - \exp \frac{2ip\pi}{n/d} \right) \\ &= \varphi_{\frac{n}{d}}(X), \text{ avec les notations de l'énoncé,} \end{aligned}$$

donc $X^n - 1 = \prod_{d|n} \varphi_{\frac{n}{d}}(X)$.

Comme les $\frac{n}{d}$ décrivent l'ensemble des diviseurs de n si d parcourt l'ensemble des diviseurs de n, on a aussi :

$$X^n - 1 = \prod_{d/n} \varphi_d(X).$$

Prouvons, par récurrence, que les $\varphi_r(X)$ sont à coefficients entiers.

On a $\varphi_1(X) = X - 1 \in \mathbb{Z}[X]$.

Si on suppose que pour tout $r \leqslant n-1$ on a $\varphi_r(X)$ dans $\mathbb{Z}[X]$, comme $\varphi_n(X) \times \prod_{\substack{d|n \\ d \neq n}} \varphi_d(X) = X^n - 1$, on sait déjà que $\varphi_n(X)$ est unitaire, (les φ_d le sont par définition), à coefficients dans $\mathbb{Q}$ *a priori*, mais en posant, avec φ_n de degré p, et $q = n-p$, $\varphi_n(X) = X^p + a_{p-1}X^{p-1} + \ldots + a_0$, (les a_r rationnels) et $\prod_{\substack{d|n \\ d \neq n}} \varphi_d(X) = X^q + b_{q-1}X^{q-1} + \ldots + b_0$, (les b_s entiers), par produit, le coefficient de $X^{n-1} = X^{p+q-1}$ est :

$0 = a_{p-1} + b_{q-1}$ d'où $a_{p-1} = -b_{q-1}$ entier ;

puis le coefficient de X^{n-2}, (si $n \geqslant 2$) sera :

$0 = a_{p-2} + a_{p-1}b_{q-1} + b_{q-2}$, avec a_{p-1}, b_{q-1} et b_{q-2} entiers d'où a_{p-2} entier, et, par récurrence, en allant jusqu'au terme de degré q, on justifie l'appartenance des a_j à $\mathbb{Z}$, en prenant le terme de degré X^{j+q}, d'où $0 = a_j + \sum_{\substack{k+l=j+q \\ j<k\leqslant p}} a_k b_l$, avec $a_p = 1$, et $a_{j+1}, a_{j+2}, \ldots, a_{p-1}$ déjà entiers.

b) On a $\varphi_n(a) \times \prod_{\substack{d|n \\ d \neq n}} \varphi_d(a) = a^n - 1$, et par hypothèse p divise $\varphi_n(a)$, donc p divise $a^n - 1$, soit $a^n = 1$ dans le corps $\mathbb{Z}/p\mathbb{Z} = K$, donc dans le groupe multiplicatif K*, l'ordre de a divise n.

Par ailleurs, l'identité $X^n - 1 = \prod_{d|n} \varphi_d(X)$, appliquée avec $n = d'$ un diviseur strict de n, et pour $X = a$, donne : $a^{d'} - 1 = \prod_{d|d'} \varphi_d(a)$, avec les $\varphi_d(a)$ tous premiers à p, d'où $a^{d'} \neq 1$ dans $\mathbb{Z}/p\mathbb{Z}$: l'ordre de a dans K*

est n. Comme $a \not\equiv 0(p)$, par le petit Théorème de Fermat on a $a^{p-1} = 1$ dans $\mathbb{Z}/p\mathbb{Z}$, d'où $p-1$ multiple de n, soit p du type $\lambda n + 1$.

c) On suppose qu'il n'existe qu'un nombre fini de nombres premiers de la forme $\lambda n + 1$, soit b leur produit et $m = nb$.

L'identité $X^m - 1 = \varphi_m(X) \cdot \prod_{\substack{d|m \\ d \neq m}} \varphi_d(X) = \varphi_m(X)\psi_m(X)$ est obtenue avec des polynômes φ_m et ψ_m premiers entre eux car sans zéros communs, comme on l'a vu au a).

Comme φ_m, et ψ_m qui est un produit de polynômes cyclotomiques, sont dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$, il existe, (Bézout) deux polynômes U et V dans $\mathbb{Q}[X]$ tels que $1 = U(X)\varphi_m(X) + V(X)\psi_m(X)$, d'où après multiplication par un entier pour rendre entiers les coefficients de U et V, l'existence de a entier > 0, et de deux polynômes R et S de $\mathbb{Z}[X]$ cette fois, tels que :

$a = R(X)\varphi_m(X) + S(X)\psi_m(X)$, d'où *a fortiori* :

$a = R(a)\varphi_m(a) + S(a)\psi_m(a)$.

Tout diviseur premier p de $\varphi_m(a)$ divise $a^m - 1 = \varphi_m(a)\psi_m(a)$, donc est premier avec a, mais alors est aussi premier avec $\psi_m(a) = \prod_{\substack{d|m \\ d \neq m}} \varphi_d(a)$, (sinon il diviserait a), donc d'après le b) un tel p est du type $p = 1 + \lambda m = 1 + \lambda bn$: p est du type $1 + kn$, c'est donc l'un des nombres premiers dont le produit vaut b, donc p divise 1 : c'est absurde sauf si $\varphi_m(a) = 1$.

Or φ_m est un polynôme de degré $\geqslant 1$ et il existe une infinité de valeurs a et de couples (R, S) vérifiant l'égalité du type $a = R(X)\varphi_m(X) + S(X)\psi_m(X)$: on peut multiplier cette relation par un entier quelconque.

Il existe donc a entier > 0 tel que $\varphi_m(a) \neq 1$, ce qui achève de justifier, par l'absurde, l'existence d'une infinité de nombres premiers du type $\lambda n + 1$.

3.21. Déblayons le terrain. Comme on travaille sur $\mathbb{C}[X]$, on peut écrire $P^n + Q^n = R^n$ sous la forme $P^n + Q^n - R^n = 0$, et, avec λ racine $n^{\text{ième}}$ de -1 et $R_1 = \lambda R$, sous la forme symétrique $P^n + Q^n + R_1^n = 0$, le remplacement de R par R_1 ne changeant rien quant à une éventuelle proportionnalité des polynômes.

Justifions le résultat par récurrence sur le plus grand degré, en introduisant la propriété :

$\mathscr{P}_q$: $(\forall (P, Q, R) \in (\mathbb{C}_q[X])^3, P^n + Q^n = R^n \Rightarrow P, Q, R$ proportionnels) ;

$\mathscr{P}_0$ est vérifiée, les trois polynômes étant constants.

On suppose $\mathscr{P}_r$ vraie pour $0 \leqslant r < q$.

Soient $(P, Q, R) \in (\mathbb{C}_q[X])^3$, avec $P^n + Q^n = R^n$.

Comme un zéro commun, x_0, à deux des trois polynômes P, Q et R annule le troisième, après simplification par $X - x_0$, on se retrouve avec trois polynômes de $\mathbb{C}_{q-1}[X]$, qui seront proportionnels d'après $\mathscr{P}_{q-1}$, d'où P, Q et R proportionnels, et $\mathscr{P}_q$ vérifiée dans ce cas.

On suppose donc P, Q et R deux à deux premiers entre eux et, (symétrie des rôles joués), P par exemple de degré le plus élevé, q, sinon P, Q et R seraient dans $\mathbb{C}_{q-1}[X]$, avec $\mathscr{P}_{q-1}$ vraie.

On a $P^n = R^n - Q^n$, ce qui se factorise, si on introduit :

$\omega = \exp\left(2i\dfrac{\pi}{n}\right)$, en :

$$P^n = \prod_{k=0}^{n-1} (R - \omega^k Q).$$

Pour $k \neq k'$, k et k' dans $\{0, 1, ..., n-1\}$, les polynômes $R - \omega^k Q$ et $R - \omega^{k'} Q$ sont premiers entre eux, car un zéro commun, a, serait tel que $R(a) = \omega^k Q(a) = \omega^{k'} Q(a)$ avec $\omega^k \neq \omega^{k'}$, d'où $Q(a) = R(a) = 0$ ce qui est exclu, $(R \wedge Q = 1)$.

Soit a un zéro de $R - \omega^k Q$, a est zéro de P, donc $(x-a)^n$ divise P^n, et comme a n'est pas zéro des facteurs $R - \omega^{k'} Q$, pour $k' \neq k$, c'est qu'en fait $(X-a)^n$ divise $R - \omega^k Q$.

En écrivant $R - \omega^k Q = (X-a)^n R_1$, et en recommençant le raisonnement pour un zéro, b, de R_1, on aura $(X-b)^n$ qui divise R_1, et on justifie ainsi que chaque $R - \omega^k Q$ est du type $(S_k)^n$, avec $S_k \in \mathbb{C}[X]$.

En particulier, $(n \geqslant 3)$, on a les trois relations :

$$\begin{cases} R - Q = S_0^n \\ R - \omega Q = S_1^n \\ R - \omega^2 Q = S_2^n. \end{cases} \qquad \begin{vmatrix} -\omega \\ 1 \end{vmatrix}, \quad \begin{vmatrix} -1 \\ 1 \end{vmatrix}.$$

Les deux premières donnent, $(\omega \neq 1)$: $R = \dfrac{S_1^n - \omega S_0^n}{1-\omega}$ et $Q = \dfrac{S_1^n - S_0^n}{1-\omega}$, d'où, en remplaçant dans la troisième :

$(1-\omega)S_2^n = S_1^n(1-\omega^2) - \omega(1-\omega)S_0^n$, soit encore :

$S_2^n = (1+\omega)S_1^n - \omega S_0^n$, ou $((1+\omega)^{1/n}S_1)^n = (\omega^{1/n}S_0)^n + S_2^n$,

et on sent approcher l'hypothèse de récurrence car, $R - \omega^k Q$ étant de degré q au plus, avec $R - \omega^k Q = (S_k)^n$, on a chaque S_k de degré $< q$: ils sont dans $\mathbb{C}_{q-1}[X]$.

Donc les polynômes S_0, S_1 et S_2 en particulier sont proportionnels. En écrivant $S_k = \lambda_k S$ pour $k = 0, 1, 2$, avec des λ_k complexes, on obtient $R = \dfrac{\lambda_1^n - \omega\lambda_0^n}{1-\omega} S^n = \alpha S^n$, puis $Q = \dfrac{\lambda_1^n - \lambda_0^n}{1-\omega} S^n = \beta S^n$, avec α et β complexes, d'où $P^n = R^n - Q^n = (\alpha^n - \beta^n)S^{n^2}$, donc $P = \gamma S^n$, avec γ racine $n^{\text{ième}}$ de $\alpha^n - \beta^n$.

On obtient bien P, Q et R proportionnels, d'où $\mathscr{P}_q$ vérifiée.

3.22. On introduit les polynômes interpolateurs de Lagrange associés aux entiers $k, k+1, ..., k+n$, en notant, pour $0 \leqslant j \leqslant n$,

$$L_j(X) = \prod_{\substack{r=0 \\ r \neq j}}^{n} \frac{(X-(k+r))}{j-r}.$$

Le polynôme P, de degré n, se décompose dans cette base des L_j en $P = \sum_{j=0}^{n} P(k+j)L_j$, et, si on justifie que, pour tout i de $\mathbb{Z}$, $L_j(i)$ est dans $\mathbb{Z}$, les $P(k+j)$, $(0 \leqslant j \leqslant n)$ l'étant, on aura bien $P(i)$ dans $\mathbb{Z}$.

On a $L_j(i) = \prod_{\substack{r=0 \\ r \neq j}}^{n} \dfrac{(i-k-r)}{j-r}$. C'est un rationnel, de dénominateur $(-1)^{n-j}j!(n-j)!$.

Le numérateur est nul si $i-k \in \{0, 1, ..., j-1, j+1, ..., n\}$, donc dans ce cas $L_j(i) = 0$ est dans $\mathbb{Z}$; et si $i-k = j$, on a $L_j(k+j) = 1$, dans $\mathbb{Z}$ aussi.

Il reste à examiner le cas de i tel que $i-k>n$ ou $i-k<0$.

Commençons par $i>k+n$.

En posant $i-k=n+p$, $p\geqslant 1$, le numérateur de $L_j(i)$ est $(n+p)(n+p-1)...(n+p-j+1)(n+p-j-1)...p$, d'où en fait :

$$L_j(i) = (-1)^{n-j}\frac{(n+p)...(n+p-j+1)}{j!}\times\frac{(n+p-j-1)...p}{(n-j)!}$$

$$= (-1)^{n-j}C_{n+p}^{j}C_{n+p-j-1}^{n-j} \text{ qui est bien dans } \mathbb{Z}.$$

Enfin, pour $i-k<0$, si on pose $i-k=-q, q\geqslant 1$, on obtient pour numérateur de $L_j(i)$, le produit :

$$(-q)(-q-1)...(-q-j+1)(-q-j-1)...(-q-n)$$

$$= (-1)^n q(q+1)...(q+j-1)\cdot(q+j+1)...(q+n), \text{ donc}$$

$$L_j(i) = (-1)^j\frac{(q+j-1)...(q+1)q}{j!}\cdot\frac{(q+n)(q+n-1)...(q+j+1)}{(n-j)!}$$

$$= (-1)^j C_{q+j-1}^{j}C_{q+n}^{n-j}, \text{ là encore dans } \mathbb{Z}.$$

Chaque $L_j(i)$ étant dans $\mathbb{Z}$, $P(i)$ est dans $\mathbb{Z}$, pour tout i de $\mathbb{Z}$.

3.23. Pour faire apparaître $a-\frac{p}{q}$ quelque part, on peut, si a est zéro d'ordre α de P, penser à factoriser $(X-a)^\alpha$ et écrire $P(X) = (X-a)^\alpha Q(X)$, avec $Q(a)\neq 0$.

Les zéros d'un polynôme étant isolés, il existe alors $\eta>0$ tel que sur la boule fermée de centre a de rayon η, Q ne s'annule pas, et $\mathscr{B}_f(a,\eta)$ étant un compact de $\mathbb{R}$, Q est bornée sur ce compact d'où l'existence d'une constante M telle que $0<|Q(x)|\leqslant M$ sur $\mathscr{B}_f(a,\eta)$.

Soit alors $(p,q)\in\mathbb{Z}\times\mathbb{N}^*$. Si $\left|a-\frac{p}{q}\right|>\eta$, si on impose à $c>0$ cherché d'être tel que $\eta\geqslant c$, pour $q\geqslant 1$ et $r>0$ on aura $\eta\geqslant c\geqslant\frac{c}{q^r}$, d'où $\left|a-\frac{p}{q}\right|>\frac{c}{q^r}$.

Retenons la condition $r>0$, à imposer, ainsi que $c\leqslant\eta$.

Si $\left|a-\frac{p}{q}\right|\leqslant\eta$, on a $\left|\frac{p}{q}-a\right|^\alpha = \frac{\left|P\left(\frac{p}{q}\right)\right|}{\left|Q\left(\frac{p}{q}\right)\right|}$,

d'où $\left|\frac{p}{q}-a\right|^{\alpha} \geqslant \frac{1}{M}\left|P\left(\frac{p}{q}\right)\right| = \frac{1}{Mq^{d^\circ P}}\left|q^{d^\circ P}P\left(\frac{p}{q}\right)\right|$.

Mais $a \neq \frac{p}{q}$ et a est le seul zéro de P sur $\mathscr{B}_f(a, \eta)$, donc $P\left(\frac{p}{q}\right)$ est non nul, d'où, $q^{d^\circ P}P\left(\frac{p}{q}\right)$ étant entier puisque $P \in \mathbb{Z}[X]$, $\left|q^{d^\circ P}P\left(\frac{p}{q}\right)\right| \geqslant 1$, et l'inégalité :

$$\left|a-\frac{p}{q}\right|^{\alpha} \geqslant \frac{1}{Mq^{d^\circ P}} \text{ d'où l'on déduit :}$$

$$\left|a-\frac{p}{q}\right| \geqslant \frac{1}{M^{1/\alpha}q^{(d^\circ P/\alpha)}}, \text{ pour les } \frac{p}{q} \text{ dans } \mathscr{B}_f(a, \eta).$$

En posant $c = \inf\left(\eta, \frac{1}{M^{1/\alpha}}\right)$, et $r = \frac{d^\circ P}{\alpha}$, (nombre > 0), on a bien $c > 0$ et r dans $\mathbb{R}$ tels que, $\forall (p, q) \in \mathbb{Z} \times \mathbb{N}^*$, on ait $\left|\frac{p}{q}-a\right| \geqslant \frac{c}{q^r}$.

b) En fait, si on fixe q dans $\mathbb{N}^*$, l'ensemble A_q des $\frac{p}{q}$, p dans $\mathbb{Z}$, est fermé dans $\mathbb{R}$, ne contient pas a, donc $\delta = d(a, A_q)$ est une distance strictement positive, et si d est un nombre > 0 tel que $\delta > \frac{d}{q^2}$, on aura, $\forall p \in \mathbb{Z}$, $\left|a-\frac{p}{q}\right| \geqslant \frac{d}{q^2}$. On n'a pas de mal à obtenir cette infinité de couples !

c) On peut justifier le résultat par récurrence sur n, degré du polynôme P.

Si P de $\mathbb{Z}[X]$ est de degré 1, son seul zéro est dans $\mathbb{Q}$, donc le problème ne se pose pas.

Si P de $\mathbb{Z}[X]$, est de degré 2, avec a irrationnel, zéro d'ordre $> \frac{2}{2} = 1$, ici a est zéro double et P s'écrit $P(X) = b(X-a)^2$, avec $b \in \mathbb{Z}$, d'où $P(X) = bX^2 - 2abX + ba^2$ dans $\mathbb{Z}[X]$, d'où $2ab$ dans $\mathbb{Z}$ et a dans $\mathbb{Q}$: exclu.

Notons $\mathscr{P}_n$ la propriété : si P de $\mathbb{Z}[X]$, de degré n, admet a pour zéro irrationnel, a est de multiplicité $\leqslant \frac{n}{2}$.

On vient de voir que $\mathscr{P}_2$ est vérifiée. On suppose les propriétés $\mathscr{P}_k$, $2 \leqslant k \leqslant n$ vérifiées, et soit $P \in \mathbb{Z}[X]$, de degré $n+1$ ayant un zéro irrationnel a.

Procédons par l'absurde en supposant la multiplicité de a strictement supérieure à $\frac{n+1}{2}$, avec $\frac{n+1}{2} \geqslant \frac{2+1}{2} > 1$.

Les polynômes P et P' ayant a pour zéro commun dans $\mathbb{R}$, ne sont pas premiers entre eux dans $\mathbb{R}[X]$, or ils sont dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$, et *a fortiori* ils ne sont pas premiers entre eux dans $\mathbb{Q}[X]$.

Mais alors, si P est irréductible dans $\mathbb{Q}[X]$, il ne peut pas avoir de diviseur autre que 1 et P dans $\mathbb{Q}[X]$, (à une constante multiplicative près), donc il est premier avec P' dans $\mathbb{Q}$, ce qui est exclu.

En décomposant P dans $\mathbb{Q}[X]$, on peut écrire,

soit $P = P_1P_2$ avec P_1 et P_2 premiers entre-eux dans $\mathbb{Q}[X]$,

soit $P = P_1^r$ avec $P_1 \in \mathbb{Q}[X]$ et $r \geqslant 2$.

Dans le premier cas, a est zéro de P_1 par exemple, et pas de P_2, avec une multiplicité $> \frac{n+1}{2} > \frac{d^\circ P_1 + 1}{2}$, ce qui est absurde car $\mathscr{P}_{d^\circ P_1}$ est vérifiée, et P_1 de $\mathbb{Q}[X]$ est proportionnel à un polynôme de $\mathbb{Z}[X]$, le facteur de proportionnalité étant une constante.

Dans le deuxième cas, avec a zéro de multiplicité α_1 dans P_1, il l'est de multiplicité $\alpha_1 r$ dans P.

De plus, si P_1 est de degré n_1, P est de degré $n+1 = rn_1$.

On a par hypothèse $\alpha_1 r > \frac{rn_1}{2}$, d'où $\alpha_1 > \frac{n_1}{2}$, avec $n_1 \leqslant n$: comme $\mathscr{P}_{n_1}$ est supposée vraie, c'est absurde, là encore P_1 étant proportionnel, avec facteur de proportionnalité constant, à un polynôme de $\mathbb{Z}[X]$.

On a bien $\mathscr{P}_{n+1}$ vérifiée, d'où le résultat par récurrence.

3.24. On suppose le polynôme P de $\mathbb{C}[X]$, de degré $n \geqslant 2$, (pour que le polynôme dérivé ait des zéros), et, P étant scindé sur $\mathbb{C}[X]$, on l'écrit $P(X) = \lambda \prod_{k=1}^{n} (X - z_k)$, avec $z_k = x_k + iy_k$ et $y_k = \operatorname{Im}(z_k) > 0$ pour $k = 1, 2, ..., n$, les z_k ne sont donc pas forcément distincts.

On pose $Q(X) = \lambda \prod_{k=2}^{n} (X - z_k)$, donc $P(X) = (X - z_1)Q(X)$ et $P'(X) = Q(X) + (X - z_1)Q'(X)$.

Supposons que $z_0 = x_0 + iy_0$ soit un zéro de P', avec $y_0 = \text{Im}\,(z_0) \leqslant 0$.

On a $z_0 \neq z_k$, $k = 1, ..., n$, et comme $z_2, ..., z_n$ sont les zéros de Q, $Q(z_0) \neq 0$. Mais comme $Q(z_0) = -(z_0 - z_1)Q'(z_0)$, on a aussi $Q'(z_0) \neq 0$, d'où $z_0 - z_1 = -\dfrac{Q(z_0)}{Q'(z_0)}$, ou mieux, $z_0 - z_1 = -\dfrac{1}{\dfrac{Q'(z_0)}{Q(z_0)}}$, ce qui va permettre d'aller chercher la dérivée logarithmique et d'écrire :

$$z_0 = z_1 - \frac{1}{\sum_{k=2}^{n} \frac{1}{z_0 - z_k}}.$$

Comme $\text{Im}\,(z_0) \leqslant 0$ et $\text{Im}\,(z_k) > 0$, pour $k = 1, ..., n$, on a $\text{Im}\,(z_0 - z_k) < 0$, donc $\text{Im}\,\dfrac{1}{z_0 - z_k} > 0$ et aussi $\text{Im}\left(\sum_{k=2}^{n} \dfrac{1}{z_0 - z_k}\right) > 0$.

En passant à l'inverse, puis à l'opposé, on obtient une partie imaginaire strictement positive, et en ajoutant z_1, avec $\text{Im}\,(z_1) > 0$, il vient $\text{Im}\,(z_0) = \text{Im}\,(z_1) + \text{Im}\left(-\dfrac{1}{\sum_{k=2}^{n} \frac{1}{z_0 - z_k}}\right) > 0$, ce qui contredit l'hypothèse $\text{Im}\,(z_0) \leqslant 0$ du départ, qui est donc absurde. Donc les zéros de P' ont leurs parties imaginaires strictement positives.

3.25. Supposons que P admette m racines distinctes, $\lambda_1, ..., \lambda_m$ de multiplicités respectives $\alpha_1, ..., \alpha_m$, et que P – 1 en ait n, $\mu_1, ..., \mu_n$, de multiplicités $\beta_1, ..., \beta_n$. Comme P et P – 1 n'ont pas de racine commune (sinon – 1 = 0), les λ_i et les μ_j sont distincts.

De plus, P et P' ont $m' = \sum_{i=1}^{m} (\alpha_i - 1)$ racines communes, (comptées avec leurs multiplicités), soit, avec $d = \sum_{i=1}^{m} \alpha_i$ = degré de P, $m' = d - m$ racines communes.

De même P – 1 et P' ont $n' = \sum_{j=1}^{n} (\beta_j - 1) = d - n$ racines communes, (comptées avec leurs multiplicités).

Comme P et $P-1$ sont sans zéro commun, P' admet au moins $m'+n'$ zéros, comptés avec leurs multiplicités, d'où :

$d-1 =$ degré de $P' \geqslant m'+n' = d-m+d-n$, soit encore :

$d \leqslant m+n-1$.

Vu les rôles symétriques joués par P et Q, on a également m racines distinctes de Q, (les mêmes λ_i), et n de $Q-1$, donc si δ est le degré de Q, on a aussi $\delta \leqslant m+n-1$.

Mais alors, P et Q sont nuls sur les m valeurs distinctes λ_i, et valent 1 sur les n valeurs distinctes, (et distinctes des λ_i), μ_j, donc $P-Q$, de degré $m+n-1$ au plus, s'annule $m+n$ fois d'où $P-Q=0$ et $P=Q$.

3.26. On constate que A est toujours de rang $\geqslant 2$, ($a \neq 0$ car $d^\circ P = 2$, et le mineur $\begin{vmatrix} 0 & a \\ a & b \end{vmatrix} \neq 0$).

Par ailleurs A est la matrice des composantes de P, XP, Q et XQ dans la base canonique $\{X^3, X^2, X, 1\}$ de $\mathbb{C}_3[X]$.

Si A est de rang 2, avec {XP, P} famille libre, on a deux scalaires λ et μ tels que $Q = \lambda XP + \mu P$, avec $d^\circ P = d^\circ Q = 2$ donc $\lambda = 0$, et Q, proportionnel à P admet deux racines communes avec P.

Réciproquement, si P et Q ont mêmes racines, ces polynômes sont proportionnels, et si $Q = \mu P$, $XQ = \mu(XP)$ donc A est de rang 2.

Si A est de rang 3, on a des scalaires $\alpha, \beta, \gamma, \delta$ non tous nuls tels que $\alpha P + \beta XP + \gamma Q + \delta XQ = 0$, soit encore :

$$(\beta X + \alpha)P = -(\delta X + \gamma)Q.$$

Mais alors, en factorisant P sur $\mathbb{C}[X]$, on a soit deux racines distinctes pour P, et l'une annule Q, soit une racine double λ pour P, mais $(X-\lambda)^2$ divise $-(\delta X+\gamma)Q$, donc λ annule Q : dans tous les cas P et Q ont au moins une racine commune, et une seule sinon A serait de rang 2.

Si P et Q ont un et un seul zéro commun λ. On peut écrire $P = a(X-\lambda)(X-\mu)$ et $Q = a'(X-\lambda)(X-\mu')$ avec $\mu \neq \mu'$, d'où l'égalité

$$\begin{aligned} a'(X-\mu')P &= aa'(X-\lambda)(X-\mu)(X-\mu') \\ &= a(X-\mu)Q, \end{aligned}$$

soit $a'XP - a'\mu'P - aXQ + a\mu Q = 0$, avec $aa' \neq 0$ et $\mu \neq \mu'$ d'où une combinaison linéaire non triviale, nulle, entre P, XP, Q et XQ. Ces polynômes forment une famille de rang 3 au plus, et pas de rang 2 sinon P et Q auraient 2 zéros communs.

Donc rang $A = 3 \Leftrightarrow$ P et Q ont un seul zéro commun.

Il en résulte que rang A = 4 $\Leftrightarrow$ P et Q n'ont aucun zéro commun, donc rang A = 4 – nombre de racines communes.

3.27. Le polynôme P, de degré $n-1$, admet $n-1$ racines complexes. On a $(X-1)P(X) = X^n - 1$ et $P(1) \neq 0$, donc les racines de P sont les racines $n^{\text{ième}}$ de l'unité, sauf 1.

Si $n = 1$, P est constant, c'est donc $n \geqslant 2$ qu'il faut supposer.

Soit alors $\theta_k = e^{2ik\frac{\pi}{n}}$, avec $1 \leqslant k \leqslant n-1$, l'un des $n-1$ zéros de P, on aura $(\theta_k)^m = e^{2ikm\frac{\pi}{n}}$ qui reste une racine $n^{\text{ième}}$ de l'unité, et c'est 1 si et seulement si km est multiple de n, donc s'il existe p entier tel que $km = pn$. Mais alors :

1°) si m et n sont premiers entre eux, n divise k, avec $1 \leqslant k \leqslant n-1$: c'est impossible, et $m \wedge n = 1 \Rightarrow (\theta_k)^m \neq 1$;

2°) si d est le p.g.c.d de m et n, avec $d \neq 1$, en prenant $k = \frac{n}{d}$, on a $km = n \cdot \frac{m}{d}$ entier multiple de n, $\left(\frac{m}{d} \in \mathbb{N}\right)$, donc $(\theta_k)^m = 1$.

En notant $\mathscr{R}$ l'ensemble des racines de P, cet ensemble est stable par l'application $z \rightsquigarrow z^m$ si et seulement si m et n sont premiers entre-eux. Et en fait, il est invariant car dans ce cas l'application $z \rightsquigarrow z^m$ est injective sur $\mathscr{R}$, car avec $k \neq k'$, tous deux entre 1 et $n-1$, on a par exemple $k < k'$ et $\theta_k^m = \theta_{k'}^m$, si et seulement si $e^{2i(k'-k)\frac{\pi}{n}m} = 1$, soit avec $1 \leqslant k'-k < k' \leqslant n-1$, si et seulement si $(k'-k)m$ est multiple de n, ce qu'on a vu être impossible au 1°.

Donc l'ensemble des racines de P est invariant par $z \rightsquigarrow z^m$ si et seulement si m et n sont premiers entre eux.

3.28. a) La fraction rationnelle R est de classe C^∞ au voisinage de z_0, zéro d'ordre k, et, par Taylor Young à l'ordre k, on peut écrire :

$$R(z) = \frac{R^{(k)}(z_0)}{k!}(z-z_0)^k(1+\varepsilon(z)), \text{ avec } \lim_{z \to z_0} \varepsilon(z) = 0.$$

Pour mettre en évidence la partie imaginaire de $R(z)$ lorsque z décrit le cercle de centre z_0 et de rayon r, on va tout écrire à l'aide des modules et arguments.

Posons $\dfrac{R^{(k)}(z_0)}{k!} = \rho e^{i\alpha}$, $\rho > 0$, puis $z - z_0 = re^{i\theta}$, (ce sera θ qui varie), et $1 + \varepsilon(z) = a(z)e^{i\varphi(z)}$, avec $a(z) > 0$, et, comme $\lim\limits_{z \to z_0} (1 + \varepsilon(z)) = 1$, on a $\lim\limits_{z \to z_0} a(z) = 1$ et $\lim\limits_{z \to z_0} \varphi(z) = 0$: on impose à $r = |z - z_0|$ d'être assez petit pour que l'argument, $\varphi(z)$, de $1 + \varepsilon(z)$ reste dans $\left[-\frac{\pi}{4}, \frac{\pi}{4}\right]$, $\left(\text{disons } \exists r_0 > 0 \text{ tel que } 0 < r \leqslant r_0 \Rightarrow |\varphi(z)| \leqslant \frac{\pi}{4}\right)$.

Alors l'argument de $R(z)$ sera $k\theta + \alpha + \varphi(z)$, et la partie imaginaire de $R(z)$ est du signe de $\sin(k\theta + \alpha + \varphi(z))$.

Posons $\theta_p = \dfrac{1}{k}\left(p\pi + \dfrac{\pi}{2} - \alpha\right)$, on aura

$$k\theta_p + \alpha + \varphi(z) = p\pi + \frac{\pi}{2} + \varphi(z),$$

avec $\dfrac{\pi}{2} + \varphi(z) \in \left[\dfrac{\pi}{4}, \dfrac{3\pi}{4}\right]$ pour $0 < |z - z_0| \leqslant r_0$.

Mais alors si p est pair le sinus de $(k\theta_p + \alpha + \varphi(z))$ est > 0, et si p est impair il est négatif, (bien sûr $z = z_0 + re^{i\theta p}$ dans l'expression $\varphi(z)$).

Pour $p = 0, 1, ..., 2k$, on obtient les bornes de $2k$ intervalles consécutifs, entre $\dfrac{1}{k}\left(\dfrac{\pi}{2} - \alpha\right)$ et $\dfrac{1}{k}\left(\dfrac{\pi}{2} - \alpha\right) + 2\pi$, intervalles tels que $\sin(\text{Arg } (R(z)))$ soit de signe contraire aux extrémités, d'où $2k$ zéros de Im $(R(z))$ sur chaque cercle de rayon $r \in]0, r_0]$, centré en z_0.

b) Avec $(\lambda, \mu) = (1, 0)$, puis $= (0, 1)$, on obtient déjà le fait que P et Q ont tous leurs zéros réels. Vu la symétrie des rôles de P et Q montrons qu'entre deux zéros consécutifs a et b, $(a < b)$ de P, Q s'annule.

Sinon $x \rightsquigarrow R(x) = \dfrac{P(x)}{Q(x)}$ est définie sur $[a, b]$, nulle en a et b, donc, (Théorème de Rolle), il existe $c \in]a, b[$ avec $R'(c) = 0$.

La fraction rationnelle S définie par $S(x) = R(x) - R(c)$ admet alors c pour zéro double : il existe donc un $r > 0$ assez petit pour que $a < c - r < c + r < b$, et que sur le cercle de centre c de rayon r,

Im $(R(z) - R(c))$ s'annule au moins quatre fois. Comme ici $R(c)$ est réel, (P et Q sont à coefficients réels), on a Im $(R(z))$ qui s'annule quatre fois : l'un des zéros, notons le z_0, n'est pas réel, et $R(z_0) = \mathrm{Re}(R(z_0)) + i\ \mathrm{Im}\,(R(z_0)) = \mathrm{Re}(R(z_0)) = \mu$ est réel, et $\dfrac{P(z_0)}{Q(z_0)} - \mu = 0$, d'où un zéro imaginaire, z_0, (non réel), du polynôme $P - \mu Q$, ce qui contredit l'hypothèse. Donc Q s'annule sur $[a, b]$.

3.29. Soit θ l'argument des deux racines, qui peuvent donc s'écrire $\rho_1 e^{i\theta}$ et $\rho_2 e^{i\theta}$, on aura $s = (\rho_1 + \rho_2)e^{i\theta}$ et $p = \rho_1\rho_2 e^{2i\theta}$ d'où $\dfrac{s^2}{p} = \dfrac{(\rho_1 + \rho_2)^2}{\rho_1\rho_2} = 4 + \dfrac{(\rho_1 - \rho_2)^2}{\rho_1\rho_2}$ et la condition $\dfrac{s^2}{p} \geqslant 4$, (en particulier $\dfrac{s^2}{p}$ est réel).

Réciproquement, si s et p sont tels que $\dfrac{s^2}{p}$ soit un réel supérieur à 4, le discriminant de $X^2 - sX + p$ s'écrit $\Delta = s^2 - 4p = p\left(\dfrac{s^2}{p} - 4\right)$.

Posons $s = ae^{i\theta}$, ($a > 0$ car $\dfrac{s^2}{p} \geqslant 4$ n'admet pas le cas $s = 0$), et $\dfrac{s^2}{p} = 4 + b^2$ avec $b \geqslant 0$.

On aura $p = \dfrac{a^2 e^{2i\theta}}{4 + b^2}$ et $\Delta = \dfrac{a^2 b^2 e^{2i\theta}}{4 + b^2}$ d'où les racines

$$s \pm (\Delta)^{1/2} = ae^{i\theta} \pm \frac{ab}{\sqrt{4 + b^2}}\, e^{i\theta}$$

$$= \frac{ae^{i\theta}}{\sqrt{4 + b^2}} (\sqrt{4 + b^2} \pm b).$$

Comme $\sqrt{4 + b^2} - b$ est un réel positif, les deux racines ont même argument θ, et pour modules respectifs $\dfrac{a}{\sqrt{4 + b^2}} (\sqrt{4 + b^2} - b)$ et $\dfrac{a}{\sqrt{4 + b^2}} (\sqrt{4 + b^2} + b)$.

La condition nécessaire et suffisante cherchée est donc $\frac{s^2}{p}$ réel supérieur ou égal à 4.

3.30. Parmi toutes les matrices de $\mathcal{M}_n(\mathbb{C})$ figurent les matrices diagonales, qui vont conduire à un calcul plus simple des A_k, que l'on étendra aux matrices diagonalisables puis quelconques.

Aussi je commence par supposer A diagonale : $A = \text{diag}(\lambda_1, ..., \lambda_n)$. On a $A_1 = A(A - (\text{trace } A)I_n) = A^2 - \sigma_1 A$, avec σ_1 somme des racines. Comme $A^2 = \text{diag}(\lambda_1^2, ..., \lambda_n^2)$, la trace de A_1 sera $\sum_{i=1}^{n} \lambda_i^2 - \sigma_1^2$, et on comprend qu'un calcul sur les fonctions symétriques des racines s'amorce.

Notons $\sigma_1, \sigma_2, ..., \sigma_n$ les fonctions symétriques élémentaires de $\lambda_1, \lambda_2, ..., \lambda_n$.

$$\text{On a } \sigma_1^2 = \left(\sum_{j=1}^{n} \lambda_j\right)^2 = \sum_{j=1}^{n} (\lambda_j)^2 + 2 \sum_{1 \leq i < j \leq n} \lambda_i \lambda_j$$

$$= \sum_{j=1}^{n} (\lambda_j)^2 + 2\sigma_2,$$

donc $\text{trace}(A_1) = \sum_{j=1}^{n} (\lambda_j)^2 - \sigma_1^2 = -2\sigma_2$, et on a :

$$A_2 = A\left(A_1 - \frac{1}{2}(\text{trace } A_1)I_n\right),$$

$$= A(A^2 - \sigma_1 A + \sigma_2 I_n).$$

On peut alors essayer de justifier, par récurrence sur k, le fait que A_k est un polynôme en A, noté $P_k(A)$, de degré $k+1$, avec :

$$\mathcal{H}_k : P_k(X) = X\left(X^k + \sum_{p=1}^{k} (-1)^p \sigma_p X^{k-p}\right),$$

et si on y parvient, on obtiendra $A_n = A\chi_A(A)$, $\chi_A(X)$ étant le polynôme caractéristique de A, d'où $\chi_A(A) = 0$, (Cayley Hamilton) et la nullité de A_n dans ce cas.

Les relations $\mathcal{H}_1$ et $\mathcal{H}_2$ sont vérifiées.

Supposons les $\mathscr{H}_p$ vérifiées jusqu'au rang k.

$$\text{Alors } A_{k+1} = A\left(A_k - \frac{1}{k+1}\,\text{trace}\,(A_k)I_n\right),$$

$$= A\left(A^{k+1} + \sum_{p=1}^{k}(-1)^p\sigma_p A^{k+1-p} - \frac{1}{k+1}(\text{trace}\,A_k)I_n\right),$$

d'après l'hypothèse de récurrence utilisée pour exprimer $A_k = P_k(A)$, et on aura $\mathscr{H}_{k+1}$ vérifiée si on justifie l'égalité :

$$-\frac{1}{k+1}\,\text{trace}\,(A_k) = (-1)^{k+1}\sigma_{k+1},$$

ce qui permettra de faire rentrer le dernier terme dans la somme.

Comme A est diagonale, ainsi que les puissances de A, la trace de A_k est facile à exprimer, par linéarité de la trace, et on veut justifier que :

$$\text{trace}\,(A_k) = \sum_{i=1}^{n}\lambda_i^{k+1} + \sum_{p=1}^{k}(-1)^p\sigma_p\left(\sum_{i=1}^{n}\lambda_i^{k+1-p}\right) = (-1)^k(k+1)\sigma_{k+1},$$

où encore que l'on a la relation notée $\mathscr{R}$:

$$\mathscr{R}\colon \sum_{i=1}^{n}\lambda_i^{k+1} = (-1)^k(k+1)\sigma_{k+1} + \sum_{p=1}^{k}(-1)^{p+1}\sigma_p\left(\sum_{i=1}^{n}\lambda_i^{k+1-p}\right).$$

Pour justifier cette relation $\mathscr{R}$, si $(\alpha_1, \ldots, \alpha_n)$ est un n.uplet d'entiers, je vais noter $\sum\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\ldots\lambda_n^{\alpha_n}$ le polynôme symétrique contenant $\lambda_1^{\alpha_1}\lambda_2^{\alpha_2}\ldots\lambda_n^{\alpha_n}$.

Par exemple, σ_p sera noté $\sum\lambda_1\ldots\lambda_p$, ou σ_1 sera noté $\sum\lambda_1$.

On a alors :

$$\sum_{j=1}^{n}\lambda_j^{k+1} = \sum\lambda_1^{k+1} = \sum\lambda_1\sum\lambda_1^k - \sum\lambda_1\lambda_2^k$$

$$= \sigma_1\sum\lambda_1^k - \left(\sum\lambda_1\lambda_2\sum\lambda_2^{k-1} - \sum\lambda_1\lambda_2\lambda_3^{k-1}\right)$$

$$= \sigma_1\sum\lambda_1^k - \sigma_2\sum\lambda_1^{k-1} + \sum\lambda_1\lambda_2\lambda_3^{k-1}.$$

Pour simplifier les notations, posons $S_k = \sum_{j=1}^{n}\lambda_j^k = \sum\lambda_1^k$ avec notre notation, on a vérifié les égalités :

$$S_{k+1} = \sigma_1 S_k - \sum \lambda_1 \lambda_2^k$$
$$= \sigma_1 S_k - \sigma_2 S_{k-1} + \sum \lambda_1 \lambda_2 \lambda_3^{k-1}.$$

Supposons justifiée l'égalité, pour $p < k$:

$$S_{k+1} = \sum_{i=1}^{p} (-1)^{i-1} \sigma_i S_{k+1-i} + (-1)^p \sum \lambda_1 \lambda_2 \dots \lambda_p \lambda_{p+1}^{k+1-p}.$$

C'est vrai pour $p = 1$ et 2.

Supposons d'abord $k - p \geqslant 2$.

On a alors, avec $\lambda_{p+1}^{k+1-p} = \lambda_{p+1} \cdot \lambda_{p+1}^{k-p}$:

$$\sum \lambda_1 \lambda_2 \dots \lambda_p \lambda_{p+1}^{k+1-p} = \sum \lambda_1 \lambda_2 \dots \lambda_{p+1} \sum \lambda_1^{k-p} - \sum \lambda_1 \dots \lambda_{p+1} \lambda_{p+2}^{k-p},$$

car si on calcule le produit :

$(\sum \lambda_1 \lambda_2 \dots \lambda_{p+1})(\sum \lambda_{p+2}^{k-p})$, en développant, on obtiendra en fait :

$\left(\sum_{1 \leqslant i_1 < i_2 < \dots < i_{p+1} \leqslant n} \lambda_{i_1} \lambda_{i_2} \dots \lambda_{i_{p+1}} \right) \left(\sum_{j=1}^{n} \lambda_j^{k-p} \right)$, et j peut être l'un des i_k, d'où des termes en $\lambda_{i_1} \dots \lambda_{i_{r-1}} (\lambda_{i_r})^{k+1-p} \lambda_{i_{r+1}} \dots \lambda_{i_{p+1}}$ termes que l'on voulait, mais il y a en trop tous ceux avec j qui n'est pas l'un des i_k, et dont la somme, si $k + 1 - p > 1$, donne l'expression symétrique notée $\sum \lambda_1 \dots \lambda_{p+1} \lambda_{p+2}^{k-p}$, ceci parce que $k - p \geqslant 2$.

Dans ce cas la formule devient :

$$S_{k+1} = \sum_{i=1}^{p} (-1)^{i-1} \sigma_i S_{k+1-i} + (-1)^p \sigma_{p+1} (S_{k-p})$$
$$+ (-1)^{p+1} \sum \lambda_1 \dots \lambda_{p+1} \lambda_{p+2}^{k-p},$$

et on a justifié la récurrence.

Par contre, si $k - p = 1$, la fin est modifiée car alors :

$(\sum \lambda_1 \dots \lambda_k)(\sum \lambda_k)$, qui représente en fait :

$\left(\sum_{1 \leqslant i_1 < \dots < i_k \leqslant n} \lambda_{i_1} \dots \lambda_{i_k} \right) \left(\sum_{j=1}^{n} \lambda_j \right)$, donne bien la somme symétrique des termes notée $\sum \lambda_1 \dots \lambda_{k-1} \lambda_k^2$, mais les termes obtenus en trop,

lorsque j ne figure pas dans $\{i_1, ..., i_k\}$ est cette fois égale à $(k+1)\sum_{1 \leq i_1 < ... < i_k < i_{k+1} \leq n} \lambda_{i_1} ... \lambda_{i_k} \lambda_{i_{k+1}}$ car j peut prendre l'une quelconque des $k+1$ valeurs du $(k+1)$.uplet.

C'est donc $(k+1)\sigma_{k+1}$ qu'il faut retrancher, et dans l'égalité :

$$S_{k+1} = \sum_{i=1}^{k-1} (-1)^{i-1} \sigma_i S_{k+1-i} + (-1)^{k-1} \sum \lambda_1 ... \lambda_{k-1} \lambda_k^2,$$ (résultat justifié jusqu'à $p = k-1$, par récurrence), on remplace $\sum \lambda_1 ... \lambda_{k-1} \lambda_k^2$ par $\sigma_k S_1 - (k+1)\sigma_{k+1}$, d'où l'égalité :

$$S_{k+1} = \sum_{i=1}^{k} (-1)^{i-1} \sigma_i S_{k+1-i} + (-1)^k (k+1)\sigma_{k+1},$$ ce qui est bien l'égalité $\mathscr{R}$ que nous voulions justifier, (enfin moi, peut-être pas vous !).

La relation $\mathscr{H}_k$ est donc justifiée par récurrence, et conduit à l'expression :

$$P_n(X) = X\left(X^n + \sum_{p=1}^{n} (-1)^p \sigma_p X^{n-p}\right) = (-1)^n X \chi_n(X),$$

avec $\chi_n(X) = \det(A - XI_n)$, polynôme caractéristique de A, annulé par A, d'où $P_n(A) = A_n = 0$, si A est diagonale.

Si maintenant A est diagonalisable, avec Q régulière et $A' = Q^{-1}AQ$ diagonale, la suite des A'_k construite à partir de $A'_0 = A'$ est la suite des $Q^{-1}A_kQ$, car la trace est conservée par passage à une matrice semblable, d'où $A'_n = 0 = Q^{-1}A_nQ$ et $A_n = 0$.

Enfin, dans $\mathscr{M}_n(\mathbb{C})$, l'ensemble $\mathscr{D}$ des matrices diagonalisables est partout dense, et par récurrence sur k, on vérifie facilement que A donne A_k est continue en A, d'où par passage à la limite le résultat pour A quelconque dans $\mathscr{M}_n(\mathbb{C})$.

CHAPITRE IV

Algèbre linéaire

Idées générales

• Voir si une propriété est stable par linéarité pour se ramener éventuellement aux bases.

• Pour des espaces de dimension finie, une inclusion et une égalité des dimensions donne l'égalité, (faux en dimension infinie).

• Pour une application linéaire de E dans F, espaces de même dimension *finie*, (injective) $\Leftrightarrow$ (surjective) $\Leftrightarrow$ (bijective). C'est faux en dimension infinie.

• La notion de sous-espace stable par un endomorphisme est importante, ainsi que l'existence d'un supplémentaire stable aussi, ce qui conduit, en dimension finie, au calcul matriciel par blocs. En particulier, lien entre hyperplans stables et noyaux des vecteurs propres de ${}^t u$.

• En ce qui concerne les valeurs propres, ne pas oublier les distinctions liées à la dimension de l'espace, avec l'existence du polynôme caractéristique en dimension finie ; puis, en dimension finie précisément, à la nature du corps car un polynôme sur un corps K n'est pas forcément scindé.

• Le calcul de A^n, pour une matrice carrée A, qui peut servir dans des séries en « puissances de A » peut se faire de plusieurs façons :

1°) en diagonalisant, si c'est possible, (exercice 4.1) ;

2°) en utilisant **Cayley Hamilton**, ou tout polynôme Q annulant A, qui conduit, en divisant X^n par Q, à un calcul facile, (voir exercice 4.3) ;

3°) pour obtenir Q annulant A, on peut mettre A sous la forme $A = B + C$ avec B et C qui commutent, (c'est vrai si l'une des matrices est celle d'une homothétie), voir 4.2. ;

4°) ne pas oublier la décomposition de **Dunford**, $A = D + N$ avec D diagonalisable et N nilpotente qui commutent, sur $\mathcal{M}_n(\mathbb{C})$, (4.9), (4.10).

Quelques résultats incontournables :

• le Théorème de la base incomplète ; (4.5),

• l'existence des supplémentaires des sous-espaces ; (4.5),

- le théorème de factorisation d'un endomorphisme ;
- le théorème des noyaux ;
- stabilité des sous-espaces propres de u par v qui commute avec u ;
- polynômes d'endomorphismes avec Bézout s'il y a du « premiers » dans l'air ;
- $n \cdot$ linéarité des déterminants par rapport aux vecteurs colonnes ou aux vecteurs lignes ; (4.6).

Ne pas oublier non plus :

- que la dimension d'un sous-espace propre sur $E \approx K^n$ est $n - \text{rang}\,(A - \lambda I_n)$, pour la matrice A ; 4.7, 4.37 ;
- que $A \in \mathcal{M}_n(K)$ est diagonalisable sur K si et seulement si son polynôme caractéristique est scindé sur K, avec, pour chaque valeur propre, une dimension du sous-espace propre égale à sa multiplicité ; 4.7, 4.38 ;
- mais aussi qu'un endomorphisme u est diagonalisable si et seulement si il annule un polynôme scindé à racines simples, (4.38) ;
- pour calculer A^n, *ou trouver le commutant de A*, si A est carrée d'ordre p, p petit, une jordanisation peut servir ; (en fait on détermine des noyaux de $(A - \lambda_j \text{id})^k$, λ_j valeur propre de A, qui doivent être stables par B qui commute avec A, voir 4.11 : il n'est même pas toujours nécessaire de vraiment jordaniser) ; voir aussi 4.12 ;
- attention au rôle symétrique des données : il se retrouve dans la conclusion, (voir 4.22).

La jordanisation, (ce qui revient, dans la décomposition de Dunford, à prendre une base bien adaptée) est souvent utile du simple fait de son existence, (voir 4.26).

Une égalité de sous-espaces vectoriels en dimension finie, c'est souvent une inclusion et des dimensions égales, (voir 4.30), je me répète, je sais, mais c'est tellement important.

Le fait de traiter des questions abstraites ne dispense pas de savoir indexer la base canonique de $\mathcal{L}(E)$, une base de E de dimension finie étant fixée, (4.37).

Quand une notion est stable par changement de base, on a tout intérêt à choisir la base la mieux adaptée, (4.38).

Il peut être très utile, en dimension 2 ou 3, d'avoir une vision géométrique des choses, (4.39).

L'intuition, cela se développe. Ainsi une matrice symétrique réelle étant diagonalisable en base orthonormée, on peut, connaissant un pre-

mier vecteur propre évident, chercher les autres dans l'hyperplan orthogonal, (voir 4.47).

Les matrices équivalentes, il est rare que l'on s'en serve, mais cela existe, (4.50).

Quand on veut diagonaliser en dimension finie, l'adjonction (ou le retrait) d'une homothétie peut souvent faciliter les choses (4.52).

La considération de la nature des éléments intervenant facilite souvent la recherche d'un exercice. Ainsi, en 4.4, si on se persuade que l'on travaille dans l'algèbre des matrices, on trouvera une solution plus courte qu'en passant dans un espace vectoriel associé et en considérant l'action des matrices sur les vecteurs.

Une redite, (mais enseigner, n'est-ce pas répéter ?) : la connaissance du cours, c'est-à-dire de la façon de l'établir et non la connaissance d'une liste de résultats, cela doit vous permettre de l'adapter et de façonner à votre tour des raisonnements pour des situations nouvelles, (voir 4.23). C'est le but d'un apprentissage bien conduit.

Énoncés

4.1. Calculer l'exponentielle de la matrice $\begin{pmatrix} 3 & 2 & -2 \\ -1 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}$.

4.2. Soit la matrice A de $\mathcal{M}_n(\mathbb{R})$, de terme général a_{ij} avec $a_{ii} = 0$ et $a_{ij} = 1$ si $i \neq j$. Montrer que A est inversible, calcul de A^{-1} et de e^A.

4.3. Soit $A = \begin{pmatrix} -2 & -1 & 2 \\ -15 & -6 & 11 \\ -14 & -6 & 11 \end{pmatrix}$, calculer A^n pour n dans $\mathbb{N}$.

4.4. Soit A et B dans $\mathcal{M}_n(\mathbb{C})$ telles qu'il existe λ dans $\mathbb{C}$ avec $\lambda AB + A + B = 0$. Montrer qu'elles commutent.

4.5. Soient E et F deux espaces vectoriels de dimension finie, G un sous-espace vectoriel de E et $L = \{u \in L(E, F) ; G \subset \text{Ker } u\}$. Montrer que L est un espace vectoriel, quelle est sa dimension.

4.6. Diagonaliser A matrice carrée d'ordre n de terme général $a_{ij} = ij^2$.

4.7. Soit

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_n \\ -1 & x & & 0 \\ & \ddots & \ddots & \\ 0 & & \ddots & x \\ & & -1 & \end{pmatrix}$$ dans $\mathcal{M}_{n+1}(\mathbb{R})$. Est-elle la matrice d'un endomorphisme injectif ; est-elle diagonalisable ?

4.8. Soit $\mathcal{H}$ un hyperplan de $\mathcal{M}_n(\mathbb{R})$, $n \geqslant 2$. Montrer que $\mathcal{H}$ contient au moins une matrice inversible.

4.9. Déterminer l'ensemble des matrices de $\mathcal{M}_n(\mathbb{C})$ telles que $e^M = I$. Quelle est l'image de $\mathcal{M}_n(\mathbb{C})$ par l'application $M \rightsquigarrow e^M$.

4.10. Soit $A \in \mathcal{M}_n(\mathbb{R})$, montrer que $\det e^A = e^{\operatorname{tr} A}$.

4.11. Commutant dans $\mathcal{M}_3(\mathbb{R})$ de $A = \begin{pmatrix} 1 & 2 & 2 \\ -1 & 1 & -1 \\ 1 & 0 & 2 \end{pmatrix}$, et calcul de e^A.

4.12. Commutant dans $\mathcal{M}_3(\mathbb{R})$ de $A = \begin{pmatrix} 7 & 5 & 1 \\ 6 & -1 & 2 \\ 6 & 1 & 3 \end{pmatrix}$. Généralisation.

4.13. Soit E un espace vectoriel de dimension finie sur un corps K, et g dans GL(E). Calculer le déterminant et la trace de l'endomorphisme $\varphi : a \rightsquigarrow gag^{-1}$, de Hom (E) dans Hom (E).

4.14. Calculer :

$$\det \begin{pmatrix} a_1+b_1 & b_1 & b_1 & & b_1 \\ b_2 & a_2+b_2 & b_2 & & b_2 \\ b_3 & b_3 & a_3+b_3 & \dots & b_3 \\ \dots & \dots & \dots & \dots & \dots \\ b_n & b_n & b_n & \dots & a_n+b_n \end{pmatrix}.$$

4.15. Calculer le déterminant des $(C_{i+j-2}^{j-1})_{1 \leqslant i,j \leqslant n+1}$.

4.16. Soit P un polynôme complexe. Existence et unicité de Q dans $\mathbb{C}[X]$ tel que $Q(0) = 0$ et $Q(X+1) - Q(X) = P(X)$.

On pose $\phi(P) = Q$, et on définit une suite $(P_n)_{n \in \mathbb{N}}$ de polynômes de $\mathbb{C}[X]$ par la donnée de $P_0 = 1$ et la récurrence $P_n = \phi(P_{n-1}) = \phi^n(P_0)$.

Montrer que les P_n forment une base de $\mathbb{C}[X]$, calcul des P_n.

4.17. Soit ϕ l'application de $\mathcal{M}_n(\mathbb{R})$ dans $\mathcal{M}_n(\mathbb{R})$ qui à une matrice A associe sa transposée. Calculer son déterminant et sa trace.

L'application ϕ est-elle diagonalisable ?

4.18. Soit $A = \begin{pmatrix} 1 & j & j^2 \\ j & j^2 & 1 \\ j^2 & 1 & j \end{pmatrix}$. Pour X dans $\mathcal{M}_3(\mathbb{C})$, on pose $\phi(X) = AXA$.

Déterminer les valeurs propres de ϕ, ainsi que son image.

4.19. Soient A et B de $\mathcal{M}_n(\mathbb{C})$, telles qu'il existe P non nulle dans $\mathcal{M}_n(\mathbb{C})$ vérifiant $AP = PB$. Montrer que A et B ont une valeur propre commune.

4.20. Soit E un espace vectoriel réel de dimension finie n et σ un endomorphisme de E tel que $\sigma^2 = -\mathrm{id}_E$.

Montrer que n est pair et qu'avec $n = 2p$, il existe une base de E dans laquelle la matrice M de σ est la matrice blocs :

$$M = \begin{pmatrix} 0 & -I_p \\ I_p & 0 \end{pmatrix}.$$

4.21. Polynôme caractéristique, dans $K = \mathbb{Z}/p\mathbb{Z}$, (avec p premier), de la matrice

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_p \\ a_p & a_1 & a_2 & \cdots & a_{p-1} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_2 \\ a_2 & \cdots & a_p & a_1 & \end{pmatrix}.$$

4.22. Soient A et B dans $\mathcal{M}_n(K)$ tels que $A + B = AB$. Montrer que $A - I_n$ est inversible.

4.23. Soit $(M_i)_{1 \leqslant i \leqslant n}$ une famille de matrices de $\mathcal{M}_n(\mathbb{C})$ nilpotentes et qui commutent deux à deux. Montrer que $\prod_{i=1}^{n} M_i = 0$. Est-ce vrai sur un corps quelconque ?

4.24. Soit E un espace vectoriel normé de dimension finie, G le groupe des automorphismes de E et a dans L(E). On pose $F_a = \{g^{-1}ag \mid g \in G\}$. Montrer que F_a est fermé si et seulement si a est diagonalisable.

4.25. Calculer le déterminant d'ordre n :

$$D_n = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-2} & x_1^{n+1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-2} & x_2^{n+1} \\ \vdots & & & & & \\ 1 & x_n & x_n^2 & & x_n^{n-2} & x_n^{n+1} \end{vmatrix}, \text{ avec } n \geqslant 2.$$

4.26. Soit u un endomorphisme nilpotent de $E \approx K^n$, de rang $n-1$. Quels sont les sous-espaces de E stables par u.

4.27. Soient p_1 et p_2 deux projecteurs de E, espace vectoriel sur un corps K, tels que $p_1 p_2 = 0$. On considère $q = p_1 + p_2 - p_2 p_1$. Montrer que q est un projecteur, dont on précisera le noyau et l'image.

4.28. Soit un K · espace vectoriel E de dimension finie, f dans $\mathscr{L}(E)$, a et b deux éléments distincts de K tels que $(f - a\mathrm{Id}_E) \circ (f - b\mathrm{Id}_E) = 0$.

a) Établir l'existence de λ et μ non nuls dans K tels que $\lambda(f - a\mathrm{Id}_E)$ et $\mu(f - b\mathrm{Id}_E)$ soient des projecteurs.

b) Montrer que $\mathrm{Im}\,(f - b\mathrm{Id}_E) = \mathrm{Ker}\,(f - a\mathrm{Id}_E)$.

c) Calculer f^n pour tout n dans $\mathbb{N}$.

d) Si $ab \neq 0$, montrer que f est dans GL(E) et calculer f^n pour tout n de $\mathbb{Z}$.

4.29. Soit $(F_j)_{j \in \mathbb{N}}$, une suite de sous-espaces vectoriels de E, espace vectoriel réel de dimension n, les F_j étant tous de dimension $p < n$. Montrer que $\bigcup_{j=0}^{+\infty} F_j \neq E$. Montrer que l'on peut trouver un sous-espace vectoriel W de E tel que, pour chaque j, $W \oplus F_j = E$.

4.30. Soient u et v deux endomorphismes de $\mathbb{R}^n$. Comparer $\mathrm{rg}(u) + \mathrm{rg}(v)$; $|\mathrm{rg}(u) - \mathrm{rg}(v)|$; $\mathrm{rg}(u+v)$.

Prouver l'équivalence :

$$(\mathrm{rg}(u+v) = \mathrm{rg}(u) + \mathrm{rg}(v)) \Leftrightarrow \begin{cases} \mathrm{Im}\, u \cap \mathrm{Im}\, v = \{0\} \\ \text{et} \\ \mathrm{Ker}\, u + \mathrm{Ker}\, v = \mathbb{R}^n. \end{cases}$$

4.31. Soit $E = \left\{ \begin{pmatrix} a & b & c \\ c & a & b \\ b & c & a \end{pmatrix} \in \mathcal{M}_3(\mathbb{R}) \right\}$. Déterminer toutes les matrices de E telles que $M^2 = I_3$. Interprétation géométrique de ces matrices.

4.32. On pose :

$$D_n(X) = \begin{vmatrix} 1+X^2 & X & 0 & & 0 \\ X & 1+X^2 & X & \dots & 0 \\ 0 & X & 1+X^2 & \dots & 0 \\ & & \ddots & & \\ 0 & 0 & 0 & & 1+X^2 \end{vmatrix}, \text{ déterminant.}$$

Montrer qu'il s'agit d'un polynôme en X, quel est son degré. Le calculer.

4.33. Soit A et B dans $\mathcal{M}_n(\mathbb{R})$ et $M = \begin{pmatrix} A & -B \\ B & A \end{pmatrix}$.

Montrer que $\det M \geqslant 0$.

4.34. Soient P, Q, R et S dans $M_n(\mathbb{C})$. Calculer $\det \begin{pmatrix} I_n & 0 \\ P & Q \end{pmatrix}$ et $\det \begin{pmatrix} R & 0 \\ S & I_n \end{pmatrix}$.

Soient A, B, C, D dans $M_n(\mathbb{C})$ telles que $AC = CA$. Calculer $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix}$.

4.35. Soit $(E, \| \ \|)$ un $\mathbb{R}$ espace vectoriel normé de dimension n et E^* le dual de E, muni de la norme $|||\ |||$ définie par $|||\varphi||| = \sup \{|\varphi(x)| \ ; \ \|x\| = 1\}$. On note S la sphère unité du dual.

Soit $\mathcal{B} = (a_1, \dots, a_n)$ une base fixée de E. On considère l'application $f : S^n \rightsquigarrow \mathbb{R}$ qui à $(\varphi_1, \dots, \varphi_n)$ associe le déterminant des $\varphi_j(a_i)$.

a) Montrer que f possède un maximum atteint.

b) Soit $\mathscr{C} = (\varepsilon_1, ..., \varepsilon_n)$ qui réalise le maximum de f. Montrer que $\mathscr{C}$ est une base de E^* et que $g : E^n \rightsquigarrow E^n$ définie par : $g(y_1, ..., y_n) = \left(\sum_{j=1}^{n} \varepsilon_j(a_i) y_j \right)_{1 \leqslant i \leqslant n}$, est bijective.

c) Si $(e_1, ..., e_n) = g^{-1}(a_1, ..., a_n)$, montrer que $(\varepsilon_1, ..., \varepsilon_n)$ est la base duale de $(e_1, ..., e_n)$.

d) Établir que, pour tout $(\varphi_1, ..., \varphi_n)$ de S^n, on a $f(\varphi_1, ..., \varphi_n) = \det(\varphi_j(e_i)) f(\varepsilon_1, ..., \varepsilon_n)$.

e) En admettant que, pour tout x de E, $\|x\| = \sup \{|\varphi(x)| ; \varphi \in S\}$ montrer que pour tout j, $\|e_j\| = 1$.

4.36. Soit E un espace vectoriel sur un corps K, et λ un scalaire de K.

a) Si u est une affinité, (linéaire) de rapport λ, montrer que $u^2 = (\lambda + 1)u - \lambda I$.

b) Si u de $\mathscr{L}(E)$, vérifie l'égalité $u^2 = (\lambda + 1)u - \lambda I$, et si $u \neq I$, montrer que u est diagonalisable si et seulement si $\lambda \neq 1$, et que u est alors une affinité dont on précisera les éléments.

On suppose $\lambda = 1$ et $u \neq I$. Montrer que $(u - I)^2 = 0$, puis que u, non diagonalisable, n'admet qu'un sous-espace propre n'ayant pas de sous-espace supplémentaire stable par u.

4.37. Soit E un espace vectoriel de dimension finie ; soit f dans $\mathscr{L}(E)$. On pose $F(u) = f \circ u$ pour tout u de $\mathscr{L}(E)$. Montrer que toute valeur propre de f est valeur propre de F, et comparer les dimensions des sous-espaces propres associés.

4.38. Soit $\mathscr{M}$ l'ensemble des matrices carrées réelles d'ordre n. Soit A une matrice de $\mathscr{M}$ vérifiant : $A^2 - 5A + 6I_n = 0$. On pose $F(M) = AM + MA$ pour toute matrice M de $\mathscr{M}$. Étudier les éléments propres de F.

4.39. Soit α réel. Déterminer $\lim_{n \to +\infty} \begin{pmatrix} 1 & -\dfrac{\alpha}{n} \\ \dfrac{\alpha}{n} & 1 \end{pmatrix}^n$.

4.40. Soit E un $\mathbb{C}$ espace vectoriel de dimension finie, u et v deux endomorphismes de E. Montrer que u et v ont un vecteur propre commun dans chacun des cas suivants :

a) $uv = vu$,

b) $uv - vu = \alpha u$, avec $\alpha \neq 0$,

c) $uv - vu = \alpha u + \beta v$, avec α et β non nuls.

4.41. Calculer le déterminant d'ordre n, D_n, de la matrice de terme général $a_{i,j}$ avec $a_{i,i} = a + b$, $a_{i,i+1} = ab$, $a_{i+1,i} = 1$, les autres $a_{i,j}$ étant nuls.

4.42. Calculer A^n, avec $A = \begin{pmatrix} 0 & 1 & 1 \\ -2 & 3 & 2 \\ 1 & -1 & 0 \end{pmatrix}$.

4.43. Soit U dans $\mathcal{M}_n(\mathbb{C})$, et V la matrice bloc, dans $\mathcal{M}_{2n}(\mathbb{C})$, $V = \begin{pmatrix} 0 & I_n \\ U & 0 \end{pmatrix}$.

Comparer les sous-espaces propres de U et de V. Condition nécessaire et suffisante sur U pour que V soit diagonalisable.

4.44. La matrice :

$$A = \begin{pmatrix} a & b & 0 & \dots & 0 & b \\ b & a & b & & 0 & 0 \\ 0 & b & a & \ddots & 0 & 0 \\ & \ddots & \ddots & \ddots & \ddots & \\ 0 & 0 & 0 & \ddots & a & b \\ b & 0 & 0 & & b & a \end{pmatrix}$$

est-elle inversible, (avec a et b réels) ?

4.45. Soit $A \in \mathcal{M}_n(\mathbb{R})$ et i fixé dans $\{1, \dots, n\}$. A toute matrice $X = (x_{rs})_{1 \leqslant r,s \leqslant n}$ on associe la matrice $\varphi(X)$ avec $\varphi(X) = X + S(X)A$ avec $S(X) = \sum_{j=1}^{n} x_{ij}$. Noyau et valeurs propres de φ.

4.46. Soit A dans $\mathscr{M}_n(\mathbb{R})$, la matrice de terme général a_{ij} avec $a_{ij} = 1$ lorsque $i = 1$ ou n, ou $j = 1$ ou n, et 0 sinon.

Valeurs propres, vecteurs propres. Est-elle diagonalisable ?

4.47. La matrice :

$$A = \begin{pmatrix} 0 & \dots & 0 & a_1 \\ \vdots & & \vdots & \vdots \\ 0 & & 0 & a_{n-1} \\ a_1 & \dots & a_{n-1} & a_n \end{pmatrix}$$

est-elle diagonalisable sur un corps quelconque ?

4.48. Valeurs propres et vecteurs propres de :

$$A = \begin{pmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{pmatrix}.$$

4.49. Soient a et b deux nombres complexes et M la matrice de $\mathscr{M}_n(\mathbb{C})$ de terme général m_{ij} avec $m_{ii} = 0$, pour tout i, et $m_{ij} = a$ si $i > j$, b si $i < j$.

Valeurs propres, sous-espaces propres et diagonalisation éventuelle de M.

4.50. Soit E un espace vectoriel sur un corps K commutatif de caractéristique nulle, et $p_1, \dots, p_k$ des projecteurs de E dont la somme est un projecteur. Montrer que si $i \neq j$, $p_i \circ p_j = 0$.

4.51. Soit f une application non constante de $\mathscr{M}_n(\mathbb{C})$ dans $\mathbb{C}$ telle que, pour tout couple (A, B) de matrices, on ait $f(AB) = f(A)f(B)$.

Montrer que $f(A) = 0$ si et seulement si A est non inversible.

4.52. Soit G un groupe fini et E un espace vectoriel de dimension finie sur $\mathbb{C}$. Soit f un morphisme de groupes de G dans GL(E).

Pour a dans G, on pose $\varphi(a) = \text{trace}\,(f(a))$. Montrer que $\varphi(a^{-1}) = \overline{\varphi(a)}$. L'endomorphisme $f(a)$ est-il diagonalisable ?

4.53. Soit $A = (a_{ij})_{1 \leqslant i,j \leqslant n}$, avec les relations $a_{ii} = a_{i1} = a_{1i} = 1$, pour tout i, les autres coefficients étant nuls. La matrice est-elle diagonalisable, si oui, la diagonaliser.

4.54. Soient M et N deux matrices de $\mathcal{M}_n(\mathbb{C})$.

a) On suppose que M et N commutent. Soit f dans $\mathbb{C}[X, Y]$ et γ une valeur propre de $f(M, N)$. Montrer qu'il existe α et β, valeurs propres respectivement de M et N, telles que $\gamma = f(\alpha, \beta)$.

b) On suppose qu'il existe ω, racine $q^{\text{ième}}$ de l'unité telle que $MN = \omega NM$, et que N est inversible. Montrer qu'il existe des complexes $\lambda_1, ..., \lambda_k$ tels que les valeurs propres de M soient $\lambda_1, \omega\lambda_1, \omega^2\lambda_1, ...$; $\lambda_2, \omega\lambda_2, ..., ...$ Préciser les pointillés !

4.55. Soit $(a_1, ..., a_n)$ dans $\mathbb{C}^n$ et M la matrice dont tous les termes sont nuls, à l'exception de $m_{i, n-i+1}$ qui vaut a_i.

Diagonalisation de M.

Reprendre la question dans le cas où M a au plus un terme non nul dans chaque ligne et chaque colonne.

4.56. Soit A une matrice carrée d'ordre n, à coefficients dans $\{0, 1\}$, de trace nulle, symétrique, et telle qu'il existe un entier $d \geqslant 1$, tel que A vérifie l'égalité :

$$(1)\quad A^2 + A - (d-1)I_n = J,$$

J étant la matrice de terme général constant égal à 1.

Soit U le vecteur colonne de terme général 1.

a) Montrer que $AU = dU$, en déduire que $n = d^2 + 1$.

b) Soient a et b les racines de $x^2 + x - (d-1) = 0$, montrer que le spectre de A est inclus dans $\{a, b, d\}$.

c) Montrer que d est l'un des entiers 1, 2, 3, 7, 57. Déterminer A si $d = 1$ ou $d = 2$.

4.57. Soit $A \in \mathcal{M}_n(\mathbb{R})$, de terme général a_{ij}, avec : $\forall i = 1, ..., n$, $a_{ii} = 0$ et, $\forall i \neq j$, $a_{ij} + a_{ji} = 1$. Montrer que rang $(A) \geqslant n - 1$.

4.58. Soit un corps fini K, de caractéristique différente de 2. Calculer le cardinal de l'ensemble des A de $GL_n(K)$ tels que $A^2 =$ identité.

4.59. Valeurs propres et vecteurs propres de la matrice réelle carrée d'ordre n de terme général $m_{ij} = x_i + x_j$, $x_1, x_2, ..., x_n$ étant donnés.

Solutions

4.1. Le polynôme caractéristique s'écrit :

$\chi_A(X) = X^2(3-X) + 2 - 2X - 2X = -X^3 + 3X^2 - 4X + 2$. On a $\chi_A(1) = 0$, d'où $\chi_A(X) = (X-1)(-X^2 + 2X - 2)$, de zéros simples 1 et $1 \pm i$.

La matrice est diagonalisable sur $\mathbb{C}$, on trouve pour matrice de passage $P = \begin{pmatrix} 1 & 2 & 2 \\ -1 & -1-i & -1+i \\ 0 & 1 & 1 \end{pmatrix}$ et $P^{-1}AP = \text{diag}\,(1, 1-i, 1+i)$.

On a alors $A^n = P\,\text{diag}\,(1, (1-i)^n, (1+i)^n)P^{-1}$, d'où $e^A = P\,\text{diag}\,(e, e^{1-i}, e^{1+i})P^{-1}$, ce qui, avec $P^{-1} = \frac{1}{2}\begin{pmatrix} 2 & 0 & -4 \\ i & i & 1-i \\ -i & -i & 1+i \end{pmatrix}$ conduit à :

$$e^A = e\begin{pmatrix} 1+2\sin 1 & 2\sin 1 & -2+2\cos 1-2\sin 1 \\ -1+\cos 1-\sin 1 & \cos 1-\sin 1 & 2-2\cos 1 \\ \sin 1 & \sin 1 & \cos 1-\sin 1 \end{pmatrix}.$$

4.2. Si J est la matrice carrée d'ordre n de terme général constant égal à 1, $A = J - I$. Or $J^2 = nJ$, et J et I commutent, donc :

$$\begin{aligned} A^2 &= J^2 - 2J + I = (n-2)J + I \\ &= (n-2)(J-I) + (n-2)I + I, \end{aligned}$$

d'où l'égalité $A^2 + (2-n)A = (n-1)I = A(A + (2-n)I)$.

On suppose $n \geqslant 2$, d'où en fait A inversible d'inverse :

$$A^{-1} = \frac{1}{n-1}(A + (2-n)I).$$

Quand au calcul de $e^A = e^{-I+J}$ avec $-I$ et J qui commutent, on a $e^A = e^{-I}e^J$.

Puis $e^{-I} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} I = \frac{1}{e} I$, et de $J^2 = nJ$, on tire, par récurrence, $J^k = n^{k-1}J$, pour $k \geqslant 1$, donc :

$$e^J = I + \sum_{k=1}^{\infty} \frac{n^{k-1}}{k!} J = I + \frac{1}{n}(e^n - 1)J,$$

donc $e^A = \frac{1}{e}\left(I + \frac{e^n - 1}{n} J\right) = \frac{I}{e} + \frac{e^n - 1}{ne} J$.

4.3. On trouve pour polynôme caractéristique $\chi_A(\lambda) = (1-\lambda)^3$. Comme 1 est seule valeur propre et que A n'est pas l'identité, A est non diagonalisable. Comme $\chi_A(A) = 0$, (Cayley Hamilton), en divisant X^n par $(X-1)^3$ on détermine un reste $R_n(X)$, de degré 2 au plus par l'identité :

$X^n = (X-1)^3 Q(X) + a_n X^2 + b_n X + c_n$; en dérivant 2 fois, on obtient des relations du type :

$nX^{n-1} = (X-1)^2 Q_1(X) + 2a_n X + b_n$ et :

$n(n-1)X^{n-2} = (X-1)Q_2(X) + 2a_n$,

Q_1 et Q_2 étant des polynômes qu'il importe peu de calculer car on va substituer 1 à X, d'où le système :

$$\begin{cases} 2a_n = n(n-1), \\ 2a_n + b_n = n, \\ a_n + b_n + c_n = 1, \end{cases}$$

qui donne $a_n = \frac{n(n-1)}{2}, b_n = n(2-n)$ et $c_n = \frac{n^2 - 3n + 2}{2}$, d'où

$$A^n = \frac{n(n-1)}{2} A^2 + n(2-n)A + \frac{(n-1)(n-2)}{2} I.$$

On peut remarquer que ce résultat, valable pour $n = 1$ et 2, l'est aussi pour $n = 0$ et même pour $n \in \mathbb{Z}$.

En effet l'égalité $(A-I)^3 = 0 = A^3 - 3A^2 + 3A - I$, donne encore $A(A^2 - 3A + 3I) = I$, d'où :

$$A^{-1} = A^2 - 3A + 3I = \frac{-1(-2)}{2} A^2 + (-1)(3)A + \frac{(-2)(-3)}{2} I,$$

relation vérifiée pour $n = -1$, mais plus généralement, en multipliant l'égalité $(A-I)^3 = 0$ par $(A^{-1})^3$ on obtient

$(A^{-1}-I)^3 = 0 = (A^{-1})^3 - 3(A^{-1})^2 + 3A^{-1} - I$, donc A^{-1} annule aussi le polynôme $X^3 - 1$, ce qui conduit, comme pour A^n, à l'égalité

$$(A^{-1})^n = \frac{n(n-1)}{2}(A^{-1})^2 + n(2-n)A^{-1} + \frac{(n-1)(n-2)}{2} I.$$

En multipliant par A^2, pour $n \geqslant 2$, on obtient l'égalité

$$A^{-(n-2)} = \frac{n(n-1)}{2} I + n(2-n)A + \frac{(n-1)(n-2)}{2} A^2$$

et en posant $p = -(n-2)$, d'où $n = -p+2$, on est conduit à l'égalité

$$A^p = \frac{(1-p)(-p)}{2} A^2 + (2-p)pA + \frac{(2-p)(1-p)}{2} I$$

soit encore :

$$A^p = \frac{p(p-1)}{2} A^2 + p(2-p)A + \frac{(p-1)(p-2)}{2} I$$

avec cette fois p entier négatif, et une relation valable $\forall p$ dans $\mathbb{Z}$.

4.4. Soit x un vecteur propre de B, pour la valeur propre β, on a $\lambda A(\beta x) + A(x) + \beta x = 0$ soit $(1+\lambda\beta)(A(x)) = -\beta x$.

Si $1+\lambda\beta = 0$, on aurait $-\beta x = 0$ avec $x \neq 0$ d'où $\beta = 0$ et $1+\lambda\beta = 1$: curieux non ? Donc $1+\lambda\beta \neq 0$ et $A(x) = -\dfrac{\beta}{1+\lambda\beta} x$: x est vecteur propre commun à A et B.

Comme en transposant, on a $\lambda {}^tB {}^tA + {}^tA + {}^tB = 0$, on peut dire aussi que ${}^tA$ et ${}^tB$ ont un vecteur propre commun, forme linéaire φ dans le dual E^* de $E = \mathbb{C}^n$, d'où un hyperplan $H = \operatorname{Ker}\varphi$ stable par A et B, et avec $E = H \oplus \mathbb{C}a$, des matrices semblables à A et B s'écrivant en matrices blocs :

$$A' = \left(\begin{array}{c|c} A_1 & U_1 \\ \hline 0 & \alpha_1 \end{array}\right) \text{ et } B' = \left(\begin{array}{c|c} B_1 & V_1 \\ \hline 0 & \beta_1 \end{array}\right), \text{ avec } A_1 \text{ et } B_1 \text{ dans}$$

$\mathcal{M}_{n-1}(\mathbb{C})$, α_1 et β_1 scalaires, U_1 et V_1 vecteurs colonnes dans $\mathbb{C}^{n-1}$.

L'égalité $\lambda AB + A + B = 0$, par changement de base, donne

$\lambda A'B' + A' + B' = 0$ ce qui conduit, en calculant :

$$A'B' = \left(\begin{array}{c|c} A_1B_1 & A_1V_1 + \beta_1U_1 \\ \hline 0 & \alpha_1\beta_1 \end{array}\right),$$

à la relation $\lambda A_1B_1 + A_1 + B_1 = 0$, d'où l'idée de procéder par récurrence.

Si $n = 1$, toutes les matrices d'ordre 1 commutent.

On suppose le résultat vérifié pour des matrices d'ordre $n-1$ au plus.

Pour A et B d'ordre n, vérifiant $\lambda AB + A + B = 0$, le calcul précédent conduit à A_1 et B_1 qui commutent, (hypothèse de récurrence). Comme le scalaire $\alpha_1\beta_1$ est $\beta_1\alpha_1$, on aura $A'B' = B'A'$ si on justifie l'égalité $A_1V_1 + \beta_1U_1 = B_1U_1 + \alpha_1V_1$, sachant que :

$$\begin{cases} \lambda A_1B_1 + A_1 + B_1 = 0, \\ \lambda(A_1V_1 + \beta_1U_1) + U_1 + V_1 = 0, \\ \lambda\alpha_1\beta_1 + \alpha_1 + \beta_1 = 0. \end{cases}$$

La dernière relation s'écrit $\alpha_1(1 + \lambda\beta_1) + \beta_1 = 0$ et elle prouve que $1 + \lambda\beta_1$ est non nul, sinon $\beta_1 = 0$ et alors $1 + \lambda\beta_1 = 1 \neq 0$.

Mais alors la deuxième relation donne $U_1 = -\dfrac{1}{1+\lambda\beta_1}(\lambda A_1V_1 + V_1)$, et on va justifier l'égalité cherchée sous la forme :

$B_1U_1 - \beta_1U_1 = A_1V_1 - \alpha_1V_1$. On a :

$$B_1U_1 - \beta_1U_1 = -\frac{1}{1+\lambda\beta_1}(\lambda B_1A_1V_1 + B_1V_1) + \frac{\beta_1}{1+\lambda\beta_1}(\lambda A_1V_1 + V_1),$$

$$= \frac{1}{1+\lambda\beta_1}(-\lambda B_1A_1V_1 - B_1V_1 + \beta_1\lambda A_1V_1 + \beta_1V_1),$$

avec $B_1A_1 = A_1B_1$, (hypothèse de récurrence qui s'applique), donc $-\lambda B_1A_1 = A_1 + B_1$, vu la première relation, et il reste :

$$B_1U_1 - \beta_1U_1 = \frac{1}{1+\lambda\beta_1}(A_1V_1 + \beta_1\lambda A_1V_1) + \frac{\beta_1}{1+\lambda\beta_1}V_1.$$

Comme $\dfrac{\beta_1}{1+\lambda\beta_1} = -\alpha_1$, (toujours la troisième relation), on a finalement $B_1U_1 - \beta_1U_1 = A_1V_1 - \alpha_1V_1$ et finalement A' et B' commutent, donc A et B aussi.

Et maintenant, une solution courte !

Si λ est nul, on a $A + B = 0$, donc $A = -B$ et A et B commutent dans ce cas.

Si $\lambda \neq 0$, en essayant de factoriser $\lambda AB + A + B$ sous la forme $(\lambda A + \ )\ (B + \ )$, on forme :

$$(\lambda A + I_n)(B + \lambda^{-1} I_n) = \lambda AB + A + B + \lambda^{-1} I_n$$

$$= \lambda^{-1} I_n,$$

d'où, après multiplication par λ, judicieusement effectuée :

$$(\lambda A + I_n)(\lambda B + I_n) = I_n .$$

Dans ce cas, les matrices $\lambda A + I_n$ et $\lambda B + I_n$, inverses l'une de l'autre, commutent, il en est donc de même de λA et λB, l'identité commutant avec tout. Comme $\lambda \neq 0$, on a finalement A et B qui commutent.

4.5. L'application nulle, de noyau E, contient G dans son noyau, donc elle est dans L *qui est non vide* ; et si u et v sont dans L, λ et μ dans le corps de base, pour tout x de G on a :

$$(\lambda u + \mu v)(x) = \lambda u(x) + \mu v(x) = \lambda 0 + \mu 0 = 0,$$

donc $G \subset \mathrm{Ker}\,(\lambda u + \mu v)$ et $\lambda u + \mu v$ est dans L qui est *sous-espace de* L(E, F).

Si $\dim G = p$ et $\dim E = n$, avec $\{e_1, ..., e_p\}$ base de G que l'on complète en $\mathscr{B} = \{e_1, ..., e_p\ ;\ e_{p+1}, ..., e_n\}$ base de E, on aura u dans L si et seulement si, $\forall j \leqslant p$, $u(e_j) = 0$. Si $\dim F = q$, et si $\mathscr{C} = \{\varepsilon_1, ..., \varepsilon_q\}$ est une base de F, la matrice de u de L dans les bases $\mathscr{B}$ de E et $\mathscr{C}$ de F est donc une matrice ayant ses p premières colonnes nulles, les $n - p$ dernières quelconques, d'où L de dimension $q(n-p) = (\dim F)(\dim E - \dim G)$.

Remarque. En dimension quelconque, avec H supplémentaire de G dans E, on a $(u \in L) \Leftrightarrow (u|_G = 0)$, donc u est déterminé par sa restriction à H, quelconque, d'où en fait $L \approx L(H, F)$.

4.6. En notant $L_1 = (1\ 2^2\ 3^2\ ...\ n^2)$ la première ligne (non nulle) de A, on s'aperçoit que la $i^{\text{ième}}$ ligne lui est proportionnelle : $L_i = iL_1$, donc A est de rang 1, 0 est valeur propre d'ordre $n - 1$ au moins, de sous-espace propre de dimension $n - 1$. La trace λ de la matrice étant non nulle, $(\lambda = 1 + 2^3 + 3^3 + ... + n^3)$, λ est valeur propre simple donc A est diagonalisable.

Recherche des vecteurs propres : avec $X = (x_1, ..., x_n)$, la $i^{\text{ième}}$ ligne de l'égalité $AX = 0$ est $i(x_1 + 2^2x_2 + ... + n^2x_n) = 0$, donc le noyau est l'hyperplan H d'équation $x_1 + 2^2x_2 + ... + n^2x_n = 0$ dont une base serait formée des vecteurs V_j : $(j^2, 0, ..., 0, -1, 0 ... 0)$, $(-1$ en $j^{\text{ième}}$ position), pour $j = 2, 3, ..., n$.

De même, la $i^{\text{ième}}$ ligne de $AX = (1 + 2^3 + ... + n^3)X$ est

$$ix_1 + i \cdot 2^2x_2 + ... + in^2x_n = (1 + 2^3 + ... + n^3)x_i,$$

et il est clair que le choix de $x_j = j$, pour tout j, donne

$$i(1^3 + 2^3 + ... + n^3) = (1 + 2^3 + ... + n^3)x_i = (1 + 2^3 + ... + n^3)i,$$

d'où $(1, 2, ..., n)$ pour vecteur propre.

4.7. On calcule $\det A$ en développant par rapport à la première ligne d'où, avec a_j en $(j+1)^{\text{ième}}$ colonne :

$$\det A = a_0x^n + \sum_{j=1}^{n} (-1)^{j+1+1} a_j \begin{vmatrix} -1 & x & 0 & & 0 \\ & \ddots & \ddots & & \\ 0 & & x & & \\ & & -1 & & \\ \hline & & & x & \\ & 0 & & -1 & 0 \\ & & & \ddots & \ddots \\ & & & 0 & -1 \; x \end{vmatrix}$$

(j colonnes | $n-j$ colonnes)

$$= a_0x^n + \sum_{j=1}^{n} (-1)^j(-1)^j a_j x^{n-j} = \sum_{j=0}^{n} a_j x^{n-j}.$$

En notant P ce polynôme, on aura A inversible si et seulement si x non zéro de P.

Le polynôme caractéristique $\chi_A(\lambda)$ de A s'obtient en remplaçant a_0 par $a_0 - \lambda$ et x par $x - \lambda$, donc :

$$\chi_A(\lambda) = (a_0 - \lambda)(x - \lambda)^n + a_1(x - \lambda)^{n-1} + ... + a_{n-1}(x - \lambda) + a_n.$$

Quel que soit λ réel, (ou complexe), la matrice $A - \lambda I_{n+1}$ est de rang n au moins, (mineur des n premières colonnes, n dernière lignes valant $(-1)^n$), donc un sous-espace propre éventuel est de dimension 1 au plus : on aura A diagonalisable si et seulement si χ_A n'a que des zéros simples, tous dans $\mathbb{R}$.

(*Remarque* : si $a_n = a_{n-1} = \ldots = a_{n-p} = 0, \lambda = x$ est racine multiple d'ordre $p+1$, dans ce cas A est non diagonalisable).

4.8. On note E_{ij} la matrice ayant tous ses termes nuls, sauf celui en $i^{\text{ième}}$ ligne, $j^{\text{ième}}$ colonne qui vaut 1. La famille des $E_{i,j}$, pour $1 \leqslant i \leqslant n$ et $1 \leqslant j \leqslant n$ est la base canonique de $\mathcal{M}_n(\mathbb{R})$.

Si pour tout $i \neq j$, $E_{ij} \in \mathcal{H}$, la matrice $A = \sum_{i \neq j} E_{ij}$ est dans l'hyperplan $\mathcal{H}$. Or, en notant B la matrice de terme général 1, $A = B - I_n$.

Mais B est de rang 1, (n vecteurs colonnes égaux, non nuls), de trace n, elle est diagonalisable de valeurs propres 0 d'ordre $n-1$ et n d'ordre 1, donc A a pour valeurs propres – 1, d'ordre $n-1$ et $n-1$, simple, d'où $\det A = (-1)^{n-1}(n-1) \neq 0$ car $n \geqslant 2$, et A est inversible dans $\mathcal{H}$.

S'il existe un couple (i,j) *avec* $i \neq j$, tel que $E_{ij} \notin \mathcal{H}$, on a $\mathcal{M}_n(\mathbb{R}) = \mathcal{H} \oplus \mathbb{R}E_{ij}$.

Considérons la matrice identité I_n, inversible. Si $I_n \in \mathcal{H}$, on n'a rien à dire d'autre, sinon, on décompose I_n dans cette somme directe, avec $I_n = (I_n - \lambda E_{ij}) + \lambda E_{ij}$, ($\lambda \neq 0$, mais peu importe), et la matrice $I_n - \lambda E_{ij}$ est dans $\mathcal{H}$, de déterminant 1 car elle est triangulaire, ($i \neq j$) avec des 1 sur la diagonale, donc inversible.

4.9. On sait, (Théorème de Dunford), que M de $\mathcal{M}_n(\mathbb{C})$ s'écrit, de manière unique, sous la forme $M = D + N$, avec N nilpotente et D diagonalisable, N et D commutant. De plus $I_n = I_n + 0$ est décomposée. Comme D et N commutent, on a :

$$e^M = e^{D+N} = e^D e^N, \text{ avec, si N est nilpotente d'ordre } k+1,$$

$$e^N = I_n + \sum_{p=1}^{k} \frac{N^p}{p!} = I_n + N', \text{ avec N' également nilpotente.}$$

Mais alors, $e^M = e^D + e^D N'$, et e^D, (série en D) et N', (polynôme en N) commutent, et comme N' contient N en facteur, on a $N'^{k+1} = 0$

aussi, donc $(e^{D}N')^{k+1} = e^{(k+1)D}N'^{k+1} = 0$: $e^{D}N'$ est nilpotente, e^{D} est diagonalisable, la somme valant I_n c'est que $e^{D} = I_n$ et $e^{D}N' = 0$, (unicité de la décomposition de Dunford pour I_n). Continuons la recherche en supposant la matrice D diagonale. Si $D = \text{diag}(d_1, d_2, ..., d_n)$, on a facilement

$$e^{D} = \text{diag}(e^{d_1}, e^{d_2}, ..., e^{d_n}),$$

donc $e^{D} = I_n \Leftrightarrow e^{d_k} = 1 \Leftrightarrow d_k \in 2i\pi\mathbb{Z}$, pour $k = 1, 2, ..., n$.

Puis, avec e^{D} inversible, la nullité de $e^{D}N'$ équivaut à celle de

$$N' = N\Bigg(\underbrace{I_n + \sum_{p=2}^{k} \frac{N^{p-1}}{p!}}\Bigg)$$

inversible car de déterminant 1 dans une base convenable, ou du type $I_n + N''$ avec N'' nilpotent car contenant N en facteur), donc finalement $e^{D}N' = 0 \Leftrightarrow N = 0$.

On a donc $(e^{M} = I_n) \Leftrightarrow$ (M semblable à $\text{diag}(d_1, d_2, ..., d_n)$, avec pour tout $k = 1, ..., n$, $d_k \in 2i\pi\mathbb{Z}$).

Considérons alors l'application $\phi : M \rightsquigarrow e^{M}$, de $\mathcal{M}_n(\mathbb{C})$ dans $M_n(\mathbb{C})$. Comme M et $-M$ commutent, $e^{M-M} = e^{0} = I_n = e^{M} \circ e^{-M}$, donc $e^{M} \in GL_n(\mathbb{C})$, d'où $\phi(\mathcal{M}_n(\mathbb{C})) \subset GL_n(\mathbb{C})$.

Justifions l'égalité.

Soit $A \in GL_n(\mathbb{C})$, elle est semblable à une matrice blocs diagonale,

$$A' = \begin{pmatrix} A_1 & & 0 \\ & A_2 & \\ 0 & & \ddots \\ & & & A_p \end{pmatrix}$$

, avec $A_j = \lambda_j I_n + N_j$, N_j nilpotente et les λ_j non nuls car A' est inversible.

Avec $P^{-1}AP = A'$, comme $\exp(PMP^{-1}) = P(\exp M)P^{-1}$, (calcul facile), si on résoud $\exp(M) = A'$, on aura $\exp(PMP^{-1}) = PA'P^{-1} = A$. Donc on travaille sur la forme A', et, (calcul par bloc), sur chaque bloc A_j en fait.

On aura prouvé l'égalité $\phi(\mathcal{M}_n(\mathbb{C})) = GL_n(\mathbb{C})$, si on montre que, pour $Y = \lambda I_p + N$, avec λ non nul, et N nilpotente, on peut trouver X carrée d'ordre p telle que $e^X = Y$. On peut factoriser λ non nul, et chercher X telle que $e^X = \lambda I_p(I_p + N')$ avec $N' = \frac{1}{\lambda} N$, nilpotent aussi.

Avec μ complexe tel que $e^\mu = \lambda$, (μ existe car λ est non nul) et D étant l'homothétie de rapport μ sur $\mathbb{C}^p$, on a $e^D = \lambda I_p$, et on doit résoudre $e^X = e^D \circ (I_p + N')$, soit encore $e^{-D} \circ e^X = I_p + N'$.

Comme D, homothétie, commute avec X quelconque, c'est encore $e^{-D+X} = I_p + N'$ que l'on doit résoudre.

Or, pour $|x| < 1$, (x réel), $\ln(1+x) = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{x^k}{k}$, série absolument convergente, de valuation 1, que l'on peut donc substituer à t dans le développement en série entière de $e^t = \sum_{n=0}^{+\infty} \frac{t^n}{n!}$, de rayon de convergence infinie, et en « réordonnant » par rapport aux puissances de x, l'expression $\sum_{n=0}^{+\infty} \frac{1}{n!} \left(\sum_{k=1}^{+\infty} (-1)^{k-1} \frac{x^k}{k} \right)^n$ on obtient $e^{\ln(1+x)} = 1 + x$.

Comme pour N' nilpotente $M' = \sum_{k=1}^{+\infty} (-1)^k \frac{N'^k}{k}$ est une somme finie, de r termes si N' est nilpotente d'ordre $r+1$, la matrice $e^{M'} = e^{\sum_{k=1}^{r} (-1)^{k-1} \frac{N'^k}{k}} = \prod_{k=1}^{r} e^{(-1)^{k-1} \frac{N'^k}{k}}$ devient un produit fini de r « séries entières en puissances de N' », qui commutent, donc on peut réindexer par rapport aux puissances de N' et on trouvera $I_p + N'$, les coefficients se calculant à partir de règles algébriques, et à partir des $\frac{1}{n!}$ et des $\frac{(-1)^k}{k}$: on peut donc trouver M' telle que $e^{M'} = I_p + N'$, en posant $X - D = M'$ on trouve alors X telle que $e^X = e^D(I_p + N')$ et ceci achève la justification.

4.10. *Première méthode* : qui peut le plus, peut le moins.

Si on justifie le résultat pour A dans $\mathcal{M}_n(\mathbb{C})$, il le sera pour A dans $\mathcal{M}_n(\mathbb{R})$. Dans ce cas, A est semblable à une matrice $A' = D + N$, avec D diagonale et N nilpotente, D et N commutant. Comme alors e^A est semblable à $e^{A'}$, on aura $\det e^A = \det e^{A'}$, et aussi $\operatorname{trace} A = \operatorname{trace} A'$, (notions stables par passage aux matrices semblables). On traite donc l'exercice en partant de $A = D + N$, (au lieu de A'), avec $D = \operatorname{diag}(d_1, ..., d_n)$.

On a alors $e^A = e^D e^N$ avec $e^D = \operatorname{diag}(e^{d_1}, ..., e^{d_n})$, et $e^N = I_n + N + \frac{N^2}{2!} + ... + \frac{N^k}{k!}$ si N est nilpotente d'ordre $k+1$.

Mais N, nilpotente, se trigonalise en N' de diagonale nulle, donc e^N est semblable à une matrice triangulaire n'ayant que des 1 sur la diagonale, d'où $\det e^N = 1$.

On obtient $\det(e^A) = \det(e^D)\det(e^N)$,

$$= \prod_{j=1}^{n} e^{d_j} = e^{\sum_{j=1}^{n} d_j} = e^{\operatorname{trace} A}.$$

Deuxième méthode : vérifier la propriété sur une forme de la matrice plus commode sans aller chercher l'artillerie lourde.

Les matrices réelles sont trigonalisables dans $\mathcal{M}_n(\mathbb{C})$: $\exists P$ dans $GL_n(\mathbb{C})$ telle que $P^{-1}AP = T$ soit triangulaire, avec sur la diagonale, les valeurs propres distinctes ou non, $d_1, ..., d_n$, de A.

On a $e^T = \sum_{k=0}^{+\infty} \frac{1}{k!} P^{-1}A^kP$,

car $T^k = P^{-1}A(PP^{-1})A \ldots AP = P^{-1}A^kP$; soit encore $e^T = P^{-1}e^AP$: e^T et e^A, semblables, ont même déterminant.

Or T^k est triangulaire, de diagonale $d_1^k, ..., d_n^k$, donc on vérifie facilement que e^T est triangulaire, de diagonale $e^{d_1}, ..., e^{d_n}$, d'où $\det e^A = \det e^T = e^{d_1} \ldots e^{d_n} = e^{\operatorname{trace} A}$.

4.11. Le polynôme caractéristique de A est :

$$P(\lambda) = \begin{vmatrix} 1-\lambda & 2 & 2 \\ -1 & 1-\lambda & -1 \\ 1 & 0 & 2-\lambda \end{vmatrix}$$

$$= (1-\lambda)^2(2-\lambda) - 2 - 2(1-\lambda) + 2(2-\lambda) = (1-\lambda)^2(2-\lambda),$$

(on développe par la règle de Sarrus).

La matrice $A - I_3 = \begin{pmatrix} 0 & 2 & 2 \\ -1 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix}$ est de rang 2, le sous-espace propre est de dimension 1, A n'est pas diagonalisable. Elle est trigonalisable sur $\mathbb{C}$, et même ici sur $\mathbb{R}$, car si on prend deux vecteurs propres ε_1 et ε_2 pour les valeurs propres 2, (simple) et 1 (double), n'importe quel vecteur ε_3 tel que $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\} = \mathscr{C}$ soit base de $\mathbb{R}^3$, sera une base de trigonalisation.

Recherche de ε_1 : on résoud le système :

$$\begin{cases} -x + 2y + 2z = 0 \\ -x - y - z = 0, \text{ de solution } (0, 1, -1). \end{cases}$$

Recherche de ε_2 : on résoud :

$$\begin{cases} 2y + 2z = 0 \\ -x - z = 0, \text{ de solution } (1, 1, -1). \end{cases}$$

Cherchons $\varepsilon_3 = (x, y, z)$ tel que dans la base $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ la matrice de l'endomorphisme a, de matrice A dans la base $\mathscr{B} = (e_1, e_2, e_3)$ initiale soit $A' = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, (on jordanise sans le dire).

On traduit $a(\varepsilon_3) = \varepsilon_2 + \varepsilon_3$ en revenant dans la base $\mathscr{B}$. C'est :

$$A\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & 2 & 2 \\ -1 & 1 & -1 \\ 1 & 0 & 2 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} + \begin{pmatrix} x \\ y \\ z \end{pmatrix},$$

soit encore un système à résoudre :

$$\begin{cases} 2y + 2z = 1 \\ -x - z = 1 \\ x + z = -1, \end{cases}$$

système de rang deux, de solution $x = -1-z, y = \frac{1}{2}-z$, z quelconque, choisi cependant tel que $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ soit une base : $z = -1$ convient et donne pour matrice de passage $P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 3/2 \\ -1 & -1 & -1 \end{pmatrix}$. On a alors $P^{-1}AP = A' = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Une matrice B commute avec A si et seulement si $B' = P^{-1}BP$ commute avec A'.

On a Vect $(\varepsilon_1) = \text{Ker}\,(A' - 2I_3)$: cet espace doit être stable par B' qui commute avec A' donc avec $A' - 2I_3$; il en est de même de Vect $(\varepsilon_2) = \text{Ker}\,(A' - I_3)$, et aussi de Vect $(\varepsilon_2, \varepsilon_3) = \text{Ker}\,(A' - I_3)^2$, donc la matrice B' doit être du type :

$$B' = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & \gamma \\ 0 & 0 & \delta \end{pmatrix}.$$

La relation $A'B' = B'A'$ équivaut alors, (calcul par blocs), à :

$$\begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \beta & \beta+\gamma \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \beta & \gamma+\delta \\ 0 & \delta \end{pmatrix}$$

soit à $\beta = \delta$, donc $B' = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & \gamma \\ 0 & 0 & \beta \end{pmatrix}$.

Mais alors, le sous-espace vectoriel F, des matrices de $\mathcal{M}_3(\mathbb{R})$, qui commute avec A, est de dimension trois.

C'est l'ensemble des $PB'P^{-1}$. Comme il contient par ailleurs I_3, A, et A^2, matrices indépendantes, (car si on a des scalaires u, v, w, réels, tels que $uA^2 + vA + wI_3 = 0$, avec 1 et 2 valeurs propres de A, on aurait 1 et 2 zéros du polynôme $R(x) = ux^2 + vx + w$, qui serait scindé à racines simples, et A serait diagonalisable), c'est que $F = \text{Vect}\,(I, A, A^2)$.

En fait la détermination précise de P était inutile pour trouver le commutant sous cette forme.

Par contre, elle servira pour le calcul de e^{A}. Un calcul immédiat donne

$$A'^{n} = \begin{pmatrix} 2^n & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}, \text{ donc } e^{A} = Pe^{A'}P^{-1},$$

soit $e^{A} = P\begin{pmatrix} e^2 & 0 & 0 \\ 0 & e & e \\ 0 & 0 & e \end{pmatrix}P^{-1}$, car $\sum_{n=0}^{+\infty} \frac{n \cdot 1}{n!} = \sum_{n=1}^{+\infty} \frac{1}{(n-1)!} = e$. Libre à vous d'achever les calculs avec la détermination de P^{-1}.

4.12. Le polynôme caractéristique de A est, sauf erreur, $\chi_A(\lambda) = -\lambda^3 + 9\lambda^2 + 27\lambda - 53$: il n'a rien de remarquable.

Mais $\lim_{\lambda \to -\infty} \chi_A(\lambda) = +\infty, \chi_A(0) = -53$; $\chi_A(3) = 82$ et $\lim_{\lambda \to +\infty} \chi_A(\lambda) = -\infty$: ce polynôme admet trois racines réelles distinctes, $\lambda_1, \lambda_2, \lambda_3$ donc A est diagonalisable.

Soit $\mathscr{B} = \{e_1, e_2, e_3\}$ une base de vecteurs propres associés à ces valeurs propres distinctes.

Chaque droite $D_i = \text{Vect}(e_i) = \text{Ker}(A - \lambda_i I_3)$ est alors stable par B dans le commutant de A, donc dans la base $\mathscr{B}$ des e_i, une matrice du commutant est diagonale. Ce commutant, $\mathscr{E}$ est donc un sous-espace de dimension 3 au plus, de $\mathscr{M}_3(\mathbb{R})$. Or il contient I_3, A et A^2, indépendantes car l'existence de u, v, w réels non nuls tels que $uA^2 + vA + wI_3 = 0$ donnerait un polynôme $P(x) = ux^2 + vx + w$ annulé par les trois valeurs propres distinctes de A : c'est absurde.

Finalement le commutant est $\mathscr{E} = \{\alpha I_3 + \beta A + \gamma A^2 ; (\alpha, \beta, \gamma) \in \mathbb{R}^3\}$.

4.13. On utilise une base fixée $\mathscr{B}$ de E, et on identifie alors Hom (E) et l'espace vectoriel $\mathscr{M}_n(K)$ des matrices carrées d'ordre n sur K, rapporté à la base $\mathscr{C}$ des matrices $E_{i,j}$ de termes tous nuls, sauf celui de la $i^{\text{ième}}$ ligne, $j^{\text{ième}}$ colonne qui vaut 1.

Par ailleurs, on note γ_{rs} le terme général de la matrice de g dans la base $\mathscr{B}$ de E, (ou bien, on identifie g et la matrice des γ_{rs}).

Soient $\varphi_1 : a \rightsquigarrow ga$ et $\varphi_2 : b \rightsquigarrow bg^{-1}$, applications linéaires de Hom (E) dans Hom (E), on a : $\varphi = \varphi_1 \circ \varphi_2 = \varphi_2 \circ \varphi_1$.

On a :

$$\varphi_1(E_{ij}) = (\gamma_{rs}) \underbrace{\begin{pmatrix} & 0 & \\ 0 & \vdots & 0 \\ & 0 & \\ & 1 & \\ & 0 & \\ & \vdots & \\ & 0 & \end{pmatrix}}_{j^{\text{ième}} \text{ colonne}} = \underbrace{\begin{pmatrix} & \gamma_{1i} & \\ 0 & \gamma_{2i} & 0 \\ & \vdots & \\ & \gamma_{ni} & \end{pmatrix}}_{j^{\text{ième}} \text{ colonne}};$$

(1 figurant en $i^{\text{ième}}$ ligne), soit encore :

$$\varphi_1(E_{ij}) = \sum_{k=1}^{n} \gamma_{ki} E_{kj}.$$

La matrice de φ_1 dans la base $\mathscr{C}$, ordonnée dans l'ordre : $E_{11}, \ldots, E_{n1}$; $E_{12}, \ldots, E_{n2}$; ... ; $E_{1n}, \ldots, E_{nn}$; est la matrice bloc :

$\varphi_1(E_{11}) \ldots \varphi_1(E_{n1}) \ldots\ldots\ldots\ldots \varphi_1(E_{1n}) \ldots \varphi_1(E_{nn})$

$$\begin{pmatrix} \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1n} \\ \vdots & (g) & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nn} \end{pmatrix} & & \\ & \ddots & \\ & & \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1n} \\ \vdots & (g) & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nn} \end{pmatrix} \end{pmatrix} \begin{matrix} E_{11} \\ \vdots \\ E_{n1} \\ \\ \\ \\ E_{1n} \\ \vdots \\ E_{nn} \end{matrix},$$

matrice d'ordre n^2, ayant n fois le bloc (g) sur la diagonale.

De la même façon, et en notant γ'_{rs} le terme général de g^{-1}, (dans la base $\mathscr{B}$ de départ), on aura :

$$\varphi_2(E_{ij}) = \begin{pmatrix} 0 \\ 0\cdots 0\ 1\ 0\cdots 0 \\ 0 \end{pmatrix} (\gamma'_{rs}) = \begin{pmatrix} 0 \\ \gamma'_{j1} \text{ - - - - - } \gamma'_{jn} \\ 0 \end{pmatrix} \begin{matrix} i^{\text{ième}} \text{ ligne} \\ \\ j^{\text{ième}} \text{ colonne} \end{matrix}$$

donc $\varphi_2(E_{ij}) = \sum_{k=1}^{n} \gamma'_{jk} E_{ik}$.

On indexe cette fois la base $\mathscr{C}$ dans l'ordre :

$E_{11}, ..., E_{1n}$; $E_{21}, ..., E_{2n}$; ..... ; $E_{n1}, ..., E_{nn}$;

pour obtenir la matrice de φ_2 qui sera bloc diagonale avec n fois le bloc g^{-1} sur la diagonale.

Comme le déterminant est indépendant de la base, (la trace aussi), on a $\det \varphi_1 = (\det g)^n$, et $\det(\varphi_2) = (\det g^{-1})^n$,

d'où $\det \varphi = \det(\varphi_1 \circ \varphi_2) = (\det g)^n \cdot (1/\det g)^n = 1$.

Quant à la trace, morphisme additif, la décomposition $\varphi = \varphi_1 \circ \varphi_2$ est peu utile, mais les calculs intermédiaires vont servir.

$$\text{On a } \varphi(E_{ij}) = \varphi_2(\varphi_1(E_{ij})) = \varphi_2\left(\sum_{k=1}^{n} \gamma_{ki} E_{kj}\right)$$

$$= \sum_{k=1}^{n} \gamma_{ki} \varphi_2(E_{kj}) = \sum_{k=1}^{n} \gamma_{ki} \left(\sum_{r=1}^{n} \gamma'_{jr} E_{kr}\right).$$

Le coefficient de E_{ij} est donc $\gamma_{ii}\gamma'_{jj}$ et la trace de φ devient

$$\sum_{i=1}^{n}\sum_{j=1}^{n} \gamma_{ii}\gamma'_{jj} = \left(\sum_{i=1}^{n} \gamma_{ii}\right)\left(\sum_{j=1}^{n} \gamma'_{jj}\right)$$

$$= (\text{trace } g)(\text{trace } g^{-1}).$$

4.14. Une belle et facile application de l'aspect n · linéaire alterné du déterminant.

En notant B_i la ligne $(b_i, ..., b_i)$, (b_i partout),

et A_i la ligne $(0, ... 0, a_i, 0, ..., 0)$, ($a_i$ en $i^{\text{ième}}$ position), on a la matrice des n lignes $L_1, ..., L_n$ avec $L_i = A_i + B_i$, et

$B_i = b_i(1, 1, ..., 1)$ en fait, donc les B_i sont proportionnelles. Mais alors, en considérant le déterminant comme fonction n linéaire alternée des vecteurs lignes, on a :

$$D = \det(A_1 + B_1, A_2 + B_2, ..., A_n + B_n),$$

qui est une somme de 2^n déterminants obtenus en choisissant, en $i^{\text{ième}}$ place, A_i ou B_i. Si, pour deux indices i et j distincts, on choisit B_i et B_j, lignes proportionnelles, le déterminant obtenu est nul. Il ne reste donc que $n+1$ termes, $\det(A_1, A_2, ..., A_n) = a_1 a_2 ... a_n$, et les n termes $\det(A_1, ..., A_{i-1}, B_i, A_{i+1}, ..., A_n) = a_1 ... a_{i-1} b_i a_{i+1} ... a_n$, d'où

$$D = a_1 ... a_n + \sum_{i=1}^{n} a_1 ... a_{i-1} b_i a_{i+1} ... a_n.$$

4.15. La première ligne, $(i = 1)$, a pour terme général $1 = C_{j-1}^{j-1}$, ainsi que la première colonne.

Pour $i \geqslant 2$, on remplace la $i^{\text{ième}}$ ligne, L_i, par $L_i - L_{i-1} = L'_i$, en commençant par L'_n, puis L'_{n-1}, ...

La première colonne devient $(1, 0, ..., 0)$, et pour $i \geqslant 2, j \geqslant 2$, le terme général de la ligne L'_i devient :

$$C_{i-1+j-1}^{j-1} - C_{i-2+j-1}^{j-1} = C_{i-2+j-1}^{j-2}, \text{ (d'après le triangle de Pascal).}$$

On note $C'_1, ..., C'_n$ les colonnes de la matrice obtenue, que l'on remplace, j variant de n à 2, par $C''_j = C'_j - C'_{j-1}$, et on garde $C''_1 = C'_1$. On obtient pour $j \geqslant 2$:

$$C''_j = \begin{pmatrix} 1 \\ j-1 \\ C_j^{j-2} \\ \vdots \\ C_{i-2+j-1}^{j-2} \\ \vdots \\ C_{n+j-2}^{j-2} \end{pmatrix} - \begin{pmatrix} 1 \\ j-2 \\ C_{j-1}^{j-3} \\ \vdots \\ C_{i-2+j-2}^{j-3} \\ \vdots \\ C_{n+j-3}^{j-3} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ C_{j-1}^{j-2} \\ \vdots \\ C_{i-2+j-2}^{j-2} \\ \vdots \\ C_{n+j-3}^{j-2} \end{pmatrix},$$

et le déterminant obtenu est encore celui de la matrice :

$$\mathscr{M} = \begin{pmatrix} 1 & 0 & 0 & & & 0 \\ 0 & 1 & 1 & \cdots & \cdots & 1 \\ 0 & 1 & 2 & \cdots & \cdots & n-1 \\ \vdots & \vdots & & & & \\ & & & C_{i-2+j-2}^{j-2} & \cdots & \leftarrow i^{\text{ième}} \text{ ligne, } i \geqslant 2 \\ & & & \vdots & & \\ 0 & 1 & n-1 & & & C_{2n-2}^{n-1} \end{pmatrix}$$

$j^{\text{ième}}$ colonne, $j \geqslant 2$.

En posant $i-1 = i'$, et $j-1 = j'$, on a $1 \leqslant i', j' \leqslant n$, et en supprimant la 1re ligne et la 1re colonne de $\mathscr{M}$, on obtient $\mathscr{M}'$, matrice carrée d'ordre n cette fois, de même déterminant que le déterminant cherché, de terme général $C_{i'+j'-2}^{j'-1}$.

Par récurrence descendante, on obtient, ($n = 1$ dans la formule initiale) :

$$D = \begin{vmatrix} 1 & 1 \\ 1 & 2 \end{vmatrix} = 1.$$

4.16. Les conditions posées sont affines en Q. Dans ces conditions, une existence avec unicité est souvent obtenue parce qu'il y a une application linéaire bijective quelque part.

Si Q est de degré k, de coefficient directeur a, le polynôme $Q(X+1) - Q(X)$ est de degré $k-1$, (si $k \geqslant 1$), de coefficient directeur ka. Donc si P est de degré n, Q doit être de degré $n+1$.

On considère donc $E_n = \mathbb{C}_n[X]$, et l'application θ de $\mathbb{C}_{n+1}[X]$ dans $\mathbb{C} \times \mathbb{C}_n[X]$, définie par :

$$\theta(Q) = (Q(0), Q(X+1) - Q(X)).$$

Cette application est linéaire, injective car si $\theta(Q) = 0$, le polynôme Q est périodique de période 1, nul en 0, donc nul sur tout k de $\mathbb{Z}$: il est identiquement nul.

Comme $\mathbb{C}_{n+1}[X]$ et $\mathbb{C} \times \mathbb{C}_n[X]$ sont tous les deux de dimension $n+2$, θ est donc bijective, et à chaque P de $\mathbb{C}_n[X]$, on associe un et un seul Q tel que $\theta(Q) = (0, P)$ c'est-à-dire répondant à la question.

Comme on a vu que le degré de Q est 1 + degré de P, partant de $P_0 = 1$ de degré nul, les $P_n = \phi^n(P_0)$ sont de degrés échelonnés, donc forment une base de $\mathbb{C}[X]$.

Il reste le calcul des P_n.

On a $P_1 = \phi(P_0)$, nul en 0 et de degré 1, donc du type :

$P_1(X) = kX$, k tel que $k(X+1) - kX = k = P_0 = 1$, d'où : $P_1(X) = X$.

Puis, $P_2(X) = \phi(P_1)(X)$ est aussi nul en 0, de degré 2, et on a :

$P_2(X+1) - P_2(X) = P_1(X) = X$, donc $P_2(1) - P_2(0) = 0$, d'où : $P_2(1) = 0$. Donc P_2 est du type $kX(X-1)$, k tel que :

$k(X+1)X - kX(X-1) = P_1(X) = X$, soit encore :

$kX(X+1-X+1) = X \Leftrightarrow 2k = 1$, soit $k = \frac{1}{2}$ et :

$P_2(X) = \frac{X(X-1)}{2!}$.

On vérifie alors facilement, que $P_k(X) = \frac{X(X-1)\ldots(X-k+1)}{k!}$ convient, (nul en 0 et $P_k(X+1) - P_k(X) = P_{k-1}(X)$) : c'est *la* solution.

4.17. On a $\phi \circ \phi(A) = A$, donc sur l'espace vectoriel $E = \mathcal{M}_n(\mathbb{R})$, ϕ annule le polynôme scindé à racines simples $X^2 - 1$, d'où ϕ diagonalisable, avec pour seules valeurs propres possibles 1 et - 1.

Or E est somme directe des sous-espaces F et G, avec F, ensemble des matrices symétriques, et G ensemble des matrices antisymétriques, car A de E s'écrit $A = \frac{A + {}^tA}{2} + \frac{A - {}^tA}{2}$.

Sur F, espace de dimension $n + \frac{n^2 - n}{2} = \frac{n(n+1)}{2}$, ϕ induit l'identité, et sur G, de dimension $\frac{n(n-1)}{2}$, ϕ induit $-\mathrm{id}_G$ d'où 1 valeur propre d'ordre $\frac{n(n+1)}{2}$, de sous-espace propre F, et - 1 valeur propre d'ordre $\frac{n(n-1)}{2}$, de sous-espace propre G.

On a trace $\phi = \frac{n(n+1)}{2} - \frac{n(n-1)}{2} = n$, et :

$$\det \phi = (-1)^{\frac{n(n-1)}{2}}$$

4.18. Les trois colonnes de A sont proportionnelles, donc rang (A) $\leqslant 1$, et $A \neq 0$, d'où rang (A) = 1, donc 0 est valeur propre d'ordre 2 au moins, (dimension du sous-espace propre). Comme A est de trace nulle, la troisième valeur propre est encore 0, valeur propre triple.

Dans les inclusions des noyaux des puissances de A, on a dim Ker A = 2, Ker A $\subset$ Ker A^2, sans égalité sinon la suite est stationnaire, or $A^3 = 0$, (Cayley Hamilton, ou A triangularisable avec des 0 sur la diagonale). Donc dim (Ker A^2) > 2 : cette dimension est 3, d'où $A^2 = 0$. Mais alors $\phi^2(X) = A(AXA)A = 0$, et ϕ n'admet que 0 comme valeur propre. De plus Im $\phi \subset$ Ker ϕ.

Pour chercher l'image on peut travailler sur des « formes semblables » des matrices, par un changement de base rendant A sympathique, (penser à une jordanisation de A qui est semblable à $A' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$: il ne reste pas grand chose).

Sans compliquer tout : on se place sur $\mathbb{C}^3$ canonique. Soit a endomorphisme de matrice A dans la base canonique de $\mathbb{C}^3$. On choisit $e_3 \notin$ Ker a, comme $a^2 = 0, e_2 = a(e_3)$ est non nul dans Ker a, et il existe e_1 qui complète $\{e_2\}$ en une base de Ker a. Dans la base $\{e_1, e_2, e_3\}$ la matrice de a est la forme A' jordanisée.

Si P est la matrice de passage, on a $P^{-1}AP = A'$, donc pour X de $\mathcal{M}_3(\mathbb{C})$ on aura :

$$\begin{aligned} \phi(X) = AXA &= (PA'P^{-1})(X)(PA'P^{-1}) \\ &= P(A'X'A')P^{-1}, \end{aligned}$$

avec $X' = P^{-1}XP$ qui décrit $\mathcal{M}_3(\mathbb{C})$ quand X varie dans $\mathcal{M}_3(\mathbb{C})$.

$$\text{Puis } A'X'A' = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x & y & z \\ x' & y' & z' \\ x'' & y'' & z'' \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & y \\ 0 & 0 & y' \\ 0 & 0 & y'' \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & y'' \\ 0 & 0 & 0 \end{pmatrix}$$

$$= y''A',$$

d'où $\phi(X) = y''PA'P^{-1} = y''A$ et ϕ est d'image $\mathbb{C}A$.

Remarque. Pour le noyau, en notant $(E_{uv})_{1 \leqslant u, v \leqslant 3}$ la base canonique de $\mathcal{M}_3(\mathbb{C})$, on peut constater que $\phi(E_{11}) = A$.

En calculant α_{uv} tel que $\phi(E_{uv}) = \alpha_{uv}A$, pour $(u, v) \neq (1, 1)$, on aura $\phi(\alpha_{uv}E_{11} - E_{uv}) = 0$, d'où 8 vecteurs indépendants du noyau.

4.19. Dire que A et B sont sans valeur propre commune revient à dire que leurs polynômes caractéristiques sont premiers entre eux, donc, (merci Bézout), qu'il existe U et V dans $\mathbb{C}[X]$ tels que : $U\chi_A + V\chi_B = 1$.

Mais alors, par Cayley Hamilton, on aurait :

$$U(A) \circ \chi_A(A) + V(A) \circ \chi_B(A) = V(A) \circ \chi_B(A) = I_n \text{ et :}$$

$$U(B) \circ \chi_A(B) + V(B) \circ \chi_B(B) = U(B) \circ \chi_A(B) = I_n,$$

(car $\chi_A(A) = \chi_B(B) = 0$), d'où $\chi_A(B)$ et $\chi_B(A)$ inversibles.

Puis, l'égalité $AP = PB$, donne, par récurrence, $A^kP = PB^k$, pour tout k de $\mathbb{N}$, (si $k = 0$, on note $A^0 = I_n = B^0$ et l'égalité est vérifiée), en effet, on a :

$$A^{k+1}P = A^k(AP) = A^k(PB) = (A^kP)B = PB^kB = PB^{k+1}.$$

Par linéarité, on en déduit l'égalité $Q(A)P = PQ(B)$, pour tout polynôme Q de $\mathbb{C}[X]$. En particulier on aura $0 = \chi_A(A)P = P\chi_B(A)$ avec $\chi_B(A)$ inversible, ce qui donnerait $P = 0$: c'est absurde. Donc χ_A et χ_B ne sont pas premiers entre eux : on a une valeur propre commune pour A et B.

4.20. Si A est la matrice de σ dans une base de $E \approx \mathbb{R}^n$, on a $A^2 = -I_n$ donc $(-1)^n = \det(A^2) = (\det A)^2$ est positif, d'où n pair : posons $n = 2p$.

Soit e_1 non nul dans E, posons $e_{p+1} = \sigma(e_1)$, on a $\{e_1, e_{p+1}\}$ libre, (sinon, e_1 vecteur propre de σ qui n'en a pas, ses valeurs propres étant i et $-i$), et $\sigma(e_{p+1}) = -e_1$.

On sent l'amorce d'une récurrence.

Posons $F_1 = \text{Vect}(e_1, e_{p+1})$, et soit $e_2 \notin F_1$, on pose $e_{p+2} = \sigma(e_2)$ et $F_2 = \text{Vect}(e_2, e_{p+2})$, on a $F_1 \cap F_2 = \{0\}$, car si $x = \alpha e_2 + \beta e_{p+2}$ est dans F_1, stable par σ, on aura $\sigma(x) = -\beta e_2 + \alpha e_{p+2}$ dans F_1, donc par

combinaison linéaire, $\alpha x - \beta\sigma(x) = (\alpha^2 + \beta^2)e_2$ est dans F_1, et x non nul donnerait $\alpha^2 + \beta^2 > 0$, d'où e_2 dans F_1, ce qui n'est pas.

On suppose construits des sous-espaces $F_1, ..., F_j$, $(j < p)$, du type $F_k = \text{Vect}(e_k, \sigma(e_k))$, de dimension deux, stables par σ puisque $\sigma^2 = -\text{id}_E$, en somme directe.

Alors $G = \bigoplus_{k=1}^{j} F_j \subset\!\!\!\neq E$: soit $e_{j+1} \notin G$.

Comme G est stable par σ, on démontre là encore, qu'avec $F_{j+1} = \text{Vect}(e_{j+1}, \sigma(e_{j+1}))$, (sous-espace de dimension deux comme F_1), on a $G \cap F_{j+1} = \{0\}$, car si $x = \alpha e_{j+1} + \beta\sigma(e_{j+1})$ est dans G, on obtient $\alpha x - \beta\sigma(x) = (\alpha^2 + \beta^2)e_{j+1}$ dans G et avec $\alpha^2 + \beta^2 > 0$ si x non nul, on aurait e_{j+1} dans G.

Mais alors $F_1, ..., F_j, F_{j+1}$ sont $j+1$ plans stables par σ, en somme directe, et on parvient à $E = \bigoplus_{k=1}^{p} F_p$ par ce procédé. Dans la base $(e_1, ..., e_p, \sigma(e_1), ..., \sigma(e_p))$ la matrice de σ est du type voulu.

Remarque. On peut également introduire le complexifié $\tilde{E} = \mathbb{C}^{2p}$ et l'endomorphisme $\tilde{\sigma}$ de $\tilde{E}$ de matrice A dans la base canonique de $\tilde{E}$ par exemple. Il annule le polynôme $X^2 + 1$, scindé à racines simples (sur $\mathbb{C}$), donc il est diagonalisable. De plus le polynôme caractéristique est $\det(A - \lambda I_{2p})$, à coefficients réels, donc les valeurs propres sont conjuguées : c'est i et $-i$, chacune étant de multiplicité p.

Avec $Z_1, ..., Z_p$, vecteurs colonnes de $\mathbb{C}^{2p}$, propres pour la valeur propre i, et $\bar{Z}_1, ..., \bar{Z}_p$, les conjugués pour la valeur propre $-i$, on aurait, en posant $Z_k = X_k + iY_k$, avec X_k et Y_k matrices colonnes de $\mathbb{R}^{2p}$ cette fois, les égalités $A(X_k + iY_k) = i(X_k + iY_k)$, d'où $AX_k = -Y_k$ et $AY_k = X_k$.

Comme $X_k = \frac{1}{2}(Z_k + \bar{Z}_k)$ et $Y_k = \frac{1}{2i}(Z_k - \bar{Z}_k)$, les $(X_k)_{1 \leqslant k \leqslant p}$ et les $(Y_k)_{1 \leqslant k \leqslant p}$ sont indépendants sur $\mathbb{C}$, (matrice de passage bloc diagonale d'ordre p, avec la matrice $(2, 2)$: $\begin{pmatrix} \frac{1}{2} & \frac{1}{2i} \\ \frac{1}{2} & -\frac{1}{2i} \end{pmatrix}$, régulière, sur la diagonale).

Mais alors ces $2p$ vecteurs de $\mathbb{R}^{2p}$ sont *a fortiori* indépendants, et dans la base $(Y_1, ..., Y_p ; X_1, ..., X_p)$ on a la matrice voulue.

4.21. Si on observe la localisation des a_k, on est amené à introduire la matrice

$$J = \begin{pmatrix} 0 & 1 & & & 0 \\ & \ddots & \ddots & & \\ & & \ddots & \ddots & \\ & 0 & & \ddots & 1 \\ 0 & & & & 0 \\ 1 & 0 & & & \end{pmatrix},$$

traduction, dans une base $\mathscr{B} = (e_1, ..., e_p)$ de $E \approx K^p$, d'un endomorphisme f vérifiant $f(e_1) = e_p$, et pour $2 \leqslant k \leqslant p$, $f(e_k) = e_{k-1}$.

En fait, f « permute circulairement » les indices, donc pour $2 \leqslant k \leqslant p$, on a :

$$e_1, e_2, ..., e_{k-1}, e_k, e_{k+1}, ..., e_p$$

donne, par f^k :

$$e_{p-k+1}, e_{p-k+2}, ..., e_{p-1}, e_p, e_1, ..., e_{p-k},$$

donc $A = \sum_{k=1}^{p} a_k J^{k-1}$.

Dans l'anneau, (et même, le corps car p est premier), $\mathbb{Z}/p\mathbb{Z}$, on a $(a+b)^p = a^p + b^p$, ce qui se généralise à :

$$(a_1 + a_2 + ... + a_k)^p = a_1^p + a_2^p + ... + a_k^p,$$

et ce qui se généralise, pour des matrices $A_1, ..., A_p$ *qui commutent*, en

$$(A_1 + A_2 + ... + A_k)^p = A_1^p + A_2^p + ... + A_k^p ;$$

tout ceci provenant de la nullité des coefficients du binôme C_p^k, pour $1 \leqslant k \leqslant p-1$, dans $\mathbb{Z}/p\mathbb{Z}$, avec p premier.

Ici, les $a_k J^{k-1}$ commutent, donc :

$$A^p = a_1^p I + a_2^p J^p + ... + a_p^p (J^p)^{k-1},$$

et comme $J^p = I$, il reste :

$$A^p = (a_1^p + a_2^p + ... + a_p^p) I,$$

et $\det(A^p) = (\det A)^p = (a_1^p + a_2^p + ... + a_p^p)^p$.

Il suffit de se rappeler alors que, dans $\mathbb{Z}/p\mathbb{Z}$, on a pour tout élément $a^p = a$, (Théorème de Fermat), pour en déduire l'égalité $\det A = a_1 + a_2 + ... + a_p$.

En remplaçant a_1 par $a_1 - \lambda$, on a, pour λ variant dans $\mathbb{Z}/p\mathbb{Z}$,

$$\begin{aligned}\det(A - \lambda I) &= (a_1 - \lambda) + a_2 + ... + a_p \\ &= (a_1 - \lambda)^p + a_2 + ... + a_p \\ &= (-\lambda)^p + a_1 + a_2 + ... + a_p,\end{aligned}$$

d'où le polynôme caractéristique cherché.

4.22. Les données sont symétriques en A et B : la conclusion doit l'être aussi, ce qui conduit à considérer $A - I_n$ ainsi que $B - I_n$ et leur... produit !

On a $(A - I_n)(B - I_n) = AB - A - B + I_n = I_n$, donc $A - I_n$ et $B - I_n$ sont inverses l'une de l'autre. N'est-ce pas symétrique ?

4.23. On a deux données : matrices nilpotentes de $\mathcal{M}_n(\mathbb{C})$, donc trigonalisables, avec des 0 sur la diagonale car si λ est valeur propre de M nilpotente d'ordre k, avec X vecteur propre non nul associé, on aura $0 = M^k(X) = \lambda^k X$, d'où $\lambda = 0$; et l'autre donnée : matrices qui commutent deux à deux, ce qui rappelle un résultat de cours sur une trigonalisation simultanée, résultat que nous allons étendre par récurrence au cas de p matrices. Et pour cela il faut se rappeler de la justification et commencer par justifier que, sur $E \approx K^n$, si p endomorphismes $u_1, u_2, ..., u_p$ commutent 2 à 2 et ont des polynômes caractéristiques scindés, ils ont un vecteur propre commun, non nul.

C'est vrai si $p = 2$, (cours), on le suppose pour $p - 1$, et quand on part de p endomorphismes, si λ est valeur propre de u_1, on se place sur $E_1 = \operatorname{Ker}(u_1 - \lambda \mathrm{id}_E)$, sous-espace propre de u_1, stable par chaque u_i, qui commute à u_1.

On peut donc introduire les $\tilde{u}_i$ induits par les u_i sur E_1 (avec $\tilde{u}_1$ homothétie de rapport λ), pour $2 \leqslant i \leqslant p$ on a $p - 1$ endomorphismes de E_1 qui commutent 2 à 2 et de polynômes caractéristiques scindés, (ils divisent ceux des u_i : conséquence de E_1 stable). L'hypothèse de récurrence s'applique et fournit un vecteur non nul de E_1, propre pour

chaque $\tilde{u}_i$ donc pour chaque u_i, pour $i \geqslant 2$, mais aussi pour u_1 qui est une homothétie sur E_1.

On peut alors justifier que, si $u_1, ..., u_p$ commutent deux à deux et ont des polynômes caractéristiques scindés, il existe une base commune de trigonalisation de $E \approx K^n$, et ce, par récurrence sur n.

C'est évident si $n = 1$, (toute matrice (1, 1) est triangulaire), on le suppose vrai sur un espace de dimension $n-1$, et on passe au cas de $E \approx K^n$.

Si les u_i, dans L(E), commutent, il en est de même des ${}^t u_i$ dans L(E*), E* dual de E. De plus u_i et ${}^t u_i$ ont même polynôme caractéristique. Donc les $({}^t u_i)_{1 \leqslant i \leqslant p}$ ont un vecteur propre non nul commun, φ, et le noyau H de cette forme linéaire φ est un hyperplan H stable par chaque u_i. Les endomorphismes $\tilde{u}_i$ induits par les u_i sur H commutent deux à deux, et leurs polynômes caractéristiques divisant ceux des u_i sont scindés. Donc l'hypothèse de récurrence s'applique : il existe une base $\mathscr{C}$ de H dans laquelle la matrice de chaque $\tilde{u}_i$ est triangulaire.

Si $E = H \oplus K \cdot a$, dans la base $\mathscr{B} = \mathscr{C} \cup \{a\}$, la matrice de chaque u_i est alors triangulaire.

Retour à l'exercice : il existe $P \in GL_n(\mathbb{C})$ telle que, pour $i = 1, 2, ..., n$, $P^{-1} M_i P = T_i$ soit triangulaire supérieure avec des 0 sur la diagonale. On a donc

$$M_1 M_2 \ldots M_n = P T_1 P^{-1} \cdot P T_2 P^{-1} \cdot \ldots \cdot P T_n P^{-1}$$

$$= P \left(\prod_{j=1}^{n} T_j \right) P^{-1}.$$

Si $(e_1, ..., e_n)$ est la base canonique de $\mathbb{C}^n$, (en matrices colonnes en fait), on a $T_n(e_1) = 0$, puis $T_n(e_2) \in \text{Vect } e_1 \Rightarrow T_{n-1} T_n(e_2) = 0$, et on vérifie que $T_{n-r} T_{n-r+1} \ldots T_n(e_{r+1}) = 0$ en fait, donc le produit des T_j annule chaque vecteur colonne de cette base : la matrice $T = \prod_{j=1}^{n} T_j$ est associée à l'endomorphisme nul de $\mathbb{C}^n$ et finalement $\prod_{i=1}^{n} M_i = 0$.

Si K est un corps quelconque que l'on injecte dans sa clôture algébrique $\tilde{K}$, on a $P \in GL_n(\tilde{K})$ telle que $M_i = PT_iP^{-1}$ donc $M_1 \dots M_n = P(T_1 \dots T_n)P^{-1} = POP^{-1} = 0$, et comme le produit $M_1 \dots M_n$ reste dans $\mathcal{M}_n(K)$, le résultat subsiste.

4.24. L'énoncé est insuffisant sur un point : la nature du corps qui doit être algébriquement clos.

En effet, prenons $E \approx \mathbb{R}^2$, $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ matrice de valeurs propres i et $-i$, donc non diagonalisable sur $\mathbb{R}$, matrice de a dans une base de E.

Par contre a est diagonalisable dans $\mathbb{C}$, et en utilisant le résultat de l'exercice dans ce cas, (voir après), $\tilde{F}_a$ est fermé dans $\mathcal{M}_2(\mathbb{C})$, avec $\tilde{F}_a = \{g^{-1}ag\,;\, g \in GL(\mathbb{C}^2)\}$.

Supposons que l'on ait alors une suite $(P_n)_{n \in \mathbb{N}}$ d'éléments de $GL_2(\mathbb{R})$ telle que $\lim_{n \to +\infty} P_n^{-1}AP_n = B$, cette matrice B de $\mathcal{M}_2(\mathbb{R})$, donc de $\mathcal{M}_2(\mathbb{C})$ aussi est dans $\tilde{F}_a$: il existe P dans $GL_2(\mathbb{C})$ telle que $P^{-1}AP = B$, ou, ce qui est équivalent, telle que $AP = PB$.

En posant $P = R + iS$, avec R et S dans $\mathcal{M}_2(\mathbb{R})$, comme A et B sont à coefficients réels, on a donc $AR = RB$ et $AS = SB$. Mais alors, pour tout t réel, $A(R + tS) = (R + tS)B$, et comme $\det(R + tS)$ est un polynôme de degré 2 en t, à coefficients réels, donc complexes, non nul en i, il n'est pas identiquement nul, et il existe plein plein plein de t réels tels que $R + tS$ soit régulière et que $(R + tS)^{-1}A(R + tS) = B$, donc B est dans $F_a = \{g^{-1}ag\,;\, g \in GL(\mathbb{R}^2)\}$, (on assimile la matrice et l'application linéaire). Finalement F_a est fermé bien que a ne soit pas diagonalisable.

On aborde donc l'exercice sur le corps des complexes.

On suppose a diagonalisable sur $E \approx \mathbb{C}^n$.

C'est donc qu'avec $\lambda_1, \dots, \lambda_r$ valeurs propres distinctes de multiplicités respectives $\alpha_1, \dots, \alpha_r$, on a $\dim \operatorname{Ker}(a - \lambda_j \mathrm{id}_E) = \alpha_j$ et ce pour chaque j.

Mais alors, si $b = g^{-1}ag$ est dans F_a, comme $b - \lambda_j \mathrm{id}_E = g^{-1}(a - \lambda_j \mathrm{id}_E)g$, les endomorphismes semblables $b - \lambda_j \mathrm{id}_E$ et $a - \lambda_j \mathrm{id}_E$ ont même rang, donc on aura $\dim \operatorname{Ker}(b - \lambda_j \mathrm{id}_E) = \alpha_j$, pour $j = 1, \dots, r$.

Et si b est tel que, pour $j = 1, ..., r$, $\dim \operatorname{Ker}(b - \lambda_j \mathrm{id}_E) = \alpha_j$ comme ces noyaux associés à des λ_j distincts sont en somme directe, de dimension $\alpha_1 + \alpha_2 + ... + \alpha_r = n$, c'est que b est diagonalisable avec les λ_j pour valeurs propres distinctes, de multiplicités $\alpha_1, ..., \alpha_r$: a et b admettent tous les deux la matrice $\operatorname{diag}(\underbrace{\lambda_1, ..., \lambda_1}_{\alpha_1 \text{ fois}} ; \underbrace{\lambda_2, ..., \lambda_2}_{\alpha_2 \text{ fois}} ; ... ; \underbrace{\lambda_r ... \lambda_r}_{\alpha_r \text{ fois}})$ dans des bases convenables, donc $b \in F_a$.

Finalement, pour a diagonalisable, de valeurs propres distinctes $(\lambda_1, ..., \lambda_r)$, de multiplicités respectives $\alpha_1, ..., \alpha_r$, on a :

$$(b \in F_a) \Leftrightarrow \forall j = 1, ..., r, \dim(\operatorname{Ker}(b - \lambda_j \mathrm{id}_E)) = \alpha_j,$$

$$\Leftrightarrow \forall j = 1, ..., r, \operatorname{rang}(b - \lambda_j \mathrm{id}_E) = n - \alpha_j,$$

et cette dernière formulation va permettre de conclure. En effet elle implique que pour chaque j, tous les mineurs d'ordre $n - \alpha_j + 1$ de $B - \lambda_j I_n$ sont nuls, (B matrice de b dans une base de $\mathbb{C}^n$) ; et si réciproquement on a ces conditions, le rang de $b - \lambda_j \mathrm{id}_E$ est inférieur ou égal à $n - \alpha_j$, donc $\operatorname{Ker}(b - \lambda_j \mathrm{id}_E)$ est de dimension supérieure ou égale à α_j, et ce pour chaque α_j : il y a égalité car ces noyaux sont en somme directe, (les λ_j sont distincts), et la somme des α_j vaut n.

Finalement, $b \in F_a$ si et seulement si, pour chaque j, tous les mineurs d'ordre $n - \alpha_j + 1$ de $B - \lambda_j I_n$ sont nuls : il s'agit d'écrire des polynômes, par rapport aux coefficients de B, nuls et cela définit des fermés dont on prend l'intersection. On a bien F_a fermé.

Réciproquement, si F_a est fermé, et si a n'était pas diagonalisable, c'est que en jordanisant a, il y aurait au moins un 1 au-dessus de la diagonale, en $k-1^{\text{ième}}$ ligne et $k^{\text{ième}}$ colonne par exemple. Donc dans une base $\{e_1, ..., e_n\} = \mathscr{B}$ de E la matrice A de a serait du type :

$$A = \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & 0 & 0 & \\ & & \lambda_{k-1} & 1 & \\ & & & \lambda_k & \\ & 0 & & & \ddots \\ & & & & \lambda_n \end{pmatrix}$$

, avec, si $k = 2$, pas de 0 avant le 1 ici, les λ_j n'étant pas forcément distincts. Attention, on prend $k = 2$ ou k tel que le 1 soit précédé d'un 0, au-dessus de la diagonale.

Soit $(P_r)_{r \in \mathbb{N}^*}$ avec $P_r = \operatorname{diag}(1, ..., 1, r, 1, ..., 1)$, on a :

$$\text{en } k-1^{\text{ième}} \text{ position}$$

$$P_r^{-1} = \operatorname{diag}\left(1, ..., 1, \underbrace{\frac{1}{r}}_{\text{en } k-1^{\text{ième}} \text{ position}}, 1, ..., 1\right),$$

le passage de A à $A' = AP_r$ revient à multiplier la $(k-1)^{\text{ième}}$ colonne de A par r, puis le passage de A' à $A'' = P_r^{-1}A'$ revient à multiplier la $(k-1)^{\text{ième}}$ ligne de A' par $\frac{1}{r}$, donc $P_r^{-1}AP_r = \begin{pmatrix} \lambda_1 & & & & \\ & \ddots & & & \\ & & \lambda_{k-1} & & \\ & & & \lambda_k & \\ & & & & \ddots \\ & & & & & \lambda_n \end{pmatrix}$, car dans la $(k-1)^{\text{ième}}$ colonne, il n'y a que λ_{k-1} non nul, qui a donc été multiplié par r, puis par $\frac{1}{r}$ car il est aussi dans la $(k-1)^{\text{ième}}$ ligne.

Si r tend vers $+\infty$, le coefficient au-dessus de λ_k va tendre vers 0, mais alors si B est la matrice limite, la dimension du sous-espace propre de B pour la valeur propre λ_k augmente de 1 donc B n'est pas semblable à A, ce qui contredit F_a fermé.

4.25. Il y a du Vandermonde dans l'air. Si on note c_j la colonne des x_i^{j-1}, pour j fixé, $j \geqslant 1$, et i variant de 1 à n, on a $D_n = \det(C_1, C_2, ..., C_{n-1}, C_{n+2})$, et si on parvenait à exprimer la dernière colonne C_{n+2} à l'aide de $C_n, C_{n-1}, ..., C_1$, on retrouverait un résultat connu. Qu'à cela ne tienne !

Soit $P(x) = \prod_{i=1}^{n} (x - x_i) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} + ...$ avec $\sigma_1 = \sum_{i=1}^{n} x_i$, somme des racines, et $\sigma_2 = \sum_{1 \leqslant i < j \leqslant n} x_i x_j$.

Chaque x_i étant zéro de P donne la relation :

$$x_i^n = \sigma_1 x_i^{n-1} - \sigma_2 x_i^{n-2} + ...,$$

qui, multipliée par x_i, conduit à :

$$x_i^{n+1} = \sigma_1 x_i^n - \sigma_2 x_i^{n-1} + \ldots$$

Si on fait varier i, on obtient les matrices colonnes des x_i^{n+1}, (notée C_{n+2}) et des x_i^n, (notée C_{n+1}) comme combinaison linéaire de $C_n, C_{n-1}, \ldots, C_1$. On aura :

$C_{n+2} = \sigma_1 C_{n+1} - \sigma_2 C_n +$ une combinaison des C_j, pour $j \leqslant n-1$, avec :

$C_{n+1} = \sigma_1 C_n +$ une combinaison linéaire des C_j, $j \leqslant n-1$, d'où :

$C_{n+2} = (\sigma_1^2 - \sigma_2) C_n +$ une combinaison linéaire des C_j, $j \leqslant n-1$.

L'aspect forme n.linéaire alternée d'un déterminant donne alors :

$$\begin{aligned} D_n &= \det(C_1, C_2, \ldots, C_{n-1}, (\sigma_1^2 - \sigma_2) C_n) \\ &= (\sigma_1^2 - \sigma_2) \det(C_1, \ldots, C_n) \\ &= \left(\sum_{i=1}^{n} x_i^2 + \sum_{1 \leqslant i < j \leqslant n} x_i x_j \right) \prod_{1 \leqslant i < j \leqslant n} (x_j - x_i), \end{aligned}$$

en supposant connue l'expression d'un déterminant de Vandermonde.

4.26. Le polynôme caractéristique de u, nilpotent, est $\chi_u(x) = x^n$.

Si F est sous-espace stable de dimension $k \leqslant n$, u induit un endomorphisme $\tilde{u}$ sur F, qui est encore nilpotent, donc admet pour polynôme caractéristique $\chi_{\tilde{u}}(x) = x^k$. Par Cayley Hamilton, on a donc $\tilde{u}^k = 0$, donc $F = \operatorname{Ker} \tilde{u}^k$, ($\tilde{u}$ endomorphisme de F), mais *a fortiori*, pour x dans F on a $u^k(x) = \tilde{u}^k(x) = 0$, d'où $F \subset \operatorname{Ker} u^k$.

Si on jordanise u, de rang $n-1$, la réduite de Jordan est la matrice carrée d'ordre n :

$$J = \begin{pmatrix} 0 & 1 & 0 & & & \\ 0 & 0 & 1 & & 0 & \\ & & \ddots & \ddots & & \\ & & & \ddots & 1 & \\ & 0 & & & 0 & 1 \\ & & & & 0 & 0 \end{pmatrix}$$

(il faut $n-1$ fois des 1 au-dessus de la diagonale), donc J^k est la matrice où les 1 se sont « déplacés k fois », ils commencent en première ligne, $k+1^{\text{ième}}$ colonne, pour finir en $n-k^{\text{ième}}$ ligne, dernière colonne : il y en a $n-k$, donc u^k est de rang $n-k$ et Ker u^k de dimension k, celle de F, d'où $F = \text{Ker } u^k$.

Finalement, il y a exactement $n+1$ sous-espaces stables, les Ker u^k, pour $0 \leqslant k \leqslant n$, avec Ker $u^0 = \{0\}$ et Ker $u^n = E$, Ker u^k étant de dimension k.

4.27. On a q projecteur si et seulement si $q^2 = q$, or, on a :

$q^2 = p_1^2 + p_1p_2 - p_1p_2p_1 + p_2p_1 + p_2^2 - p_2^2p_1 - p_2p_1^2 - p_2p_1p_2 + p_2p_1p_2p_1$

$= p_1 + p_2p_1 + p_2 - p_2p_1 - p_2p_1$, compte tenu de $p_1p_2 = 0$ et de $p_1^2 = p_1$ et $p_2^2 = p_2$; soit finalement, $q^2 = p_1 + p_2 - p_2p_1 = q$: on a un projecteur.

On constate que $p_1q = p_1^2 + p_1p_2 - p_1p_2p_1 = p_1$, (toujours $p_1p_2 = 0$), donc, si $x \in \text{Ker } q$, $p_1(x) = p_1(q(x)) = 0$, soit $x \in \text{Ker } p_1$.

De même, $p_2q = p_2p_1 + p_2^2 - p_2^2p_1 = p_2$, donc Ker $q \subset$ Ker p_2 et Ker $q \subset$ (Ker $p_1 \cap$ Ker p_2).

Puis, si $x \in \text{Ker } p_1 \cap \text{Ker } p_2$, $q(x) = p_1(x) + p_2(x) - p_2(p_1(x)) = 0$, donc Ker $q =$ Ker $p_1 \cap$ Ker p_2.

Pour les images, on vérifie que $qp_1 = p_1$ et $qp_2 = p_2$, d'où l'on déduit que tout $y = p_1(x)$ de Im p_1 s'écrit $q(p_1(x))$, donc est dans Im q : on a Im $p_1 \subset$ Im q et Im $p_2 \subset$ Im q, d'où Im $p_1 +$ Im $p_2 \subset$ Im q.

Puis y de Im q s'écrit $y = q(x) = p_1(x) + p_2(x - p_1(x))$ est dans Im $p_1 +$ Im p_2, et on a Im $q =$ Im $p_1 +$ Im p_2.

4.28. D'abord, comme f annule le polynôme scindé à racines simples $(X-a)(X-b)$, f est diagonalisable avec deux sous-espaces propres $F_a = \text{Ker } (f - a\text{Id}_E)$ et $F_b = \text{Ker } (f - b\text{Id}_E)$ en somme directe.

a) Pour λ non nul, le polynôme en f, $\lambda(f - a\text{Id}_E)$, admet donc F_a et F_b pour sous-espaces propres, en somme directe, pour les valeurs propres $\lambda(a-a) = 0$ et $\lambda(b-a)$. Ce sera un projecteur si et seulement si $\lambda(b-a) = 1$, soit $\lambda = \dfrac{1}{b-a}$.

De même $\mu(f - b\mathrm{Id}_E)$ est diagonalisable, avec les sous-espaces propres F_a et F_b, pour les valeurs propres $\mu(a-b)$ et 0 : on aura un projecteur si et seulement si $\mu = \dfrac{1}{a-b}$.

b) L'égalité $(f - a\mathrm{Id}_E) \circ (f - b\mathrm{Id}_E) = 0$, donne l'inclusion : $\mathrm{Im}\,(f - b\mathrm{Id}_E) \subset \mathrm{Ker}\,(f - a\mathrm{Id}_E)$.

De plus $\mathrm{Ker}\,(f - a\mathrm{Id}_E) = F_a$ et la dimension de $\mathrm{Im}\,(f - b\mathrm{Id}_E)$ est $p - \dim \mathrm{Ker}\,(f - b\mathrm{Id}_E) = p - \dim F_b$, ($p$, dimension de E) ; comme $E = F_a \oplus F_b$, on a $\mathrm{Im}\,(f - b\mathrm{Id}_E)$ de dimension $\dim F_a$, soit $\dim(\mathrm{Ker}\,(f - a\mathrm{Id}_E))$: l'inclusion est une égalité.

Comme $f - a\mathrm{Id}_E$ et $f - b\mathrm{Id}_E$ commutent, (polynômes en f), on a également $\mathrm{Im}\,(f - a\mathrm{Id}_E) = \mathrm{Ker}\,(f - b\mathrm{Id}_E)$.

c) En décomposant un vecteur x de E en $x = u + v$ dans la somme directe $\mathrm{Ker}\,(f - a\mathrm{Id}_E) \oplus \mathrm{Ker}\,(f - b\mathrm{Id}_E)$, on obtient : $x = u + v$ et $f(x) = au + bv$, d'où :

$f(x) - ax = (b-a)v \in F_b$ et :

$f(x) - bx = (a-b)u \in F_a$, d'où, comme $a \neq b$,

$$x = u + v = \frac{1}{a-b}\,(f(x) - bx) + \frac{1}{b-a}\,(f(x) - ax),$$

décomposé dans $F_a \oplus F_b$. Comme alors $f(f(x) - bx) = a \cdot (f(x) - bx)$ et $f(f(x) - ax) = b \cdot (f(x) - ax)$ on obtient, pour tout n de $\mathbb{N}^*$,

$$f^n(x) = \frac{a^n}{a-b}\,(f(x) - bx) + \frac{b^n}{b-a}\,(f(x) - ax),$$

d'où l'égalité : $f^n = \dfrac{b^n - a^n}{b-a} f + \dfrac{ba^n - ab^n}{b-a} \mathrm{Id}_E$, formule encore valable si $n = 0$, avec la convention $a^n = b^n = 1$ et $f^0 = \mathrm{id}_E$.

d) Si $ab \neq 0$, f n'ayant pas 0 pour valeur propre est injective, en dimension finie, donc bijective, et comme sur $\mathrm{Ker}\,(f - a\mathrm{Id}_E)$, (resp. $\mathrm{Ker}\,(f - b\mathrm{Id}_E)$), f^{-1} agit comme l'homothétie de rapport a^{-1}, (resp. b^{-1}), la même décomposition de x en $u + v$ conduit, pour n entier négatif, à la même expression de $f^n(x)$, donc l'expression trouvée de f^n est valable pour tout n dans $\mathbb{Z}$.

4.29. Le résultat est immédiat comme conséquence du Théorème de Baire : les F_j sont des fermés de E, car sous-espaces de dimension finie de E, comme $E \approx \mathbb{R}^n$ est complet, si la réunion des F_j est E, l'un des F_j est d'intérieur non vide, ce qui est exclu, (sous-espaces stricts).

Donnons-en une justification plus algébrique.

Si $E = \bigcup_{j \in \mathbb{N}} F_j$, soient x_1 et x_2 fixés dans E, pour tout $\lambda \in \mathbb{R}$, il existe $j(\lambda)$ dans $\mathbb{N}$ tel que $x_1 + \lambda x_2 \in E_{j(\lambda)}$. Comme $\mathbb{R}$ est de cardinal strictement supérieur à celui de $\mathbb{N}$, il existe λ' réel $\neq \lambda$ tel que $j(\lambda) = j(\lambda')$, donc $x_1 + \lambda x_2$ et $x_1 + \lambda' x_2$ sont dans $E_{j(\lambda)}$, d'où $\frac{1}{\lambda - \lambda'}((x_1 + \lambda x_2) - (x_1 + \lambda' x_2)) = x_2$ est dans $E_{j(\lambda)}$, ainsi que $\frac{1}{\lambda' - \lambda}(\lambda'(x_1 + \lambda x_2) - \lambda(x_1 + \lambda' x_2)) = x_1$.

Nous venons de vérifier, pour $k = 2$, la propriété

$\mathscr{P}(k)$: si $(x_1, x_2, ..., x_k) \in E^k$, il existe un indice j tel que $x_1, x_2, ...$ et x_k soient dans le même F_j.

Vérifions la propriété par récurrence sur k. On suppose $\mathscr{P}(k)$ vérifiée.

Soit $(x_1, ..., x_k ; x_{k+1})$ dans E^{k+1}, en appliquant $\mathscr{P}(k)$ on sait que, pour chaque λ de $\mathbb{R}$, il existe un $j(\lambda)$ tel que les k vecteurs $x_1, x_2, ..., x_{k-1}$ et $x_k + \lambda x_{k+1}$ soient dans $F_{j(\lambda)}$.

Là encore, (card $\mathbb{R}$ > card $\mathbb{N}$), il existe $\lambda' \neq \lambda$ tels que $x_k + \lambda x_{k+1}$, $x_1, x_2, ..., x_{k-1}$ et $x_k + \lambda' x_{k+1}$ soient dans le même $F_{j(\lambda)} = F_{j(\lambda')}$. Mais, avec $j = j(\lambda) = j(\lambda')$, F_j contiendra $x_1, x_2, ..., x_{k-1}$ ainsi que $x_{k+1} = \frac{1}{\lambda - \lambda'}((x_k + \lambda x_{k+1}) - (x_k + \lambda' x_{k+1}))$ et :

$x_k = \frac{1}{\lambda' - \lambda}(\lambda'(x_k + \lambda x_{k+1}) - \lambda(x_k + \lambda' x_{k+1}))$: on a bien $\mathscr{P}(k+1)$ vérifiée.

Mais alors, avec $\mathscr{B} = (e_1, ..., e_n)$ base de E, $\mathscr{P}(n)$ étant vérifiée, il existerait j tel que chaque e_k soient dans F_j d'où $E \subset F_j$ avec dim E > dim F_j : c'est absurde. On a $E \neq \bigcup_{j \in \mathbb{N}} F_j$. Pour cette première partie de l'exercice, les F_j ne sont pas forcément de même dimension.

Passons à la suite de l'exercice, où l'on suppose les F_j tous de même dimension.

Comme $\bigcup_{j \in \mathbb{N}} F_j \subset\neq E$, il existe un vecteur w_{p+1} tel que, pour tout j, $w_{p+1} \notin F_j$, mais alors F_j et la droite $\mathbb{R}e_{p+1}$ sont en somme directe.

Les $G_j = F_j \oplus \mathbb{R}w_{p+1}$ sont tous des sous-espaces de dimension $p+1$ de E. Si $p = n-1$, $G_j = E$ et $W = \mathbb{R}w_{p+1}$ convient. Sinon, la réunion des G_j est strictement contenue dans E : il existe $w_{p+2} \notin \bigcup_j G_j$, donc, pour tout j, $H_j = G_j \oplus \mathbb{R}w_{p+2}$ est sous-espace de dimension $p+2$ de E. Si $n-p = 2$, on a trouvé $W = \mathbb{R}w_{p+1} \oplus \mathbb{R}w_{p+2}$, sinon on itère le raisonnement. En $n-p$ étapes, on construit W supplémentaire commun à tous les F_j.

4.30. Comme tout $y = (u+v)(x) = u(x) + v(x) \in (\text{Im } u + \text{Im } v)$ on a $\text{rg}(u+v) \leqslant \dim(\text{Im } u + \text{Im } v) = \text{rg}(u) + \text{rg}(v) - \dim(\text{Im } u \cap \text{Im } v)$, d'où $\text{rg}(u+v) \leqslant \text{rg}(u) + \text{rg}(v)$.

Puis, en écrivant $u = (u+v) + (-v)$, et en appliquant l'inégalité précédente, on a :

$$\text{rg}(u) \leqslant \text{rg}(u+v) + \text{rg}(-v) = \text{rg}(u+v) + \text{rg}(v),$$

d'où $\text{rg}(u) - \text{rg}(v) \leqslant \text{rg}(u+v)$, mais aussi, (pas de jaloux) :

$$\text{rg}(v) - \text{rg}(u) \leqslant \text{rg}(v+u) = \text{rg}(u+v),$$

d'où l'encadrement :

$$-\text{rg}(u+v) \leqslant \text{rg}(u) - \text{rg}(v) \leqslant \text{rg}(u+v), \quad \text{et finalement les inégalités :}$$

$$|\text{rg}(u) - \text{rg}(v)| \leqslant \text{rg}(u+v) \leqslant \text{rg}(u) + \text{rg}(v).$$

Supposons l'égalité $\text{rg}(u+v) = \text{rg}(u) + \text{rg}(v)$, l'inégalité :

$$\text{rg}(u) + \text{rg}(v) = \text{rg}(u+v) \leqslant \text{rg}(u) + \text{rg}(v) - \dim(\text{Im } u \cap \text{Im } v)$$

implique déjà $\text{Im } u \cap \text{Im } v = \{0\}$.

Puis, si $x \in \text{Ker}(u+v)$, on a $u(x) + v(x) = 0$, donc $u(x) = -v(x)$ est dans $\text{Im } u \cap \text{Im } v = \{0\}$, d'où $u(x) = v(x) = 0$ et $x \in \text{Ker } u \cap \text{Ker } v$. Comme l'inclusion $\text{Ker } u \cap \text{Ker } v \subset \text{Ker}(u+v)$ est facile à justifier, on a l'égalité $\text{Ker}(u+v) = \text{Ker } u \cap \text{Ker } v$. Mais alors, pour les dimensions, on a :

$$\begin{aligned}
\dim(\text{Ker } u + \text{Ker } v) &= \dim \text{Ker } u + \dim \text{Ker } v - \dim(\text{Ker } u \cap \text{Ker } v) \\
&= (n - \text{rg}(u)) + (n - \text{rg}(v)) - \dim(\text{Ker}(u+v)) \\
&= 2n - \text{rg}(u) - \text{rg}(v) - n + \text{rg}(u+v) \\
&= n,
\end{aligned}$$

compte tenu de l'égalité $\text{rg}(u+v) = \text{rg}(u) + \text{rg}(v)$, d'où la deuxième égalité, $\text{Ker } u + \text{Ker } v = \mathbb{R}^n$.

Réciproquement, si $\text{Ker } u + \text{Ker } v = \mathbb{R}^n$ et $\text{Im } u \cap \text{Im } v = \{0\}$, soit x dans $\text{Ker } (u+v)$, alors on a toujours $u(x) = v(x) = 0$ car $u(x) = -v(x) \in \text{Im } u \cap \text{Im } v = \{0\}$ donc $\text{Ker } (u+v) \subset \text{Ker } u \cap \text{Ker } v$ et on a l'égalité, l'autre inclusion étant évidente.

Donc $\text{Ker } (u+v) = \text{Ker } u \cap \text{Ker } v$.

Mais alors, on a :

$$\text{rg } (u+v) = n - \dim (\text{Ker } (u+v)) = n - \dim (\text{Ker } u \cap \text{Ker } v).$$

Or $n = \dim (\text{Ker } u + \text{Ker } v)$

$$= \dim (\text{Ker } u) + \dim (\text{Ker } v) - \dim (\text{Ker } u \cap \text{Ker } v)$$

$$= 2n - \text{rg } (u) - \text{rg } (v) - \dim (\text{Ker } u \cap \text{Ker } v),$$

d'où $\dim (\text{Ker } u \cap \text{Ker } v) = n - \text{rg } (u) - \text{rg } (v)$, et finalement :

$\text{rg } (u+v) = n - (n - \text{rg } u - \text{rg } v) = \text{rg } (u) + \text{rg } (v)$, ce qui achève la justification de l'équivalence.

4.31. Si M est une involution, M annule le polynôme scindé à racines simples, $X^2 - 1$, donc est diagonalisable, avec comme seules valeurs propres possibles 1 et – 1.

Si 1 est valeur propre triple, $M = I_3$, $(a = 1, b = c = 0)$, et si – 1 est valeur propre triple, $M = -I_3$, $(a = -1, b = c = 0)$.

Ces deux cas de l'identité et de la symétrie point étant écartés, M aura forcément 1 et – 1 pour valeurs propres, l'une des deux étant double.

Le polynôme caractéristique est :

$$\chi_M(\lambda) = \begin{vmatrix} a-\lambda & b & c \\ c & a-\lambda & b \\ b & c & a-\lambda \end{vmatrix} = (a-\lambda)^3 + c^3 + b^3 - 3bc(a-\lambda),$$

équation du troisième degré en $a - \lambda$, qui a une racine réelle double, (et une simple) si et seulement si :

$4(-3bc)^3 + 27(b^3 + c^3)^2 = 0$, soit encore si $27(b^3 - c^3)^2 = 0$, donc si et seulement si $b = c$ car on est sur $\mathbb{R}$.

Avec $b = c$, on a encore $M = (a-b)I_3 + b \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, et la matrice

$J = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ étant de rang 1 admet un noyau de dimension 2, donc 0

est valeur propre double au moins, la trace de J est 3 d'où 3 valeur propre simple et J est diagonalisable.

Mais alors M est diagonalisable (polynôme en J), avec les mêmes sous-espaces propres et des valeurs propres valant $a-b+3b$, simple et $a-b$, double. On aura donc $M^2 = I_3$ si et seulement si on a

$$\begin{cases} ab = 1 \\ a+2b = -1, \text{ ou} \\ b = c \end{cases} \qquad \begin{cases} a-b = -1 \\ a+2b = 1, \\ b = c \end{cases}$$

(et aussi $M = I_3$ ou $-I_3$).

Ceci conduit à $b = c = -\frac{2}{3}$, $a = \frac{1}{3}$, ou à $b = c = \frac{2}{3}$ et $a = -\frac{1}{3}$.

La matrice $M_1 = \frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}$ est celle de la symétrie orthogonale (sur $\mathbb{R}^3$ canonique) par rapport au plan P d'équation $x+y+z = 0$, noyau de Ker $(M_1 - I_3)$, (il est facile de vérifier que M_1 est orthogonale).

La matrice $M_2 = \frac{1}{3}\begin{pmatrix} -1 & 2 & 2 \\ 2 & -1 & 2 \\ 2 & 2 & -1 \end{pmatrix}$ est celle de la symétrie orthogonale par rapport à la droite D = Ker $(M_2 - I_3)$, dirigée par le vecteur $\vec{V}(1, 1, 1)$, perpendiculaire au plan P.

4.32. En développant par rapport à la première colonne on a :

$$D_n = (1+X^2)D_{n-1} - X\begin{vmatrix} X & 0 & 0 & & 0 \\ X & 1+X^2 & X & \dots & 0 \\ 0 & X & 1+X^2 & \dots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & 1+X^2 \end{vmatrix},$$

le deuxième déterminant, d'ordre $n-1$, valant XD_{n-2}, (en développant par rapport à la première ligne).

Ceci donne la relation de récurrence :

$D_n = (1+X^2)D_{n-1} - X^2D_{n-2}$, ou mieux :

$D_n - D_{n-1} = X^2(D_{n-1} - D_{n-2})$, ce qui conduit à l'égalité :

$D_n - D_{n-1} = (X^2)^{n-2}(D_2 - D_1)$.

On a $D_1 = 1 + X^2$, $D_2 = (1 + X^2)^2 - X^2 = X^4 + X^2 + 1$, donc :

$D_2 - D_1 = X^4$, d'où l'égalité :

$D_n - D_{n-1} = X^{2n}$, (on retrouve $D_2 - D_1 = X^{2 \cdot 2} = X^4$).

En sommant ces relations, avec $D_1 = X^2 + 1$, on obtient l'égalité $D_n(X) = \sum_{k=0}^{n} X^{2k}$ qui apporte les réponses à toutes les questions posées.

4.33. En analysant le problème, si $n = 1$, M est une matrice (2, 2) de déterminant $a^2 + b^2 = |a + ib|^2$. Pourrait-on retrouver, par des combinaisons de lignes et de colonnes ce résultat ?

On multiplie chaque ligne de numéro $k \in [n + 1, 2n]$ par i, on a :

$$\det M = \begin{vmatrix} A & -B \\ B & A \end{vmatrix} = (i)^{-n} \begin{vmatrix} A & -B \\ iB & iA \end{vmatrix}.$$

On remplace, pour $1 \leqslant k \leqslant n$, la colonne C_k de la matrice obtenue par $C_k + iC_{k+n}$: le déterminant est inchangé, d'où :

$$\det M = i^{-n} \begin{vmatrix} A - iB & -B \\ iB - A & iA \end{vmatrix}.$$

Si, dans le déterminant obtenu, on remplace, pour $1 \leqslant k \leqslant n$, la ligne L_{k+n} par la somme $L_{k+n} + L_k$, on obtient :

$$\det M = i^{-n} \begin{vmatrix} A - iB & -B \\ 0 & -B + iA \end{vmatrix} = i^{-n} \det (A - iB) \det (i(A + iB))$$

$$= i^{-n} i^n \det (A - iB) \det \overline{(A - iB)} = |\det (A - iB)|^2,$$

donc $\det M \geqslant 0$.

4.34. En développant $\det \begin{pmatrix} I_n & 0 \\ P & Q \end{pmatrix}$ par rapport à la première ligne, n fois de suite, on arrive à $\det (Q)$, valeur de ce déterminant.

De même on a $\det \begin{pmatrix} R & 0 \\ S & I_n \end{pmatrix} = \det R$, relation obtenue en développant n fois de suite par rapport à la dernière colonne.

Pour faire le lien entre $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ et ce qui précède, on peut se demander s'il existe des matrices carrées d'ordre n, P, Q, R, S, telles que :

$$\begin{pmatrix} I_n & 0 \\ P & Q \end{pmatrix}\begin{pmatrix} R & S \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} R & S \\ PR & PS+Q \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix};$$

ce qui conduit aux conditions $R = A$, $S = B$, puis $PR = PA = C$ et $PS + Q = PB + Q = D$.

La relation $PA = C$ aura une solution si A est inversible, cas que nous allons d'abord traiter, (la densité de $GL_n(\mathbb{C})$ dans $\mathcal{M}_n(\mathbb{C})$ servira ensuite).

On suppose A inversible, donc on prendra $P = CA^{-1}$, et il reste à trouver Q telle que $PB + Q = CA^{-1}B + Q = D$, d'où $Q = D - CA^{-1}B$.

Avec P, Q, R, S ainsi trouvés et le calcul par blocs précédent, on a :

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det Q \det R = \det R \det Q$$

$$= \det A \det (D - CA^{-1}B)$$

$$= \det (AD - ACA^{-1}B).$$

Or $AC = CA$ donc $ACA^{-1}B = CAA^{-1}B = CB$ et finalement $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (AD - CB)$.

Soit A non inversible, c'est que $x = 0$ est solution du polynôme caractéristique $\chi_A(x) = \det (A - xI_n) = 0$. C'en est un zéro isolé, donc $\exists p_0 \in \mathbb{N}^*$, $\forall p \geqslant p_0$, $\det \left(A - \frac{1}{p} I_n\right) \neq 0$.

Comme A et C commutent, $A_p = A - \frac{1}{p} I_n$ et C commutent aussi, donc la justification précédente donne, avec $A_p = A - \frac{1}{p} I_n$:

$$\det \begin{pmatrix} A_p & B \\ C & D \end{pmatrix} = \det (A_p D - CB),$$

et comme $\lim_{p \to +\infty} A_p = A$, et que l'application déterminant, polynomiale par rapport aux coefficients des matrices, est continue, on a bien, si p tend vers l'infini, $\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det (AD - CB)$.

4.35. a) L'espace dual E* étant de dimension finie, n, sa sphère unité S est compacte, il en est de même de S^n. L'application f, multilinéaire par rapport aux φ_j variant dans E* espace vectoriel normé de dimension finie est continue, donc bornée sur S^n et elle atteint ses bornes, puisqu'elle est à valeurs réelles.

b) Comme pour la base duale $\mathscr{B}^* = (a_1^*, ..., a_n^*)$, que l'on norme en posant $u_j = \frac{1}{|||a_j^*|||} a_j^*$, on aura $f(u_1, ..., u_n) = 1 \Big/ \left(\prod_{j=1}^{n} |||a_j^*||| \right)$, non nul, la borne supérieure de f est non nulle et même strictement positive.

Mais alors, si elle est atteinte en $(\varepsilon_1, ..., \varepsilon_n)$, ces formes duales sont libres, sinon, l'une, ε_j, serait combinaison linéaire des autres, $\left(\varepsilon_j = \sum_{k \neq j} \lambda_k \varepsilon_k \right)$, et la $j^{\text{ième}}$ colonne C_j de la matrice des $\varepsilon_j(a_i)$ serait la combinaison linéaire $\sum_{k \neq j} \lambda_k C_k$, des autres colonnes C_k, puisque $\varepsilon_j(a_i) = \sum_{k \neq j} \lambda_k \varepsilon_k(a_i)$, pour $i = 1, 2, ..., n$; et en conséquence on aurait $\det (\varepsilon_j(a_i)) = 0$, soit $f(\varepsilon_1, ..., \varepsilon_n) = 0$.

Pour prouver la bijectivité de g, on va se donner un n.uplet $(z_1, ..., z_n)$ de vecteurs de E, chaque z_j étant connu par ses coordonnées $(z_{1j}, ..., z_{nj})$ dans une base fixée de E, et on va prouver qu'il existe un et un seul n.uplet, $(y_1, ..., y_n)$ de vecteurs de E, tel que $g(y_1, ..., y_n)$ soit $(z_1, ..., z_n)$, en calculant les composantes $(y_{ij})_{1 \leqslant i \leqslant n}$ de chaque y_j dans la même base.

En prenant la $k^{\text{ième}}$ coordonnée, dans la relation définissant g, on a, pour i variant de 1 à n :

$$(1) \qquad z_{ki} = \sum_{j=1}^{n} \varepsilon_j(a_i) y_{kj},$$

ce qui montre que le n.uplet réel, $(y_{k1}, y_{k2}, ..., y_{kn})$ est solution d'un système de n équations à n inconnues, de matrice celle des $(\varepsilon_j(a_i))_{1 \leqslant i, j \leqslant n}$, matrice régulière puisque son déterminant est $f(\varepsilon_1, \varepsilon_2, ..., \varepsilon_n)$, stricte-

ment positif. On a donc existence et unicité des $(y_{ki})_{1 \leqslant i \leqslant n}$, et ceci, pour tout k d'où la bijectivité de g qui, par ailleurs agit linéairement sur les y_j.

c) Les vecteurs e_i sont tels que $(a_1, ..., a_n) = g(e_1, ..., e_n)$ donc $a_i = \sum_{j=1}^{n} \varepsilon_j(a_i)e_j$, ce qui entraîne : $\varepsilon_k(a_i) = \sum_{j=1}^{n} \varepsilon_j(a_i)\varepsilon_k(e_j)$, puis, en modifiant les indices :

$$a_i = \sum_{k=1}^{n} \varepsilon_k(a_i)e_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{n} \varepsilon_j(a_i)\varepsilon_k(e_j) \right) e_k,$$

d'où les égalités :

$$(2) \qquad \varepsilon_k(a_i) = \sum_{j=1}^{n} \varepsilon_j(a_i)\varepsilon_k(e_j),$$

puisque le vecteur a_i n'a qu'une décomposition dans la base $e_1, ..., e_n$, car en fait, $\{e_1, ..., e_n\}$ est une base de E, $\{a_1, ..., a_n\}$ en étant une, car, en y regardant bien, les égalités (1) traduisent l'égalité matricielle ${}^tZ = M{}^tY$, en notant Y, (resp. Z) la matrice carrée d'ordre n des composantes des y_j, (resp. z_j), dans la base de E fixée au b, et M la matrice carrée régulière des $(\varepsilon_j(a_i))_{1 \leqslant i,j \leqslant n}$.

On a donc $\{z_1, ..., z_n\}$ base de E $\Leftrightarrow$ Z régulière $\Leftrightarrow {}^tZ$ régulière $\Leftrightarrow {}^tY = M^{-1}\,{}^tZ$ régulière $\Leftrightarrow \{y_1, ..., y_n\}$ base de E.

Mais les relations (2), à leur tour, prouvent que, pour k fixé et i variant de 1 à n, les réels $\varepsilon_k(e_1), \varepsilon_k(e_2), ..., \varepsilon_k(e_n)$ sont solutions d'un système de n équations linéaires, de matrice celle des $(\varepsilon_j(a_i))_{1 \leqslant i,j \leqslant n}$, matrice régulière comme on l'a vu en b). La solution de ce système est unique, or on en tient une, celle définie par $\varepsilon_k(e_k) = 1$ et, pour tout $j \neq k$, $\varepsilon_k(e_j) = 0$, ce qui définit $e_k{}^*$ en fait, donc la base des ε_k est bien la base duale de celle des e_j.

d) On a le produit matriciel :

$$(\varepsilon_j(a_i))_{1 \leqslant i,j \leqslant n}(\varphi_v(e_u))_{1 \leqslant u,v \leqslant n} = \left(\sum_{k=1}^{n} \varepsilon_k(a_i)\varphi_j(e_k) \right)_{1 \leqslant i,j \leqslant n},$$

en notant, dans l'indexation, en premier l'indice de ligne.

Mais $\sum_{k=1}^{n} \varepsilon_k(a_i)\varphi_j(e_k) = \varphi_j\left(\sum_{k=1}^{n} \varepsilon_k(a_i)e_k \right) = \varphi_j(a_i)$ puisque $g(e_1, ..., e_n) = (a_1, ..., a_n)$.

On obtient la matrice des $(\varphi_j(a_i))_{1 \leqslant i,j \leqslant n}$, et en prenant les déterminants des deux membres, on obtient l'égalité :

$$f(\varepsilon_1, ..., \varepsilon_n) \det ((\varphi_v(e_u))_{1 \leqslant u, v \leqslant n}) = f(\varphi_1, ..., \varphi_n).$$

e) Prenons alors φ dans S, la relation précédente donne, vu les valeurs des $\varepsilon_k(e_j)$:

$$f(\varepsilon_1, ..., \varepsilon_{i-1}, \varphi, \varepsilon_{i+1}, ..., \varepsilon_n) = \begin{vmatrix} 1 & & 0 & \varphi(e_1) & & 0 \\ & \ddots & & \vdots & & \\ 0 & & 1 & \varphi(e_i) & & \\ & & & \vdots & 1 & 0 \\ & & & & & \ddots \\ 0 & & & \varphi(e_n) & 0 & 1 \end{vmatrix} f(\varepsilon_1, ..., \varepsilon_n)$$

$$= \varphi(e_i) f(\varepsilon_1, ..., \varepsilon_n).$$

Or, la borne supérieure de f est atteinte en $(\varepsilon_1, ..., \varepsilon_n)$, on a donc $\varphi(e_i) f(\varepsilon_1, ..., \varepsilon_n) \leqslant f(\varepsilon_1, ..., \varepsilon_n)$, d'où $\varphi(e_i) \leqslant 1$ puisque la borne supérieure de f est > 0, (vu au b).

Avec :

$$f(-\varepsilon_1, \varepsilon_2, ..., \varepsilon_{i-1}, \varphi, \varepsilon_{i+1}, ..., \varepsilon_n) = -\varphi(e_i) f(\varepsilon_1, ..., \varepsilon_n) \leqslant f(\varepsilon_1, ..., \varepsilon_n)$$

on obtient $-\varphi(e_i) \leqslant 1$ d'où $-1 \leqslant \varphi(e_i) \leqslant 1$.

On a donc $|\varphi(e_i)| \leqslant 1$, pour toute forme φ de S, et comme $\varepsilon_i(e_i) = 1$, on aura $\|e_i\| = \sup \{|\varphi(e_i)| ; \varphi \in S\} = 1$.

4.36. a) Si u est une affinité de rapport λ, par rapport au sous-espace G, parallèlement au sous-espace F, c'est que $E = F \oplus G$, et, si p est la projection sur G parallèlement à F, on a

$$u(x) = p(x) + \lambda(x - p(x))$$
$$= (\lambda I + (1-\lambda)p)(x),$$

donc $u^2 = \lambda^2 I + 2\lambda(1-\lambda)p + (1-\lambda)^2 p^2$, puisque p et I commutent. Or $p^2 = p$, donc :

$$u^2 = \lambda^2 I + (1-\lambda^2)p, \text{ alors que :}$$
$$(\lambda+1)u - \lambda I = (\lambda+1)\lambda I + (\lambda+1)(1-\lambda)p - \lambda I$$
$$= \lambda^2 I + (1-\lambda^2)p : \text{on a bien l'égalité}$$
$$u^2 = (\lambda+1)u - \lambda I.$$

b) On a $u^2 - \lambda u - u + \lambda I = u(u - \lambda I) - (u - \lambda I)$

$$= (u - I)(u - \lambda I) = 0.$$

Donc, si $\lambda \neq 1$, u annule un polynôme scindé à racines simples donc u est diagonalisable.

Puis, si u est diagonalisable, si on suppose $\lambda = 1$, alors $(u-I)^2 = 0$, mais u devant annuler un polynôme scindé à racines simples, ce ne peut être que $u - I = 0$, ce qui est exclu par l'hypothèse $u \neq I$. Donc $\lambda \neq 1$ et on a bien, pour $u \neq I$, u diagonalisable si et seulement si $\lambda \neq 1$.

Avec $F = \text{Ker}(u - \lambda I)$ et $G = \text{Ker}(u - I)$, (éventuellement $G = \{0\}$, mais $F \neq \{0\}$ sinon $E = G$ et $u = I$), on a $E = F \oplus G$, et si $x = y + z$ avec $y \in F$ et $z \in G$ on a $u(x) = \lambda y + z$: u est l'affinité, parallèlement à F, de rapport λ, par rapport à G.

Si $G = \{0\}$, u est l'homothétie de rapport λ.

Dans le cas $\lambda = 1$, on a, dès le début du b), l'égalité $(u-I)^2 = 0$ et $u - I \neq 0$, (car $u \neq I$), donc u n'est pas diagonalisable.

Si on avait un sous-espace F, supplémentaire de $E_1 = \text{Ker}(u - I)$, et stable par u, l'endomorphisme induit par u sur F, noté $\tilde{u}$, vérifie encore l'égalité $(\tilde{u} - I)^2 = 0$.

Si on a $\tilde{u} - I \neq 0$, soit $x_0 \in F$ avec $y_0 = (\tilde{u} - I)(x_0)$ non nul, on aura $(\tilde{u} - I)(y_0) = 0$ soit $\tilde{u}(y_0) = y_0$: dans ce cas $y_0 \in E_1 = \text{Ker}(u - I)$ d'où $y_0 \in E_1 \cap F$: dur dur pour un vecteur non nul, car $E = E_1 \oplus F \Rightarrow E_1 \cap F = \{0\}$!

Si $\tilde{u} - I = 0$, ce n'est pas mieux car c'est tout F dans ce cas qui est dans E_1.

Finalement, il n'existe pas de supplémentaire stable de $E_1 = \text{Ker}(u - I)$.

4.37. On peut démontrer facilement que f et F ont mêmes valeurs propres dans le corps, mais pour les multiplicités, et dimensions des sous-espaces propres associés, il faudra recourir aux bases.

D'abord, soit λ une valeur propre de f, e_1 un vecteur propre (non nul) associé, et $\{e_1 ; e_2, ..., e_n\}$ une base de E. Si u est définie par $u(e_1) = e_1$ et $u(e_j) = 0$ pour $j \geqslant 2$, on a $F(u)$ telle que $F(u)(e_j) = f(u(e_j)) = 0$ si $j \geqslant 2$, et,

$F(u)(e_1) = f(\lambda e_1) = \lambda e_1 = (\lambda u)(e_1)$.

Donc $F(u)$ et λu sont égales sur la base $\{e_1, ..., e_n\}$ d'où λ valeur propre de F pour le vecteur propre u.

Réciproquement, si λ est valeur propre de F et si g est un élément non nul de $\mathscr{L}(E)$ tel que $F(g) = f \circ g = \lambda g$, pour tout $y = g(x)$ non nul de Im g, on a $f(y) = \lambda y$, d'où λ valeur propre de f.

Soit maintenant une base $\mathscr{B} = \{e_1, ..., e_n\}$ de E, et M la matrice des m_{ij}, matrice de f dans cette base. On considère la base des ε_{ij} de $\mathscr{L}(E)$, avec $\varepsilon_{ij}(e_j) = e_i$ et $\varepsilon_{ij}(e_k) = 0$ si $k \neq j$.

On a $F(\varepsilon_{uv}) = f \circ \varepsilon_{uv}$, telle que :

si $j \neq v$, $F(\varepsilon_{uv})(e_j) = 0$, et :

si $j = v$, $F(\varepsilon_{uv})(e_v) = f(e_u) = \sum_{i=1}^{n} m_{iu} e_i = \sum_{i=1}^{n} m_{iu} \varepsilon_{iv}(e_v)$.

Donc $F(\varepsilon_{uv})$ et $\sum_{i=1}^{n} m_{iu} \varepsilon_{iv}$ prennent les mêmes valeurs sur la base $\mathscr{B}$: ces applications linéaires sont égales.

On indexe alors la base $\mathscr{C}$ des ε_{ij} en :

$\mathscr{C} = \{\varepsilon_{11}, ..., \varepsilon_{n1} ; \varepsilon_{12}, ..., \varepsilon_{n2} ; ... ; \varepsilon_{1n}, ..., \varepsilon_{nn}\}$, et on considère la matrice $\mathscr{M}$ de F dans cette base $\mathscr{C}$, en prenant l'image par F du $u^{\text{ième}}$ vecteur du $v^{\text{ième}}$ paquet, à savoir $F(\varepsilon_{uv}) = \sum_{i=1}^{n} m_{iu} \varepsilon_{iv}$.

Cette décomposition ne fait intervenir que des vecteurs du $v^{\text{ième}}$ paquet, (deuxième indice constant, v), donc la matrice $\mathscr{M}$ sera bloc diagonale, et en $u^{\text{ième}}$ colonne dans ce bloc, on a la colonne des m_{iu}, pour i variant de 1 à n, donc la $u^{\text{ième}}$ colonne de M.

Mais alors, $\mathscr{M} = \begin{pmatrix} M & & 0 \\ & M & \\ & & \ddots \\ 0 & & M \end{pmatrix}$, matrice bloc diagonale, d'où tout ce qu'on veut. En particulier pour les polynômes caractéristiques, on a :

$$\chi_{\mathscr{M}}(\lambda) = \det(\mathscr{M} - \lambda I_{n^2}) = (\det(M - \lambda I_n))^n,$$

donc, α est valeur propre de multiplicité r de f si et seulement si α est valeur propre de multiplicité nr de F. De plus, le rang de $\mathscr{M} - \alpha I_{n^2}$ étant alors $n \times \text{rang}(M - \alpha I_n)$, (passer par les vecteurs colonnes indépen-

dants par exemple), on aura : dimension du sous-espace propre de F, pour $\alpha = n \times$ dimension du sous-espace propre de f, pour α.

4.38. Comme $x^2 - 5x + 6 = (x-3)(x-2)$, A annule un polynôme scindé à racines simples donc est diagonalisable, avec pour seules valeurs propres possibles 2 et 3. Il existe donc $P \in GL_n(\mathbb{R})$ telle que $P^{-1}AP = A' = \begin{pmatrix} 2I_p & 0 \\ 0 & 3I_{n-p} \end{pmatrix}$, matrice bloc, p pouvant être égal à 0 ou à n.

Posons $M' = P^{-1}MP = \begin{pmatrix} M'_1 & M'_2 \\ M'_3 & M'_4 \end{pmatrix}$, décomposition en matrice bloc, M'_1 étant carrée d'ordre p.

Avoir $F(M) = \lambda M = AM + MA$, avec λ scalaire réel et M non nulle, équivaut, P étant régulière, à avoir :

$$P^{-1}(AM + MA)P = (P^{-1}AP)(P^{-1}MP) + (P^{-1}MP)(P^{-1}AP)$$

$$= \lambda P^{-1}MP, \text{ soit encore } A'M' + M'A' = \lambda M', \text{ ce qui s'écrit encore :}$$

$$\begin{pmatrix} 2I_p & 0 \\ 0 & 3I_{n-p} \end{pmatrix}\begin{pmatrix} M'_1 & M'_2 \\ M'_3 & M'_4 \end{pmatrix} + \begin{pmatrix} M'_1 & M'_2 \\ M'_3 & M'_4 \end{pmatrix}\begin{pmatrix} 2I_p & 0 \\ 0 & 3I_{n-p} \end{pmatrix} = \lambda \begin{pmatrix} M'_1 & M'_2 \\ M'_3 & M'_4 \end{pmatrix}$$

et, en développant :

$$\begin{pmatrix} 4M'_1 & 5M'_2 \\ 5M'_3 & 6M'_4 \end{pmatrix} = \begin{pmatrix} \lambda M'_1 & \lambda M'_2 \\ \lambda M'_3 & \lambda M'_4 \end{pmatrix}.$$

Comme on veut M non nulle, M' doit être non nulle, donc les M'_i ne peuvent pas tous être nuls.

Si $M'_1 \neq 0$, on doit avoir $\lambda = 4$ d'où $M'_2 = M'_3 = M'_4 = 0$;

si $M'_2 \neq 0$, on doit avoir $\lambda = 5$, d'où $M'_1 = M'_4 = 0$ et M'_2 et M'_3 quelconques ;

si $M'_4 \neq 0$, on doit avoir $\lambda = 6$, avec $M'_1 = M'_2 = M'_3 = 0$.

Pour $0 < p < n$, les éléments propres de F sont donc

$\lambda = 4$, sous-espace propre de dimension p^2 ;

$\lambda = 5$, sous-espace propre de dimension $2p(n-p)$; et

$\lambda = 6$, sous-espace propre de dimension $(n-p)^2$: la somme des dimensions étant $(p + n - p)^2 = n^2$, F est diagonalisable.

Pour $p = 0$, $A = 3I_n$ en fait et $F(M) = 6M$: il n'est pas étonnant que F, homothétie de rapport 6, soit diagonalisable.

Si $p = n$, $A = 2I_n$ et $F(M) = 4M$, même conclusion.

4.39. La matrice $A_n = \begin{pmatrix} 1 & -\frac{\alpha}{n} \\ \frac{\alpha}{n} & 1 \end{pmatrix}$, de déterminant $1 + \frac{\alpha^2}{n^2}$, est celle d'une similitude directe, car elle s'écrit encore :

$$\sqrt{1+\alpha^2/n^2}\begin{pmatrix} \frac{1}{\sqrt{1+\alpha^2/n^2}} & -\frac{\alpha/n}{\sqrt{1+\alpha^2/n^2}} \\ \frac{\alpha/n}{\sqrt{1+\alpha^2/n^2}} & \frac{1}{\sqrt{1+\alpha^2/n^2}} \end{pmatrix},$$

et c'est la matrice de la similitude s_n de rapport $\left(1+\frac{\alpha^2}{n^2}\right)^{1/2}$, d'angle θ_n tel que $\cos\theta_n = \frac{1}{\sqrt{1+\alpha^2/n^2}}$, $\sin\theta_n = \frac{\alpha/n}{\sqrt{1+\alpha^2/n^2}}$, soit $\theta_n = \text{Arc sin}\frac{\alpha/n}{\sqrt{1+\alpha^2/n^2}}$.

Mais alors $(A_n)^n$ est la similitude σ_n, de rapport $\lambda_n = \left(1+\frac{\alpha^2}{n^2}\right)^{n/2}$, et d'angle $n\theta_n$, donc :

$$(A_n)^n = \lambda_n \begin{pmatrix} \cos n\theta_n & -\sin n\theta_n \\ \sin n\theta_n & \cos n\theta_n \end{pmatrix}.$$

Or $\lambda_n = e^{\frac{n}{2}\text{Ln}\left(1+\frac{\alpha^2}{n^2}\right)}$ tend vers 1 car l'exposant est équivalent à $\frac{\alpha^2}{2n}$; et $n\theta_n \sim \frac{n\alpha/n}{\sqrt{1+\alpha^2/n}}$ tend vers α, donc la limite cherchée est la matrice

$$\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}.$$

La géométrie peut avoir du bon !

4.40. a) Si u et v commutent, tout sous-espace propre de l'un est stable par l'autre. On est en dimension finie sur $\mathbb{C}$, donc les valeurs propres existent, (zéros des polynômes caractéristiques).

Soit λ une valeur propre de u, et $\tilde{v}$ induit par v sur le sous-espace propre $E_\lambda = \text{Ker}\,(u - \lambda id_E)$. En tant qu'endomorphisme en dimension finie sur $\mathbb{C}$, $\tilde{v}$ a droit à ses valeurs propres, d'où des vecteurs de E_λ, propres pour $\tilde{v}$ donc pour v, mais aussi pour u qui est une homothétie sur E_λ.

b) Si $uv - vu = \alpha u$, on justifie, par récurrence, que $u^k v - vu^k = k\alpha u^k$. C'est vrai si $k = 1$, et si c'est vrai pour k, on aura :

$u(u^k v - vu^k) = k\alpha u^{k+1}$, soit

$u^{k+1}v - (vu + \alpha u)u^k = k\alpha u^{k+1}$, ce qui donne bien :

$u^{k+1}v - vu^{k+1} = (k+1)\alpha u^{k+1}$: la propriété est vraie pour tout k.

Mais alors, si pour tout k entier, $u^k \neq 0$, l'endomorphisme φ de $\mathscr{L}(E)$ dans $\mathscr{L}(E)$ défini par $\varphi(u) = uv - vu$ admet une infinité de valeurs propres, les $k\alpha$, associées aux vecteurs propres u^k : c'est exclu en dimension finie, donc u est nilpotent et on se place sur $F = \text{Ker}\,u$, ce sous-espace est stable par v aussi car, si $x \in \text{Ker}\,u$, on a :

$$u(v(x)) - v(u(x)) = \alpha u(x) \text{ avec } u(x) = 0, \text{ d'où } u(v(x)) = 0.$$

On considère $\tilde{u}$ et $\tilde{v}$ induits par u et v sur Ker u, on a $\tilde{u}\tilde{v} - \tilde{v}\tilde{u} = 0$, (en fait $\tilde{u} = 0$) et on est ramené au cas a), les vecteurs propres de $\tilde{u}$, (resp $\tilde{v}$), étant vecteurs propres de u, (resp v).

c) On suppose que $uv - vu = \alpha u + \beta v$ avec $\alpha\beta \neq 0$.

Soit $v' = \alpha u + \beta v$.

$$\begin{aligned} \text{On a } uv' - v'u &= \alpha u^2 + \beta uv - \alpha u^2 - \beta vu \\ &= \beta(uv - vu) = \beta(\alpha u + \beta v) = \beta v'. \end{aligned}$$

Donc, d'après le b), u et v' ont un vecteur propre commun, x, pour les valeurs propres λ et μ. On a : $u(x) = \lambda x$ et $v'(x) = \mu x = \alpha u(x) + \beta v(x)$, d'où $\beta v(x) = \mu x - \alpha\lambda x$, soit $v(x) = \dfrac{\mu - \alpha\lambda}{\beta} x$: ce vecteur x est bien vecteur propre commun à u et v.

4.41. En développant par rapport à la première colonne, on obtient facilement l'égalité :

$$D_n = (a+b)D_{n-1} - \begin{vmatrix} ab & 0 & 0 & & \\ 1 & a+b & ab & & 0 \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & ab \\ 0 & & & 1 & a+b \end{vmatrix}, \text{ soit :}$$

$D_n = (a+b)D_{n-1} - abD_{n-2}$, et cette relation de récurrence, $D_n - (a+b)D_{n-1} + abD_{n-2} = 0$, jointe aux égalités $D_1 = a+b$ et $D_2 = (a+b)^2 - ab$ détermine les D_n.

L'équation caractéristique, $\lambda^2 - (a+b)\lambda + ab = 0$, a pour solutions $\frac{1}{2}\left((a+b) \pm ((a+b)^2 - 4ab)^{1/2}\right) = \frac{1}{2}(a+b \pm (a-b))$.

Si $a \neq b$, on a deux zéros distincts a et b, donc $D_n = \alpha a^n + \beta b^n$ avec $\begin{cases} \alpha a + \beta b = a+b \\ \alpha a^2 + \beta b^2 = a^2 + ab + b^2 \end{cases}$, système de solution $\alpha = \frac{a}{a-b}$ et $\beta = \frac{b}{b-a}$, d'où $D_n = \frac{a^{n+1} - b^{n+1}}{a-b}$, si $a \neq b$.

Pour $a = b$, on a une racine double, a, pour l'équation caractéristique, et une expression de D_n du type $D_n = (\alpha + \beta n)a^n$ avec : $\begin{cases} \alpha a + \beta a = 2a \\ \alpha a^2 + 2\beta a^2 = 3a^2 \end{cases} \quad \begin{vmatrix} -2a \\ 1 \end{vmatrix} \quad \begin{vmatrix} -a \\ 1, \end{vmatrix}$

d'où : $-a^2\alpha = -a^2$, soit $\alpha = 1$ et $\beta a^2 = a^2$, donc $\beta = 1$, ceci pour $a \neq 0$, et dans ce cas $D_n = (1+n)a^n$, expression valable également si $a = b = 0$ auquel cas $D_n = 0$, (matrice triangulaire inférieure avec des 0 sur la diagonale).

4.42. Si on cherche à diagonaliser A, on calcule le polynôme caractéristique :

$$\chi_A(\lambda) = \begin{vmatrix} -\lambda & 1 & 1 \\ -2 & 3-\lambda & 2 \\ 1 & -1 & -\lambda \end{vmatrix} = \lambda^2(3-\lambda) + 4 + (\lambda - 3) - 4\lambda$$

$$= (\lambda^2 - 1)(3-\lambda) - 4(\lambda - 1) = (\lambda - 1)((\lambda + 1)(3-\lambda) - 4)$$

$$= (\lambda - 1)(-\lambda^2 + 2\lambda - 1) = -(\lambda - 1)^3.$$

Comme $\lambda = 1$ est valeur propre triple, avec $A \neq I_3$, A n'est pas diagonalisable, mais $A - I_3$ est nilpotente.

On a $B = A - I_3 = \begin{pmatrix} -1 & 1 & 1 \\ -2 & 2 & 2 \\ 1 & -1 & -1 \end{pmatrix}$ de rang 1, nilpotente donc $B^2 = 0$, et $A^n = (B + I_3)^n = I_3 + nB$, soit :

$A^n = \begin{pmatrix} 1-n & n & n \\ -2n & 2n+1 & 2n \\ n & -n & -n+1 \end{pmatrix}$, sans autre forme de procès.

Pour justifier $B^2 = 0$, si $\{e_1, e_2, e_3\}$ est une base de $E = \mathbb{R}^3$, (ou K^3), avec $\{e_1, e_2\}$ base de Ker b, b endomorphisme associé à B, si la composante de $b(e_3)$ suivant e_3 est $\alpha \neq 0$, la matrice de b dans la base $\mathscr{B}$ étant triangulaire avec $(0, 0, \alpha)$ sur la diagonale, on aurait α valeur propre non nulle de b nilpotent, cela fait désordre. Donc $b(e_3) \in$ Ker b = Vect (e_1, e_2) et b^2 annule la base $\{e_1, e_2, e_3\}$.

On peut aussi penser à la forme réduite de Jordan, d'un opérateur nilpotent de rang 1.

4.43. On constate que $V^2 = \begin{pmatrix} U & 0 \\ 0 & U \end{pmatrix}$, donc, si U est diagonalisable, avec P dans $GL_n(\mathbb{C})$ telle que $P^{-1}UP = \Lambda$ soit diagonale, si Q est la matrice de $GL_{2n}(\mathbb{C})$, matrice bloc régulière $\begin{pmatrix} P & 0 \\ 0 & P \end{pmatrix}$ d'inverse $Q^{-1} = \begin{pmatrix} P^{-1} & 0 \\ 0 & P^{-1} \end{pmatrix}$, on aura $Q^{-1}V^2Q = \begin{pmatrix} \Lambda & 0 \\ 0 & \Lambda \end{pmatrix}$ diagonale.

Donc U diagonalisable $\Rightarrow$ V^2 diagonalisable.

On suppose cette fois V diagonalisable, alors V^2 l'est, et en notant $\{e_1, ..., e_{2n}\}$ la base canonique de $\mathbb{C}^{2n}$, ce qui permet d'identifier matrices et endomorphismes, F = Vect $(e_1, ..., e_n)$ est stable par V^2, vu la

forme de V^2, et l'endomorphisme induit, de matrice U par rapport à la base $(e_1, ..., e_n)$ de F, est alors diagonalisable.

Pour l'instant on a U diagonalisable si et seulement si V^2 l'est, et V diagonalisable implique V^2 diagonalisable.

Supposons alors V^2 diagonalisable, de valeurs propres distinctes $\lambda_1, \lambda_2, ..., \lambda_k$. La matrice V^2 annule le polynôme scindé $a(X) = \prod_{j=1}^{k} (X - \lambda_j)$, donc $\prod_{j=1}^{k} (V^2 - \lambda_j I_{2n}) = 0$, soit, avec δ_j tel que $(\delta_j)^2 = \lambda_j$, $\prod_{j=1}^{k} (V - \delta_j I_{2n})(V + \delta_j I_{2n}) = 0$.

Si tous les λ_j sont non nuls, le polynôme $b(X) = \prod_{j=1}^{k} (X - \delta_j)(X + \delta_j)$ est scindé à racines simples, annulé par V, qui est donc diagonalisable.

Si l'un des λ_j est nul, $\lambda_1 = 0$ par exemple, on a V qui annule le polynôme $X^2 \prod_{j=2}^{k} (X - \delta_j)(X + \delta_j)$, d'où, par le Théorème des noyaux, la somme directe :

$$\mathbb{C}^{2n} = \operatorname{Ker} V^2 \oplus \left(\bigoplus_{j=2}^{k} [\operatorname{Ker} (V - \delta_j I_{2n}) \oplus \operatorname{Ker} (V + \delta_j I_{2n})] \right),$$

avec $\{0\} \neq \operatorname{Ker} V \subset \operatorname{Ker} V^2$, donc V sera diagonalisable si et seulement si $\operatorname{Ker} V = \operatorname{Ker} V^2$, soit si V et V^2 ont même rang, ce qui est impossible.

En effet, si r est le rang de U, le rang de V est $n + r$, (vu sa définition par blocs) et le rang de $V^2 = \begin{pmatrix} U & 0 \\ 0 & U \end{pmatrix}$ est $2r$, avec $r < n$, (0 valeur propre de V^2), donc rang $(V^2) = r + r < r + n = \operatorname{rang} V$: on en déduit $\dim (\operatorname{Ker} V) < \dim (\operatorname{Ker} V^2)$, et la somme directe des sous-espaces propres de V ne peut pas donner $\mathbb{C}^{2n}$.

On a donc V^2 diagonalisable régulière $\Rightarrow$ V diagonalisable et V^2 diagonalisable non régulière $\Rightarrow$ V non diagonalisable.

Comme V^2 est de rang 2 rang (U), on a V^2 régulière si et seulement si U l'est, et finalement, on obtient :

V diagonalisable si et seulement si U l'est, avec U régulière.

Pour les sous-espaces propres, en considérant des matrices colonnes de $\mathbb{C}^n$, $\{\varepsilon_1, ..., \varepsilon_p\}$, qui forment une base d'un sous-espace propre de U pour la valeur propre non nulle λ, avec $\delta \neq 0$ tel que $\delta^2 = \lambda$, les vecteurs colonnes de $\mathbb{C}^{2n}$: $\begin{pmatrix} \varepsilon_j \\ \delta\varepsilon_j \end{pmatrix}$ sont tels que :

$$V\begin{pmatrix} \varepsilon_j \\ \delta\varepsilon_j \end{pmatrix} = \begin{pmatrix} 0 & I_n \\ U & 0 \end{pmatrix}\begin{pmatrix} \varepsilon_j \\ \delta\varepsilon_j \end{pmatrix} = \begin{pmatrix} \delta\varepsilon_j \\ \delta^2\varepsilon_j \end{pmatrix} = \delta\begin{pmatrix} \varepsilon_j \\ \delta\varepsilon_j \end{pmatrix}.$$

On a donc p vecteurs indépendants, qui forment une base du sous-espace propre de V pour la valeur propre δ, (et p autres pour l'autre valeur propre $-\delta$).

4.44. Si A est carrée d'ordre n sur $\mathbb{R}$, et si $\mathscr{B} = \{e_1, ..., e_n\}$ est la base canonique de $\mathbb{R}^n$, on considère l'endomorphisme f de E défini par $f(e_1) = e_n$ et $f(e_j) = e_{j-1}$, si $2 \leqslant j \leqslant n$. Il est facile de vérifier que $f^n = \mathrm{id}_E$, et que A est la matrice de $a\mathrm{id}_E + b(f + f^{n-1})$.

Si $\lambda_k = e^{i\frac{2k\pi}{n}} = (\lambda_1)^k$, le noyau de $f - \lambda_k \mathrm{id}_E$ est de dimension 1, car le système
$$\begin{cases} -\lambda_k x_1 + x_2 = 0 \\ -\lambda_k x_2 + x_3 = 0 \\ \cdots\cdots\cdots\cdots\cdots \\ -\lambda_k x_{n-1} + x_n = 0 \\ x_1 - \lambda_k x_n = 0, \end{cases}$$
a pour solution x_1 arbitraire, $x_2 = \lambda_k x_1, x_3 = (\lambda_k)^2 x_1, ...,$ $x_n = (\lambda_k)^{n-1} x_1$, et la dernière équation est vérifiée car $(\lambda_k)^n = 1$. Chaque λ_k étant effectivement valeur propre, avec des sous-espaces propres de dimension un, il en est de même pour $a\ \mathrm{id}_E + b(f + f^{n-1})$, qui admet pour valeurs propres $a + b(\lambda_k + \lambda_k^{n-1}) = a + b(\lambda_k + \lambda_k^{-1})$ soit $a + b\left(e^{i\frac{2k\pi}{n}} + e^{-\frac{2ik\pi}{n}}\right) = a + 2b\cos\frac{2k\pi}{n}$, $k = 0, 1, ..., n-1$.

La matrice est inversible si et seulement si $a \notin \left\{-2b\cos\frac{2k\pi}{n}, k = 0, 1, ..., n-1\right\}$.

4.45. L'application φ est linéaire, somme de l'identité et de l'application $X \rightsquigarrow S(X)A$, S étant une forme linéaire sur $\mathcal{M}_n(\mathbb{R})$.

Si $A = 0$, $\varphi = \mathrm{id}_{\mathcal{M}_n(\mathbb{R})}$ de noyau réduit à $\{0\}$, seule valeur propre 1, et sous-espace propre $E = \mathcal{M}_n(\mathbb{R})$.

Si $A \neq \{0\}$, l'application $\theta : X \rightsquigarrow S(X)A$ est de rang 1, de noyau l'ensemble des matrices vérifiant $x_{i1} + x_{i2} + \ldots + x_{in} = 0$: c'est un hyperplan de $\mathcal{M}_n(\mathbb{R})$.

Comme $\theta(A) = S(A)A$, avec $A \neq 0$, A est aussi vecteur propre de θ pour la valeur propre S(A).

Donc, si $S(A) \neq 0$, θ est diagonalisable, de valeurs propres 0 d'ordre $n^2 - 1$, et S(A) d'ordre 1, d'où φ diagonalisable de valeurs propres 1 d'ordre $n^2 - 1$ et $1 + S(A)$ d'ordre 1.

Si $S(A) = -1$, on a $\mathrm{Ker}\,\varphi = \mathrm{Vect}\,A$, et si $S(A) \neq -1$, (et $\neq 0$ pour l'instant), $\mathrm{Ker}\,\varphi = \{0\}$.

Cherchons directement $\mathrm{Ker}\,\varphi$, pour traiter le cas $S(A) = 0$. Si $X \in \mathrm{Ker}\,\varphi$ on a $X = -S(X)A$ d'où X colinéaire à A, or $\varphi(A) = (1 + S(A))A$, et ici on obtient bien : si $S(A) = -1$, $\mathrm{Ker}\,\varphi = \mathrm{Vect}\,(A)$, et si $S(A) \neq -1$, $\mathrm{Ker}\,\varphi = \{0\}$.

Pour les valeurs propres de φ, on a 1 valeur propre d'ordre $n^2 - 1$ au moins, de sous-espace propre Ker S, et si μ est la dernière valeur propre on aura $\mu + n^2 - 1 = \mathrm{trace}\,(\varphi)$.

En calculant trace (φ), on trouvera μ, ce qui donnera les valeurs propres de φ dans le cas général.

Soit $(E_{k,l})_{1 \leqslant k,l \leqslant n}$ la base canonique de $\mathcal{M}_n(\mathbb{R})$. On a : $\varphi(E_{k,l}) = E_{kl} + S(E_{k,l})A$ et le coefficient de $E_{k,l}$ dans la décomposition de $\varphi(E_{k,l})$ est $1 + S(E_{k,l})a_{k,l}$.

Comme $S(E_{k,l}) = 0$ si $k \neq i$, et 1 si $k = i$ et l quelconque, il reste 1 si $k \neq i$ et $1 + a_{i,l}$ si $k = i$, donc trace $(\varphi) = n^2 + \sum_{l=1}^{n} a_{il} = n^2 + S(A)$.

En résolvant $\mu + n^2 - 1 = n^2 + S(A)$, on trouve $\mu = 1 + S(A)$, comme dans le cas de $S(A) \neq 0$.

Les valeurs propres de φ sont donc 1 d'ordre $n^2 - 1$ si $S(A) \neq 0$ et $1 + S(A)$, d'ordre 1 et dans ce cas φ est diagonalisable ; ou 1 d'ordre n^2 si $S(A) = 0$, et alors φ n'est pas diagonalisable, toujours dans le cas $A \neq 0$, car alors $\varphi(X) = X \Leftrightarrow S(X) = 0$: on est dans un hyperplan.

4.46. Comme toute matrice symétrique réelle qui se respecte, A est diagonalisable.

On a $A = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 1 \\ 1 & 1 & \cdots & 1 & 1 \end{pmatrix}$, si $n \geqslant 3$, et $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ pour $n = 2$ et $A = (1)$ si $n = 1$, pour être complet.

Si $n = 1$, A est l'identité, (en considérant A comme application linéaire).

Si $n = 2$, A est de rang 1, de trace 2, d'où 0 valeur propre simple, de vecteurs propres $\lambda(1, -1)$, et 2 valeur propre simple, de vecteurs propres $\mu(1, 1)$.

Passons au cas général, $n \geqslant 3$, en notant $\{e_1, ..., e_n\}$ la base canonique de $\mathbb{R}^n$.

La matrice A est de rang 2, l'image étant engendrée par les deux premiers vecteurs colonnes. Le noyau est de dimension $n-2$, donc 0 est valeur propre d'ordre $n-2$ au moins. Le sous-espace propre pour la valeur propre nulle est l'intersection des deux hyperplans d'équations $x_1 + x_n = 0$ et $x_1 + x_2 + ... + x_n = 0$, d'où $x_1 + x_n = 0$ et $x_2 + x_3 + ... + x_{n-1} = 0$.

Une base est formée des vecteurs $e_2 - e_i$, avec i variant de 3 à $n-1$, et de $e_1 - e_n$.

Le sous-espace F = Ker A est stable par F, donc $F^\perp$ est stable par l'adjoint de A qui est... A, donc les autres vecteurs propres sont à chercher dans $(\text{Ker } A)^\perp = \text{Im } A^* = \text{Im } A$.

Les vecteurs de Im A ont des coordonnées du type :

$(\alpha + \beta, \alpha, \alpha, ..., \alpha, \alpha + \beta)$, ou encore

$(a, b, b, ..., b, a)$, et on a un vecteur propre pour la valeur propre λ si on peut résoudre le système :

$$\begin{cases} 2a + (n-2)b = \lambda a \\ 2a = \lambda b \end{cases} \Leftrightarrow \begin{cases} (2-\lambda)a + (n-2)b = 0 \\ 2a - \lambda b = 0, \end{cases}$$

avec une solution non nulle pour ce système homogène, ce qui n'est possible que si λ vérifie :

$$\begin{vmatrix} 2-\lambda & n-2 \\ 2 & -\lambda \end{vmatrix} = \lambda^2 - 2\lambda + 4 - 2n = 0, \text{ ou encore :}$$

$(\lambda - 1)^2 = 2n - 3$, nombre positif car $n \geqslant 3$.

On trouve pour valeurs propres, chacune d'ordre 1, $\lambda = 1 + \sqrt{2n-3}$ et $\lambda' = 1 - \sqrt{2n-3}$, et en prenant $b = 2$ et $a = \lambda$, puis λ', on trouve des vecteurs propres associés.

4.47. Sur le corps des réels, A matrice symétrique réelle est diagonalisable.

Cas d'un corps quelconque.

On note $(C_j)_{1 \leqslant j \leqslant n}$, les vecteurs colonnes de A. Les $n-1$ premiers vecteurs colonnes sont proportionnels.

Supposons $a_1 = a_2 = \ldots = a_{n-1} = 0$: alors A est diagonale.

Si l'un des a_j, pour $j \leqslant n-1$, est non nul, A est de rang 2, (le mineur $\begin{vmatrix} 0 & a_j \\ a_j & a_n \end{vmatrix}$ obtenu avec $j^{\text{ième}}$ et $n^{\text{ième}}$ lignes et colonnes est non nul). On a déjà 0 valeur propre d'ordre $n-2$ au moins, et, si $\{e_1, \ldots, e_n\}$ est la base canonique, les vecteurs $a_i e_j - a_j e_i$, pour $1 \leqslant i \leqslant n-1$, $i \neq j$, forment une base de Ker A, j ayant été fixé tel que $a_j \neq 0$.

Quelles sont les autres valeurs propres ?

En fait : (λ valeur propre) $\Leftrightarrow \exists (x_1, \ldots, x_n) \neq 0$ tel que

$$\begin{cases} a_1 x_n = \lambda x_1 \\ a_2 x_n = \lambda x_2 \\ \text{----------} \\ a_i x_n = \lambda x_i \\ \text{----------} \\ a_{n-1} x_n = \lambda x_{n-1} \\ a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = \lambda x_n. \end{cases}$$

Si $\lambda = 0$, (avec existence de $a_j \neq 0$), on retrouve $x_n = 0$, et la relation $a_1 x_1 + \ldots + a_{n-1} x_{n-1} = 0$, donc on retrouve Ker A.

Si λ est valeur propre non nulle, on doit avoir $x_i = \dfrac{1}{\lambda} a_i x_n$, pour chaque $i \leqslant n-1$, et aussi :

$$\sum_{i=1}^{n-1} a_i \left(\frac{1}{\lambda} a_i\right) x_n + a_n x_n = \lambda x_n .$$

Comme on veut un n.uplet non nul, on doit avoir $x_n \neq 0$, donc λ doit vérifier l'équation $\lambda^2 - a_n\lambda - \sum_{j=1}^{n-1} (a_j)^2 = 0$.

Si $\sum_{j=1}^{n-1} (a_j)^2 = 0$, (c'est possible sur $\mathbb{C}$), on a un seul nombre non nul solution si $a_n \neq 0$, et aucun si $a_n = 0$. Or $\lambda \neq 0$ étant trouvé les relations déterminent un sous-espace propre de dimension 1, engendré par $(a_1, a_2, ..., a_{n-1}, \lambda)$.

On suppose toujours A de rang 2, donc il existe un a_j non nul, pour $j \leqslant n-1$.

1°) Donc avec $\sum_{j=1}^{n-1} (a_j)^2 = 0$, on a 0 valeur propre d'ordre $n-1$ ou n et un noyau de dimension $n-2$: A n'est pas diagonalisable.

2°) Si $\sum_{j=1}^{n-1} (a_j)^2 \neq 0$, 0 est valeur propre d'ordre $n-2$ et on a un sous-espace propre associé de dimension $n-2$. Le discriminant $\Delta = a_n^2 + 4 \sum_{j=1}^{n-1} (a_j)^2$ peut être ou non un carré dans le corps, (pensez à $\mathbb{Q}$).

a) Si ce n'est pas un carré : pas d'autres valeurs propres, A n'est pas diagonalisable.

b) Si $\Delta = 0$, on a une valeur propre non nulle, double, et une droite comme sous-espace propre : A n'est pas diagonalisable.

c) Si Δ est un carré non nul dans le corps K, on a deux valeurs propres non nulles distinctes et A est diagonalisable.

Finalement, A est diagonalisable si et seulement si :

$(a_1, a_2, ..., a_{n-1}) = 0$, ou

$(a_1, a_2, ..., a_{n-1}) \neq 0$ mais alors $\sum_{j=1}^{n-1} a_j^2 \neq 0$ et $\Delta = a_n^2 + 4 \sum_{j=1}^{n-1} (a_j)^2$ carré non nul dans le corps K.

On peut remarquer que cette condition est vérifiée sur $\mathbb{R}$.

4.48. On peut considérer la matrice A comme symétrique réelle, alors elle sera diagonalisable. De plus, la somme des coefficients de chaque ligne valant $a+b+c$, on a déjà $a+b+c$ valeur propre et $V = (1, 1, 1, 1)$ vecteur propre associé.

On peut alors chercher des vecteurs propres dans l'hyperplan orthogonal à V, d'équation $x+y+z+t = 0$, (diagonalisation en base orthonormée) et, un calcul rapide montre que :

$$\begin{pmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{pmatrix}\begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix} = (a-b-c)\begin{pmatrix} -1 \\ -1 \\ 1 \\ 1 \end{pmatrix};$$

$$\begin{pmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = (-a+b-c)\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix};$$

$$\begin{pmatrix} 0 & a & b & c \\ a & 0 & c & b \\ b & c & 0 & a \\ c & b & a & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = (-a-b+c)\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix}.$$

Les trois vecteurs trouvés sont indépendants : la matrice des composantes est :

$$\begin{pmatrix} -1 & 1 & 1 \\ -1 & -1 & -1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix},$$ et le mineur des trois premières lignes vaut $-1-1-1+1-1-1 = -4$.

Comme ils sont dans l'orthogonal de V, on a bien une base de vecteurs propres de A, que les valeurs propres trouvées $a+b+c$, $a-b-c$, $-a+b-c$ et $-a-b+c$ soient distinctes ou non.

De plus, n'ayant fait aucune hypothèse sur le corps en fait, ce résultat est valable sur un corps K quelconque, de caractéristique $\neq 2$.

4.49. Pour calculer le polynôme caractéristique de M, et tenir compte de la présence des a sous la diagonale, et des b au-dessus, on va introduire des x partout, d'où, en prenant $x = -a$ ou $x = -b$, une matrice devenue triangulaire.

On calcule donc :

$$D(x) = \begin{vmatrix} -\lambda+x & b+x & \cdots & b+x & b+x \\ a+x & -\lambda+x & \cdots & b+x & b+x \\ \vdots & \vdots & & \vdots & \vdots \\ & & & -\lambda+x & b+x \\ a+x & \cdots & \cdots & a+x & -\lambda+x \end{vmatrix}.$$

En retranchant la première colonne aux autres, les x disparaissent dans les $n-1$ dernières colonnes obtenues, donc en développant par rapport à la première colonne, on constate que $D(x)$ est une fonction affine en x, du type $\alpha x+\beta$.

Supposons $a \neq b$.

Pour $x = -a$, $D(-a)$ est un déterminant triangulaire valant $(-1)^n(a+\lambda)^n$, et de même $D(-b) = (-1)^n(b+\lambda)^n$.

Le système : $\begin{cases} -\alpha a+\beta = (-1)^n(a+\lambda)^n & \mid\ b \\ -\alpha b+\beta = (-1)^n(b+\lambda)^n & \mid\ -a \end{cases}$

conduit à : $\beta = (-1)^n \dfrac{b(a+\lambda)^n - a(b+\lambda)^n}{b-a}$ et comme le polynôme caractéristique de la matrice M est $\chi_M(\lambda) = D(0)$, seul β nous intéresse.

Pour $a \neq b$, on a donc $\chi_M(\lambda) = \dfrac{(-1)^n}{(b-a)}\,(b(a+\lambda)^n - a(\lambda+b)^n)$.

Si $a = b$, avec J matrice de terme général 1, de rang 1 et de trace n, de noyau l'hyperplan H d'équation $x_1 + \ldots + x_n = 0$, de vecteur propre pour la valeur propre n, $V = (1, \ldots, 1)$, on peut conclure pour $M = aJ - aI_n$: les valeurs propres de M sont $-a$, d'ordre $n-1$, de sous-espace propre l'hyperplan H, et $(n-1)a$, d'ordre 1, de vecteur propre V, ceci pour $a \neq 0$ car $a = b = 0$ correspond à la matrice nulle.

Dans le cas $a = b$, M est diagonalisable.

Revenons au cas $a \neq b$.

Si a, (ou b) est nul, (un seul car $a \neq b$), M est triangulaire, de rang $n-1$, avec 0 pour seule valeur propre : elle n'est pas diagonalisable. Si $a = 0$, $V = (1, 0, \ldots, 0)$ engendre le noyau, et si $b = 0$, c'est $W = (0, \ldots, 0, 1)$ qui joue ce rôle.

On suppose donc $a \neq b$ *et* $ab \neq 0$.

Les valeurs propres vérifient la relation $\left(\dfrac{\lambda+a}{\lambda+b}\right)^n = \dfrac{a}{b}$, ($\lambda = -b$ est exclue car il faudrait $b(a-b)^n = 0$).

Soit $z_1, ..., z_n$ les n racines $n^{\text{ième}}$, distinctes, de $\frac{a}{b}$.

Comme $a \neq b$, chaque z_k est différent de 1, l'équation $\frac{\lambda_k + a}{\lambda_k + b} = z_k$, donne $\lambda_k(1 - z_k) = bz_k - a$, d'où : $\lambda_k = \frac{bz_k - a}{1 - z_k}$, ces valeurs propres étant distinctes car il est connu, (ou facile à vérifier), que la fonction homographique $z \rightsquigarrow \frac{bz - a}{1 - z}$ établit une bijection de $\mathbb{C} - \{1\}$ sur $\mathbb{C} - \{-b\}$.

La matrice M est donc diagonalisable si $a \neq b$ et $ab \neq 0$.

Soient $(x_1, ..., x_n)$ les coordonnées d'un vecteur propre V_k pour la valeur propre λ_k. Ces coordonnées doivent vérifier le système des n équations L_i du type :

$$L_i : ax_1 + ... + ax_{i-1} - \lambda_k x_i + bx_{i+1} + ... + bx_n = 0.$$

Si on garde L_n et que l'on forme les équations $L_1 - L_2$; $L_2 - L_3$; ..., $L_{n-1} - L_n$, on obtient :

$$-(a + \lambda_k)x_1 + (b + \lambda_k)x_2 = 0$$
$$-(a + \lambda_k)x_2 + (b + \lambda_k)x_3 = 0$$
$$\text{- - - - - - - - - - - - - - - - - - -}$$
$$-(a + \lambda_k)x_{n-1} + (b + \lambda_k)x_n = 0,$$

d'où $x_2 = \frac{a + \lambda_k}{b + \lambda_k} x_1 = z_k x_1$, puis $x_3 = z_k x_2 = (z_k)^2 x_1$ et finalement $x_n = (z_k)^{n-1} x_1$.

La droite vectorielle sous-espace propre pour la valeur propre λ_k est donc engendrée par $V_k = (1, z_k, z_k^2, ..., z_k^{n-1})$.

Les valeurs propres étant distinctes, la matrice M est diagonalisable dans ce cas, $(a \neq b, ab \neq 0)$.

4.50. Un projecteur p est un opérateur linéaire sur E caractérisé par la relation $p^2 = p$. Il annule le polynôme scindé à racines simples $X^2 - X$, donc il est diagonalisable avec 1 et 0 pour seules valeurs propres et sa trace est la dimension de son image, donc c'est son rang.

Si $p_1 + p_2 + ... + p_k = q$ est un projecteur, la trace étant linéaire, on a :

$$\text{trace}\,(q) = \text{rang}\,(q) = \sum_{j=1}^{k} \text{trace}\,(p_k) = \sum_{j=1}^{k} \text{rang}\,(p_j)\,.$$

Soit alors $y = q(x) = \sum_{j=1}^{k} p_j(x)$ un élément de $\text{Im}\,(q)$, il est dans la somme des $\text{Im}\,(p_j)$, et l'égalité $\dim\,(\text{Im}\,q) = \sum_{j=1}^{k} \dim\,(\text{Im}\,p_j)$ prouve que la somme des $\text{Im}\,(p_j)$ est directe, car en notant $\mathscr{B}_j$ une base de $\text{Im}\,(p_j)$, la famille $\bigcup_{j=1}^{k} \mathscr{B}_j$ est génératrice de $\text{Im}\,q$, et libre, sinon elle contiendrait strictement une base et alors on aurait :

$$\dim\,(\text{Im}\,q) < \sum_{j=1}^{k} \text{card}\,(\mathscr{B}_j)\,.$$

On va alors justifier, par récurrence sur k, le résultat. Si $q = p_1 + p_2$ est un projecteur, on a $q^2 = q$, donc : $p_1^2 + p_1p_2 + p_2p_1 + p_2^2 = p_1 + p_2$, d'où $p_1p_2 = -p_2p_1$.

Mais $y = p_1p_2(x) \in \text{Im}\,p_1$ et comme $y = -p_2p_1(x)$, on a aussi $y \in \text{Im}\,p_2$.

Comme $\text{Im}\,q = \text{Im}\,p_1 \oplus \text{Im}\,p_2$, il en résulte la nullité de y, d'où $p_1p_2 = p_2p_1 = 0$.

Supposons le résultat obtenu à l'ordre $k-1$, et soient $p_1, ..., p_k$ des projecteurs tels que $q = p_1 + ... + p_k$ soit un projecteur. En fait $p = q - p_k$ est encore un projecteur, car $p^2 = q - qp_k - p_kq + p_k$, et, comme $\text{Im}\,p_k \subset \text{Im}\,q$, pour tout x de E, $p_k(x) \in \text{Im}\,q$, sous-espace sur lequel q induit l'identité, d'où $q(p_k(x)) = p_k(x)$; mais on a aussi $p_kq = p_k$ car, si $x \in \text{Im}\,q$, $q(x) = x$, et si $x \in \text{Ker}\,q$, on a $q(x) = p_1(x) + ... + p_k(x) = 0$, avec $q(\text{E}) = \bigoplus_{j=1}^{k} p_j(\text{E})$, donc chaque $p_j(x)$ est nul, en particulier $p_k(x) = 0$, donc $p_kq(x) = 0 = p_k(x)$ sur $\text{Ker}\,q$.

Comme $\text{E} = \text{Ker}\,q \oplus \text{Im}\,q$, on a bien $p_kq = p_k$, et l'égalité $p^2 = q - p_k - p_k + p_k = q - p_k = p$.

Mais alors, l'hypothèse de récurrence s'applique au projecteur p, somme des p_j pour $1 \leqslant j \leqslant k-1$ et donne la nullité des $p_i p_j$ pour $i \neq j$, $1 \leqslant i, j \leqslant k-1$.

Le pauvre indice k semble exclu mais, (symétrie des rôles joués) pour avoir $p_i p_k = 0$, avec $i \neq k$, il suffit de choisir un troisième larron p_j, ($j \notin \{i, k\}$) et de considérer cette fois $q - p_j$ comme projecteur.

Donc pour $i \neq j$, sans autre restriction, on a $p_i p_j = 0$.

4.51. Soit A inversible, on aura $f(\mathrm{I}_n) = f(\mathrm{A})f(\mathrm{A}^{-1})$, et si on suppose $f(\mathrm{A}) = 0$, il en résulte que $f(\mathrm{I}_n) = 0$, mais alors f est constante, nulle, car pour tout B de $\mathscr{M}_n(\mathbb{C})$ on aura $f(\mathrm{B}) = f(\mathrm{I}_n\mathrm{B}) = f(\mathrm{I}_n)f(\mathrm{B}) = 0$. Ceci est exclu, donc A inversible implique $f(\mathrm{A}) \neq 0$.

Si A est non inversible, si elle est de rang r, elle est équivalente, (pas semblable pour une fois) à une matrice bloc : $\mathrm{B} = \begin{pmatrix} 0 & \mathrm{I}_r \\ 0 & 0 \end{pmatrix}$, I_r étant la matrice identité de $\mathscr{M}_r(\mathbb{C})$.

Il suffit pour cela de prendre dans $\mathrm{E} = \mathbb{C}^n$, un supplémentaire H de Ker A, (on assimile A et l'endomorphisme qu'il représente dans $\mathbb{C}^n$ rapporté à sa base canonique). Alors A induit un isomorphisme de H sur Im A.

En prenant une base $e_1, \ldots, e_{n-r}$ de Ker A, complétée par $e_{n-r+1}, \ldots, e_n$, base de H, d'où une base $\mathscr{B}$ de $\mathbb{C}^n$ au départ ; puis une base $\mathscr{C}$ de $\mathbb{C}^n$ espace d'arrivée, formée des $\mathrm{A}(e_{n-r+j}) = \varepsilon_j$, pour $1 \leqslant j \leqslant r$, complétée de façon quelconque, la matrice de A, dans les bases $\mathscr{B}$ et $\mathscr{C}$, est bien B.

Un calcul classique montre que $\mathrm{B}^r = 0$. Avec P et Q régulières telles que $\mathrm{B} = \mathrm{PAQ}$, on aura $f(\mathrm{B}) = f(\mathrm{P})f(\mathrm{A})f(\mathrm{Q})$, avec $f(\mathrm{P})$ et $f(\mathrm{Q})$ non nuls d'après la première partie.

On a alors $f(\mathrm{B}^r) = f(0)$, et $f(0) = 0$, car, f n'étant pas constante, si M et N sont dans $\mathscr{M}_n(\mathbb{C})$, avec $f(\mathrm{M}) \neq f(\mathrm{N})$, comme on a :

$f(0) = f(0\mathrm{M}) = f(0)f(\mathrm{M}) = f(0\mathrm{N}) = f(0)f(\mathrm{N})$, il vient, dans $\mathbb{C}$,

$f(0)(f(\mathrm{M}) - f(\mathrm{N})) = 0$, d'où $f(0) = 0$.

Donc $f(B^r) = 0 = (f(B))^r$, d'où $f(B)$ nul et finalement $f(A)$ nul.

On a bien justifié $f(A) = 0 \Leftrightarrow A$ non inversible.

4.52. Si G et de cardinal p, tout élément a de G vérifie l'égalité $a^p = e$, (e neutre dans G), d'où $(f(a))^p = f(a^p) = f(e) = \mathrm{id}_E$: l'endomorphisme $A = f(a)$ de l'espace vectoriel E, vérifie l'égalité $A^p = \mathrm{id}_E$. Il annule le polynôme scindé à racines simples $X^p - 1$, donc *il est diagonalisable,* avec pour valeurs propres des racines $p^{\text{ième}}$ de l'unité.

Mais, pour $\lambda_j = e^{i\theta_j}$, on a $\lambda_j^{-1} = e^{-i\theta_j} = \overline{\lambda_j}$, donc avec $f(a)$ semblable à diag $(\lambda_1, ..., \lambda_n)$, les λ_j étant des racines $p^{\text{ième}}$ de l'unité, (distinctes ou non), on aura $f(a^{-1}) = (f(a))^{-1}$ semblable à diag $(\lambda_1^{-1}, ..., \lambda_n^{-1})$ donc à diag $(\overline{\lambda_1}, ..., \overline{\lambda_n})$, et, les traces étant stables par passage aux matrices semblables, on obtient :

$$\varphi(a^{-1}) = \text{trace}\,(f(a^{-1})) = \sum_{j=1}^{n} \overline{\lambda_j} = \overline{\text{trace}\,(f(a))} = \overline{\varphi(a)}.$$

4.53. Sur $\mathbb{R}$, la matrice A, symétrique réelle est diagonalisable. Pour la diagonaliser, on est incité à considérer $B = A - I_n$, tout vecteur propre de A en étant un de B, et réciproquement.

Soit $\{e_1, ..., e_n\}$ la base canonique de $\mathbb{R}^n$. Dans cette base $\mathscr{B}$, la matrice B est :

$$B = \begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \\ 1 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

, de rang 2, donc 0 est valeur propre d'ordre $n-2$ au moins, de sous-espace propre Ker (B), sous-espace de dimension $n-2$, de base les $e_2 - e_j$, pour $j = 3, 4, ..., n$.

Par ailleurs, soit le vecteur $a = e_2 + e_3 + ... + e_n$, et f l'endomorphisme de $\mathbb{R}^n$ de matrice B dans la base $\mathscr{B}$.

On a $f(e_1) = e_2 + e_3 + \ldots + e_n = a$, et

$$f(a) = \sum_{j=2}^{n} f(e_j) = (n-1)e_1,$$

donc F = Vect (e_1, a) est stable par f. Si f est diagonalisable, l'endomorphisme induit par f sur F, (qui est de dimension 2) doit être diagonalisable. Or la matrice V de cet endomorphisme induit, dans la base $\{e_1, a\}$ est : $V = \begin{pmatrix} 0 & n-1 \\ 1 & 0 \end{pmatrix}$, de polynôme caractéristique $\lambda^2 - (n-1) = 0$, de valeurs propres distinctes $\pm\sqrt{n-1}$, (on est sur $\mathbb{R}$, et on suppose $n \geqslant 2$), de vecteurs propres $xe_1 + ya$ tels que $-\varepsilon\sqrt{n-1}x + (n-1)y = 0$, d'où $x = \varepsilon\sqrt{n-1}$ et $y = 1$ par exemple, avec $\varepsilon = 1$ ou -1.

En conclusion, sur $\mathbb{R}^n$, avec $n \geqslant 2$, les valeurs propres de A sont :

$1 + \sqrt{n-1}$ et $1 - \sqrt{n-1}$, simples, de vecteurs propres associés $\varepsilon\sqrt{n-1}e_1 + e_2 + e_3 + \ldots + e_n$, ($\varepsilon = 1$ ou -1), et : 1 valeur propre d'ordre $n-2$, de sous-espace propre associé ayant pour base les $e_2 - e_j$, $j = 3, 4, \ldots, n$.

Que peut-on dire si on remplace $\mathbb{R}$ par un corps K quelconque ?

Tout ce qui précède, jusqu'à l'introduction de $\pm\sqrt{n-1}$, est valable.

Si A est diagonalisable, f l'est sur F, or f a pour polynôme caractéristique $\lambda^2 - (n-1) = 0$.

Si $n-1$ n'est pas un carré dans K, (par exemple K = Q et $n = 6$, f n'est pas diagonalisable, donc A non plus.

Si $n-1$ est un carré dans K, posons $n-1 = w^2$. Si $w \neq 0$, on a comme dans le cas réel deux valeurs propres non nulles de f, d'où une diagonalisation de A.

Mais si $n-1 = 0$ dans K, (K = $\mathbb{Z}/p\mathbb{Z}$, avec p premier et $n = p+1$ par exemple) on ne peut plus conclure de cette façon. Mais B reste de rang 2, et on va voir que dans ce cas le polynôme caractéristique de B se réduit à $(-\lambda)^n = 0$, d'où 0 seule valeur propre mais dim (Ker B) non égale à n, donc B sera non diagonalisable, (et A non plus).

On a :

$$\chi_B(\lambda) = \begin{vmatrix} -\lambda & 1 & \cdots & 1 \\ 1 & -\lambda & \cdots & 0 \\ 1 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 1 & 0 & \cdots & -\lambda \end{vmatrix}$$

, que l'on développe par rapport à la première colonne, en mettant à part le terme de la première ligne.

On a :

$$\chi_B(\lambda) = (-\lambda)^n + \sum_{i=2}^{n} (-1)^{i+1} \left|\begin{array}{cccc|ccc} 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ -\lambda & 0 & & 0 & & & \\ 0 & -\lambda & \ddots & \vdots & & 0 & \\ & & & -\lambda \; 0 & & & \\ \hline & & & & -\lambda & & 0 \\ & 0 & & & & \ddots & \\ & & & & 0 & & -\lambda \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} i-1 \text{ lignes} \\ \left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} n-i \text{ lignes} \end{array}$$

$$= (-\lambda)^n + \sum_{i=2}^{n} (-1)^{i+1} (-\lambda)^{n-i} \begin{vmatrix} 1 & 1 & \cdots & 1 & 1 \\ -\lambda & 0 & & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & & 0 & 0 \\ 0 & 0 & \cdots & -\lambda & 0 \end{vmatrix}.$$

Le déterminant d'ordre $i-1$ qui reste à calculer se développe d'abord par rapport à la dernière colonne, et on obtient :

$$(-1)^{i-1+1} \underbrace{\begin{vmatrix} -\lambda & & 0 \\ & \ddots & \\ 0 & & -\lambda \end{vmatrix}}_{i-2} = (-1)^i (-\lambda)^{i-2} = \lambda^{i-2},$$

donc $\chi_B(\lambda) = (-\lambda)^n + \sum_{i=2}^{n} (-1)^{n-1}\lambda^{n-2}$

$= (-1)^n(\lambda^n - (n-1)\lambda^{n-2})$,

avec, dans le cas qui nous intéresse, $n-1 = 0$.

En conclusion, A est diagonalisable sur $\mathbb{R}$, ou sur un corps K dans lequel $n-1$ est un carré non nul. J'espère ne pas m'être trompé.

4.54. Les polynômes caractéristiques de M et N sont scindés sur $\mathbb{C}$, et ces matrices sont trigonalisables.

a) Si M et N commutent, il existe une base commune de trigonalisation, donc il existe P dans $GL_n(\mathbb{C})$ telle que $P^{-1}MP = U$ et $P^{-1}NP = V$ soient triangulaires supérieures, avec $\alpha_1 \ldots \alpha_n$ et $\beta_1 \ldots \beta_n$ pour éléments diagonaux.

Supposons que $f(X, Y) = \sum_{i,j} \lambda_{ij} X^i Y^j$, les coefficients λ_{ij} étant presque tous nuls.

Comme $(P^{-1}MP)^i(P^{-1}NP)^j = P^{-1}M^iN^jP$, (formule facile à vérifier si i et j sont $\geqslant 1$, car les $P^{-1}P$ intermédiaires disparaissent, mais formule valable aussi pour i ou j nul), on a :

$$P^{-1}f(M, N)P = \sum_{i,j} \lambda_{ij}(P^{-1}MP)^i(P^{-1}NP)^j$$

$$= \sum_{i,j} \lambda_{ij} U^i V^j = f(U, V),$$

mais, par produit de matrices triangulaires supérieures, puis combinaison linéaire, on a $T = P^{-1}f(M, N)P$ qui est aussi triangulaire supérieure, avec sur la diagonale, en $k^{\text{ième}}$ position, $\sum_{i,j} \lambda_{ij}(\alpha_k)^i(\beta_k)^j = f(\alpha_k, \beta_k)$.

Comme T et $f(M, N)$ sont semblables, toute valeur propre γ de $f(M, N)$ est donc du type $f(\alpha, \beta)$, avec α et β valeurs propres respectivement de M et de N.

b) Soit ω une racine $q^{\text{ième}}$ de l'unité, telle que $MN = \omega NM$, avec N inversible, ou encore $M = N(\omega M)N^{-1}$: les matrices M et ωM sont semblables.

Si λ_1 est valeur propre de M d'ordre p_1, M et ωM ayant même spectre, $\omega\lambda_1$ sera valeur propre également d'ordre p_1 de M, car valeur propre d'ordre p_1 de ωM, (trigonaliser M pour le voir).

Si ω, racine $q^{\text{ième}}$ est d'ordre r, (r diviseur de q en fait, et $r = q$ si ω est racine $q^{\text{ième}}$ primitive de l'unité), on aura de même $\omega^2\lambda_1, ..., \omega^{r-1}\lambda_1$ chacune valeur propre d'ordre p_1 de M.

Si on a ainsi toutes les valeurs propres de M, c'est terminé, sinon, à partir d'une autre valeur propre λ_2, d'ordre p_2, on récupère $\lambda_2, \omega\lambda_2, ..., \omega^{r-1}\lambda_2$, chacune de ces valeurs propres étant d'ordre p_2. Et on recommence jusqu'à obtention de toutes, (nombre fini), les valeurs propres.

Finalement, si ω est racine $q^{\text{ième}}$ de l'unité d'ordre r, (ou racine $r^{\text{ième}}$ primitive de l'unité), il existe $\lambda_1, ..., \lambda_k$ valeurs propres distinctes de M, de multiplicités $p_1, ..., p_k$, telles que les valeurs propres de M soient les éléments des k paquets $\{\lambda_j, \omega\lambda_j, ..., \omega^{r-1}\lambda_j\}$, chacune d'ordre p_j, j variant de 1 à k.

4.55. Soit $\mathscr{B} = \{e_1, ..., e_n\}$ la base canonique de $\mathbb{C}^n$ et u l'endomorphisme de matrice M dans cette base. On a : $u(e_{n-i+1}) = a_i e_i$ et $u(e_i) = a_{n-i+1}e_{n-i+1}$, donc le sous-espace vectoriel vect (e_i, e_{n-i+1}) est stable par u. Il est de dimension 2 sauf si $i = n-i+1$, ce qui ne se produit que si n est impair, d'où l'existence de deux cas.

Si n est pair, posons $n = 2p$.

Dans ce cas, $\mathbb{C}^{2p}$ est somme directe des p plans vectoriels $P_j = \text{Vect}\,(e_j, e_{n-j+1})$, pour $1 \leqslant j \leqslant p$, qui sont stables par u, et $\tilde{u}_j$ induit par u sur P_j a pour matrice : $A_j = \begin{pmatrix} 0 & a_j \\ a_{n-j+1} & 0 \end{pmatrix}$, de polynôme caractéristique : $\lambda^2 - a_j a_{n-j+1}$, dans la base $\{e_j, e_{n-j+1}\}$.

1°) Si pour chaque j, $a_j a_{n-j+1} \neq 0$, on a deux valeurs propres distinctes pour $\tilde{u}_j$, qui est donc diagonalisable, d'où u diagonalisable.

2°) Si l'un des deux nombres a_j, a_{n-j+1} est nul, mais pas les deux, $\tilde{u}_j$ n'a que 0 pour valeur propre double en étant de rang 1, donc n'est pas diagonalisable, et *a fortiori* u ne l'est pas, (stabilité des plans P_j oblige).

3°) Si lorsque $a_j = 0$ on a aussi $a_{n-j+1} = 0$, $\tilde{u}_j = 0$ est diagonalisable.

Donc M est diagonalisable si et seulement si lorsqu'il existe un a_j nul, on a aussi $a_{n-j+1} = 0$, ceci pour $n = 2p$.

Si n est impair, $n = 2p+1$, alors $\mathbb{C}^n = \left(\bigoplus_{j=1}^{p} P_j\right) \oplus \mathbb{C}e_{p+1}$, avec e_{p+1} vecteur propre de u pour la valeur propre a_{p+1}, donc la condition de diagonalisation est inchangée car, si $a_{p+1} = 0$, on a aussi $a_{2p+1-p-1+1} = a_{p+1} = 0$.

Si M *a au plus un terme non nul dans chaque ligne et chaque colonne,* il existe une permutation σ de $\{1, ..., n\}$ telle que $u(e_j) = a_{\sigma(j)}e_{\sigma(j)}$.

On décompose σ en un produit $\sigma_1 \circ \sigma_2 \circ ... \circ \sigma_r$ de cycles, le cycle σ_k étant du type $j_1 \rightsquigarrow j_2 \rightsquigarrow j_3 \rightsquigarrow ... \rightsquigarrow j_p \rightsquigarrow j_1$.

Le sous-espace vectoriel $F_k = \text{Vect}\{e_{j_1}, ..., e_{j_p}\}$, de dimension p, est alors stable par u, et $E = \bigoplus_{k=1}^{r} F_k$, les cycles portant sur des familles d'indices formant une partition de $\{1, ..., n\}$.

On a déjà (u diagonalisable) $\Leftrightarrow$ (chaque $\tilde{u}_k$ induit par u sur F_k est diagonalisable).

Or $\tilde{u}_k(e_{j_1}) = a_{j_2}e_{j_2}$ d'où $\tilde{u}_k^2(e_{j_1}) = a_{j_2}\tilde{u}_k(e_{j_2})$,

$= a_{j_2}a_{j_3}e_{j_3}$

et on obtient ainsi l'égalité $(\tilde{u}_k)^p(e_{j_1}) = a_{j_1}a_{j_2} ... a_{j_p}(e_{j_1})$, relation vérifiée aussi pour $e_{j_2}, ..., e_{j_p}$ d'où l'égalité : $(\tilde{u}_k)^p = a_{j_1} ... a_{j_p}\text{id}_{F_k}$.

Mais alors, si tous les a_{j_s} sont non nuls, $\tilde{u}_k$ annule un polynôme scindé à racines simples, donc est diagonalisable.

Si l'un des a_{j_s} est nul, mais pas tous, 0 est seule valeur propre de $\tilde{u}_k$, qui est de rang $\geqslant 1$, donc non diagonalisable.

Si tous les a_{j_s} sont nuls, $\tilde{u}_k = 0$ est diagonalisable.

Finalement, u est diagonalisable si et seulement si, dans la décomposition de σ en cycles, lorsque l'un des coefficients a_{j_s} intervenant pour ce cycle est nul, tous les coefficients intervenant sont nuls.

On peut remarquer qu'alors σ_k peut se décomposer en cycles de longueur 1, car $u(e_{j_1}) = 0 = 0 \cdot e_{j_1}$: on peut poser $\sigma(j_1) = j_1$, et de même $\sigma(j_s) = j_s$ pour chaque indice de ce cycle.

4.56. Notons $\alpha_{ij} = 0$ ou 1, le terme général de la matrice A. Comme trace A = 0 = somme d'entiers, on a chaque $\alpha_{ii} = 0$. Puis A symétrique donne $\alpha_{ij} = \alpha_{ji}$.

a) Le terme diagonal, dans la relation 1, sera tel que : $\sum_{k=1}^{n} \alpha_{ik}\alpha_{ki} + \alpha_{ii} - (d-1) = 1$, soit compte tenu du préambule :

$$\sum_{k=1}^{n} (\alpha_{ik})^2 - d + 1 = 1.$$

Or $\alpha_{ik} = 1$ ou 0 donc $\alpha_{ik}^2 = \alpha_{ik}$, d'où l'égalité : $\sum_{k=1}^{n} \alpha_{ik} \cdot 1 = d$, ce qui est la traduction de l'égalité des matrices colonnes AU et dU.

Mais alors $A^2U = A(dU) = d(AU) = d^2U$, d'où, grâce à la relation (1), l'égalité :

$$d^2U + dU - (d-1)U = nU,$$

et, le vecteur colonne U n'étant pas nul, l'égalité $d^2 + 1 = n$.

b) Si λ est valeur propre de A, il existe un vecteur colonne X, non nul, tel que $AX = \lambda X$, d'où l'égalité :

$$(\lambda^2 + \lambda - d + 1)X = JX.$$

Or JX est le vecteur colonne de terme constant $x_1 + x_2 + ... + x_n$, donc le premier membre est un vecteur colonne constant.

Si $\lambda^2 + \lambda - d + 1 \neq 0$, c'est que X est proportionnel à U, mais on a vu que AU = dU donc $\lambda = d$.

Sinon, $\lambda \in \{a, b\}$ ensemble des zéros de $x^2 + x - (d-1)$, et dans ce cas X sera dans l'hyperplan d'équation $x_1 + ... + x_n = 0$.

Dans tous les cas, le spectre de A est dans $\{a, b, d\}$.

c) L'équation $x^2 + x - (d-1) = 0$ a pour discriminant $\Delta = 1 + 4d - 4$, avec $d \geqslant 1$, d'où $\Delta > 0$, et deux zéros distincts $a = -\frac{1}{2} + \frac{\sqrt{\Delta}}{2}$ et $b = -\frac{1}{2} - \frac{\sqrt{\Delta}}{2}$.

De plus d est différent de a et b car $d^2 + d - d + 1 = d^2 + 1$ est non nul.

Notons α, β et γ les multiplicités respectives de a, b et d valeurs propres de A, symétrique réelle donc diagonalisable.

On sait que la trace de A est nulle, donc on a :

$$-\frac{(\alpha+\beta)}{2}+(\alpha-\beta)\frac{\sqrt{\Delta}}{2}+d\gamma = 0,$$

avec $\gamma \geqslant 1$, car U est vecteur propre de A pour la valeur propre d. De plus, au b), on a vu que pour la valeur propre $\lambda = d$, différente de a et b, les vecteurs propres sont proportionnels à U, donc la multiplicité γ de d est 1, (toujours parce que A est diagonalisable), et on obtient la relation :

$$(2)\quad -(\alpha+\beta)+(\alpha-\beta)\sqrt{\Delta}+2d = 0.$$

Si $\alpha = \beta$, il reste $-2\alpha+2d = 0$, donc $\alpha = d$, et $n = \alpha+\beta+\gamma = \alpha+\beta+1 = 2\alpha+1 = 2d+1$, joint à $n = d^2+1$ conduit à $d^2 = 2d$ d'où $d = 2$.

Si $\alpha \neq \beta$, compte tenu de (2) on a $\sqrt{\Delta} = \sqrt{4d-3}$ dans $\mathbb{Q}_*^+$, donc $4d-3$ est égal à $\frac{p^2}{q^2}$, avec p et q entiers non nuls premiers entre eux, mais, $4d-3$ est entier, donc $q = 1$ et $4d-3$ est du type p^2.

Mais alors, $n = d^2+1 = \frac{1}{16}(p^2+3)^2+1$, et comme $\alpha+\beta+1 = n$, on a $\alpha+\beta = \frac{1}{16}(p^2+3)^2$, et la relation (2) donne :

$$(\alpha-\beta)p = (\alpha+\beta)-2d = \frac{1}{16}(p^2+3)^2-\frac{1}{2}(p^2+3), \quad \text{d'où le système :}$$

$$\begin{cases} \alpha p+\beta p = \frac{1}{16}p(p^2+3)^2 \\ \alpha p-\beta p = \frac{1}{16}(p^2+3)(p^2+3-8) = \frac{1}{16}(p^2+3)(p^2-5) \end{cases}$$

qui conduit à :

$$\begin{cases} \alpha p = \frac{1}{32}(p^2+3)(p^3+p^2+3p-5) \\ \beta p = \frac{1}{32}(p^2+3)(p^3-p^2+3p+5). \end{cases}$$

Mais comme α et β sont des entiers, on doit avoir 32α et 32β entiers d'où 15 divisible par p.

Avec $p = 1, 3, 5$ et 15, on obtient $4d-3 = p^2 = 1, 9, 25, 225$, d'où $4d = 4, 12, 28, 228$, donc d doit appartenir à l'ensemble $\{1, 3, 7, 57\} \cup \{2\}$, 2 déjà trouvé avant.

On doit bien choisir d dans $\{1, 2, 3, 7, 57\}$.

Si on prend $d = 1$, on a $n = d^2 + 1 = 2$, d'où A symétrique avec des 0 sur la diagonale : on a deux choix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. La relation $AU = U$ exclut $A = 0$, il reste $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ qui vérifie bien l'égalité $A^2 + A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = J$.

Avec $d = 2$, on a $n = 5$.

La relation $AU = dU = 2U$, impose la présence d'exactement deux 1 par ligne et pas sur la diagonale.

Soit ensuite quatre entiers distincts dans $\{1, 2, 3, 4\}$, notés i_1, i_2, j_1 et j_2.

On suppose que : $a_{i_1 j_1} = a_{i_1 j_2} = 1$ et $a_{i_2 j_1} = a_{i_2 j_2} = 1$.

Notons k le cinquième indice. On a $a_{i_1 i_1} = a_{i_1 i_2} = a_{i_1 k} = 0$, mais aussi $a_{i_2 i_2} = a_{i_2 i_1} = a_{i_2 k} = 0$, (deux 1 par ligne), donc par symétrie : $a_{k i_1} = a_{k i_2} = 0$.

Par ailleurs $a_{j_1 i_1} = a_{j_1 i_2} = 1$, (symétrie), implique $a_{j_1 k} = 0$ d'où $a_{k j_1} = 0$, (symétrie), et de même $a_{k j_2} = 0$.

Mais alors sur la $k^{\text{ième}}$ ligne, on aurait quatre termes nuls : la somme des coefficients ne peut donner 2 : la configuration de départ est exclue.

On peut alors examiner les différents cas.

Si la première ligne est $L_1 = 0\,1\,1\,0\,0$, on a déjà la colonne C_1.

Sur la ligne L_2, qui commence par 1 0, on a *a priori* trois emplacements pour le deuxième 1 mais 1 0 1 0 0 est exclu, car par symétrie on aurait :

$A = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & & \\ 0 & 0 & & 0 & \\ 0 & 0 & & & 0 \end{pmatrix}$, d'où, (deux 1 en ligne 3), une troisième ligne $L_3 = 1\,1\,0\,0\,0$, une colonne $C_3 = 1, 1, 0, 0, 0$ par symétrie, et une ligne L_4 avec quatre zéro : c'est exclu.

On constate ainsi qu'il n'y a que 12 matrices qui conviennent et qui, (de la patience !) vérifient bien la relation $A^2 + A - I_5 = J$, vérification

à faire car on n'a pas procédé par équivalence, mais qui s'effectue en remarquant qu'en notant C_j les vecteurs colonnes de A, symétrique, cela revient, avec le produit scalaire euclidien canonique, à vérifier que $\langle C_i, C_j \rangle + a_{ij} = 1$ si $1 \leqslant i < j \leqslant n$ et $= 2$ si $i = j$.

Voici les matrices :

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

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

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

4.57. Le rang de A peut s'obtenir à partir du rang des vecteurs colonnes, (on pense vecteurs), ou des vecteurs lignes, (on pense équations linéaires).

Les hypothèses sur A incitent à considérer $A + {}^tA$, matrice avec des $0 = 2a_{ii}$ sur la diagonale, et des 1 partout ailleurs, ou encore, si J est la matrice carrée avec des 1 partout cette fois, on a :

$$A + {}^tA = J - I_n.$$

Cherchons donc à résoudre le système homogène de n équations à n inconnues : $AX = 0$, avec X vecteur colonne des x_i, $1 \leqslant i \leqslant n$.

Pour faire intervenir l'hypothèse, on considère aussi ${}^tX{}^tA$, mais alors, qui prendre, $AX = 0$ ou ${}^tX{}^tA = 0$?

Et pourquoi pas, (pour avoir les deux), ${}^tX(A + {}^tA)X$. On a ${}^tX(AX) + ({}^tX{}^tA)X = {}^tXJX - {}^tXX$.

Considérons alors, toutes les lignes de J étant égales, le système de $n+1$ équations à n inconnues, homogène :

$$S \begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + \ldots + a_{2n}x_n = 0 \\ \text{- - - - - - - - - - - - - - - -} \\ a_{n1}x_1 + \ldots + a_{nn}x_n = 0 \\ x_1 + x_2 + \ldots + x_n = 0. \end{cases}$$

Si X vérifie S, on a $AX = 0$ donc ${}^tX{}^tA = 0$ aussi, mais alors ${}^tX(JX) - {}^tXX = 0$, or $JX = 0$, (c'est la dernière équation de S), d'où ${}^tXX = \sum_{j=1}^{n} (x_j)^2 = 0$, et, sur $\mathbb{R}$, ceci donne $X = 0$.

Notre système S est de rang n, (merci Rouché Fontené) donc les n premières équations sont bien obligées de donner un système de rang $n-1$, sinon la seule dernière équation ne suffirait pas pour donner un rang n.

4.58. Un automorphisme A de $E = K^n$, tel que $A^2 = I_n$, est une symétrie. Cet automorphisme annule le polynôme $X^2 - 1 = 0$, scindé à racines simples, 1 et -1, ($1 \neq -1$ car la caractéristique de K n'est pas 2), donc A est diagonalisable et caractérisé par la donnée des deux sous-espaces propres :

$F = \{v \in E, A(v) = v\}$ et $G = \{v \in E ; A(v) = -v\}$, supplémentaires dans E.

Si on note p la dimension de F, et q le cardinal de K, on caractérise toutes les symétries en cherchant, quand p varie de 0 à n, le nombre de sous-espaces vectoriels F de dimension p, et pour chaque choix de F, en choisissant G, supplémentaire de F.

Pour $p = 0$, on n'a pas le choix : $F = \{0\}$ et $G = E$, il en est de même pour $p = n$, ce qui impose $F = E$ et $G = \{0\}$.

Soit alors p, avec $1 \leqslant p \leqslant n-1$.

Pour choisir F, il faut s'en donner une base, et pour cela, en notant $\{e_1, \ldots, e_p\}$ une telle base, il faut :

choisir e_1 non nul : il y a $q^n - 1$ choix, (card $E = q^n$) ;

choisir e_2 indépendant de e_1 : il y a $q^n - q$ choix ;

choisir e_3 non dans le plan Vect (e_1, e_2) : il y a $q^n - q^2$ choix ;

et enfin, choisir e_p indépendant de $e_1, e_2, ..., e_{p-1}$ déjà choisis, ce qui élimine les q^{p-1} vecteurs de Vect $(e_1, ..., e_{p-1})$, et donne $q^n - q^{p-1}$ choix.

On obtient ainsi $(q^n - 1)(q^n - q) \dots (q^n - q^{p-1})$ choix de la base $\mathscr{B}$, mais..., si $\mathscr{B}_0$ est une telle base, qui engendre F_0, n'importe quelle famille libre de F_0 redonnera F_0. Or, dans F_0 espace de dimension p cette fois, sur K, il y a q^p éléments, et il y a :

$$(q^p - 1)(q^p - q) \dots (q^p - q^{p-1}),$$

familles libres, car pour en obtenir une, $\{\varepsilon_1, ..., \varepsilon_p\}$, il y a :

$q^p - 1$ choix de ε_1 ; et pour chacun de ces choix il y aura :

$q^p - q$ choix de ε_2 non dans Vect (ε_1) ; puis :

$q^p - q^2$ choix de ε_3 non dans Vect $(\varepsilon_1, \varepsilon_2)$, ..., pour finir par :

$q^p - q^{p-1}$ choix de ε_p, non dans Vect $(\varepsilon_1, \varepsilon_2, ..., \varepsilon_{p-1})$.

On a donc en fait $a_p = \dfrac{(q^n - 1)(q^n - q) \dots (q^n - q^{p-1})}{(q^p - 1)(q^p - q) \dots (q^p - q^{p-1})}$ choix du sous-espace F, supposé de dimension p, des points fixes de la symétrie.

Pour chacun de ces choix, il faut choisir un supplémentaire G, de dimension $n - p$, de base $\{u_1, u_2, ..., u_{n-p}\}$, et pour cela il y a :

$q^n - q^p$ choix possible de u_1, non dans F ; puis :

$q^n - q^{p+1}$ choix de u_2, pas dans $F \oplus Ku_1$; puis :

$q^n - q^{p+2}$ choix de u_3, non dans $F \oplus$ Vect (u_1, u_2) ;

et ainsi de suite, pour terminer par :

$q^n - q^{n-1}$ choix de u_{n-p}.

Mais comme précédemment, n'importe quelle famille libre de G = Vect $(u_1, u_2, ..., u_{n-p})$ donnera le même sous-espace G, or il y a :

$$(q^{n-p} - 1)(q^{n-p} - q) \dots (q^{n-p} - q^{n-p-1})$$

choix d'une telle famille libre, d'où finalement, un nombre :

$$b_p = \frac{(q^n - q^p)(q^n - q^{p+1}) \dots (q^n - q^{n-1})}{(q^{n-p} - 1)(q^{n-p} - q) \dots (q^{n-p} - q^{n-p-1})},$$

de choix possibles du sous-espace G en somme directe avec F.

Le cardinal cherché est donc :

$$\sum_{p=0}^{n} \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{p-1})(q^n-q^p)\ldots(q^n-q^{n-1})}{(q^p-1)(q^p-q)\ldots(q^p-q^{p-1})(q^{n-p}-1)\ldots(q^{n-p}-q^{n-p-1})},$$

si, pour $p = 0$, (ou n), le terme général $a_p b_p$ vaut 1, par convention, (car que vaut $q^0 - 1$ dans ce cas, ou $q^0 - q^{-1}$?)

On peut remarquer que ce résultat est valable pour tout endomorphisme annulant un polynôme scindé de degré deux à racines simples sur K, et qu'il peut se généraliser pour un polynôme de degré 3, 4, ..., scindé à racines simples.

4.59. La matrice M, symétrique réelle a toutes ses valeurs propres réelles et diagonalise dans le groupe orthogonal.

Cependant, son allure incite à prendre une démarche vectorielle.

Soit $E = \mathbb{R}^n$ rapporté à la base canonique $\mathscr{B} = \{e_1, \ldots, e_n\}$, et u l'endomorphisme de matrice M.

En introduisant les vecteurs $a = \sum_{i=1}^{n} e_i$ et $b = \sum_{i=1}^{n} x_i e_i$, on constate que :

$$f(e_j) = \sum_{i=1}^{n} (x_i + x_j)e_i = b + x_j a,$$

donc l'image de f est dans $F = \text{Vect}(a, b)$.

Premier cas : $\{a, b\}$ famille liée, donc, comme a est non nul, on a b du type λa, et, pour tout i, $x_i = \lambda$, d'où $f(e_j) = 2\lambda a$.

Si $\lambda = 0, f \equiv 0$: faut-il préciser valeurs et vecteurs propres ?

Si $\lambda \neq 0$, M est la matrice de terme constant 2λ non nul.

Elle est de rang 1, 0 est valeur propre d'ordre $n-1$, le noyau est l'hyperplan d'équation $y_1 + y_2 + \ldots + y_n = 0$, (les x_i étant occupés ailleurs, on note y_i les coordonnées), de base les vecteurs $e_j - e_1, j \geqslant 2$ par exemple.

La trace, $2n\lambda$, donne la dernière valeur propre, et comme $f(e_j) = 2\lambda a$, en sommant il vient $f(a) = (2n\lambda)a$: le vecteur a est vecteur propre pour cette valeur propre.

Deuxième cas : $\{a, b\}$ famille libre.

L'image étant contenue dans $F = \text{Vect}(a, b)$, f est au plus de rang 2.

Si on somme les relations $f(e_j) = b + x_j a$, en posant $s = x_1 + ... + x_n$, on obtient :

$$f(a) = nb + sa .$$

De même, le calcul de $\sum_{j=1}^{n} x_j f(e_j) = \sum_{j=1}^{n} (x_j b + x_j^2 a)$, conduit, avec $t = x_1^2 + x_2^2 + ... + x_n^2$, à :

$$f(b) = sb + ta .$$

Mais alors F = Vect (a, b) est stable par f, et $\tilde{f}$ induit sur F par f, diagonalisable car symétrique réel, sera diagonalisable.

La matrice de $\tilde{f}$ dans la base $\{a, b\}$ de F est :

$$A = \begin{pmatrix} s & t \\ n & s \end{pmatrix},$$

de polynôme caractéristique $(\lambda - s)^2 - nt = 0$.

Comme les x_i ne sont pas tous nuls, (sinon $b = 0$), t est strictement positif, et on a deux valeurs propres distinctes, $\lambda = s + \varepsilon\sqrt{nt}$, avec $\varepsilon = 1$ ou -1.

Un vecteur $\alpha a + \beta b$ est propre pour la valeur propre λ si on a :

$$(s - \lambda)\alpha + t\beta = -\varepsilon\sqrt{nt}\alpha + t\beta = 0 .$$

Une solution est donc $\alpha = t$, $\beta = \varepsilon\sqrt{nt}$, donc $\left(\sum_{j=1}^{n} x_j^2\right) a + \varepsilon \sqrt{n \sum_{j=1}^{n} x_j^2}\, b$ est vecteur propre pour la valeur propre $s + \varepsilon \sqrt{n \sum_{j=1}^{n} x_j^2}$.

Pour le noyau, comme il existe j_0 avec $x_{j_0} \neq x_1$, (les x_j tous égaux à x_1 conduisent à $\{a, b\}$ famille liée), et comme $f(e_k - e_1) = (x_k - x_1)a$, on aura, pour tout $k \geqslant 2$, $k \neq j_0$, (avec $j_0 \geqslant 2$) :

$$f((x_{j_0} - x_1)(e_k - e_1) - (x_k - x_1)(e_{j_0} - e_1)) = 0 .$$

Les $e'_j = e_j - e_1$, pour $j \geqslant 2$, étant $n - 1$ vecteurs libres, les $\varepsilon_k = (x_{j_0} - x_1)e'_k - (x_k - x_1)e'_{j_0}$, avec $k \geqslant 2$ et $k \neq j_0$ sont aussi libres, $(x_{j_0} - x_1 \neq 0)$: on a $n - 2$ vecteurs libres dans le noyau de f.

En fait le noyau est exactement de dimension $n-2$ dans ce cas, car, avec $x_{j_0} - x_1 \neq 0$, on a :

$$f(e_{j_0} - e_1) = (x_{j_0} - x_1)a\,, \text{ d'où } f\left(\frac{e_{j_0} - e_1}{x_{j_0} - x_1}\right) = a\,, \text{ puis :}$$

$$f\left(e_{j_0} - x_{j_0} \cdot \frac{e_{j_0} - e_1}{x_{j_0} - x_1}\right) = b + x_{j_0}a - x_{j_0}a = b\,.$$

L'image est effectivement F de dimension 2. Les valeurs propres de $\tilde{f}$, endomorphisme de rang 2, induit par f sur F, sont non nulles, f est de rang $\geqslant 2$, mais $\operatorname{Ker} f$ est de dimension $\geqslant n-2$: en fait f est exactement de rang 2 et on a diagonalisé f.

CHAPITRE V

Formes quadratiques, espaces euclidiens et préhilbertiens réels

L'étude des formes quadratiques commence par la détermination du caractère défini ou non, dégénéré ou non d'une forme, ainsi qu'en dimension finie, par la recherche d'une décomposition en carrés, (**Gauss peut servir**), ce qui, dans le cas réel, donnera la signature.

Sur les espaces euclidiens, ou plus généralement sur les espaces préhilbertiens réels, on a un mélange d'algèbre et de topologie sur un espace vectoriel normé, la norme étant associée à un produit scalaire, d'où une structure très riche.

Prennent de l'importance les notions de :

1°) *base orthonormée*, (qui existent sur tout espace de dimension dénombrable ;

2°) *projection orthogonale* sur un sous-espace F, à condition d'avoir $E = F \oplus F^{\perp}$; ne pas oublier les symétries orthogonales ;

3°) *opérateur adjoint d'un autre*, avec les autoadjoints, (diagonalisables en dimension finie) et les isométries.

Dans ce type d'espaces, il est bon de garder présents à l'esprit un certain nombre de résultats. Par exemple :

• une propriété stable par bilinéarité sera vraie sur $E \times E$ si elle l'est pour les couples (x, y) de vecteurs d'une base, (exercice 5.3) ;

• importance des bases orthonormées pour les calculs, en particulier des distances, ou plus astucieusement des carrés des distances, (5.1) ;

• le procédé **d'orthonormalisation de Schmidt**, non seulement donne l'existence d'une base orthonormée en dimension dénombrable, mais la « matrice » de passage est triangulaire, (voir 5.1), et on obtient facilement des inégalités ;

• ce procédé de Schmidt donne des polynômes de degrés échelonnés, orthogonaux pour un produit scalaire du type $\int_I P(t)Q(t)\rho(t)dt = \langle P, Q \rangle$, avec des hypothèses convenables ;

• la **matrice de Gramm** des $\langle e_i, e_j \rangle$, cela existe ;

• la **méthode de Gauss** donne les nouvelles coordonnées en fonction des anciennes, donc les lignes de P^{-1} si P est la matrice de passage ;

• si A est une matrice quelconque, ${}^tAA$ et $A{}^tA$ sont des matrices symétriques positives : (5.4) ; (5.6), sur $\mathbb{R}$, bien entendu ;

• sur E **euclidien**, la norme d'un opérateur linéaire u est $|||u|||$ = (rayon spectral de $u^*u)^{1/2}$; (5.5.).

• la topologie n'est jamais loin, la convexité non plus ; ne pas oublier **Pythagore** ni les triangles isocèles, ni la géométrie du plan, même dans le plus horrible des préhilbertiens, (5.2) ;

• si F est sous-espace de dimension finie de E, avec $(e_1, ..., e_n)$ base orthonormée de F, le projeté de x quelconque sur F est $\sum_{i=1}^{n} \langle x, e_i \rangle e_i$ et c'est le point de F le plus près de x ;

• si F, sous-espace de dimension dénombrable stricte de E, de base orthonormée $(e_i)_{i \in \mathbb{N}}$ est partout dense dans E pour la norme préhilbertienne, pour tout x de E on a $\|x\|^2 = \sum_{i \in \mathbb{N}} (\langle x, e_i \rangle)^2$: c'est **l'égalité de Bessel** ; la famille des (e_i) est dite **totale**, (voir exercice 5.15).

Penser également à **la décomposition polaire** des éléments de GL(E), avec E euclidien, c'est-à-dire l'écriture $a = up$ avec $a \in GL(E)$, $u \in O(E)$, p opérateur symétrique défini positif, (voir 5.6) ; voir aussi 11.12 pour le cas complexe, et l'extension à une matrice non inversible.

Apprendre un cours, c'est aussi en connaître les détails. Ainsi, savoir que dans l'inégalité de Cauchy Schwarz il y a égalité si et seulement si les vecteurs sont liés, cela peut être utile, voir 5.16.

Il existe aussi des résultats techniques utiles à connaître. Ainsi, sur E euclidien, si $f * f = g * g$, il existe s orthogonal tel que $f = s \circ g$, (voir 5.9).

Pensez toujours, pour traiter une question, à analyser la manière dont les données interviennent, (linéairement, multilinéairement, continûment...), pour fragmenter la difficulté. Par ailleurs, si une première étude n'aboutit pas, demandez vous pourquoi avant de tout rejeter. Voir 5.3.

Dans le même ordre d'idée, une matrice orthogonale, $P = (p_{ij})_{1 \leq i,j \leq n}$, cela permet d'obtenir des 1 = des tas de choses, ce qui permet de transformer un nombre en somme, ($\alpha = \sum_{k=1}^{n} \alpha p_{ki}^2$ par exemple), et d'obtenir des expressions indexées de la même manière. Allez voir du côté de 5.26.

Énoncés

5.1. Soit E un espace vectoriel euclidien de dimension n, et $u_1, ..., u_n$ des vecteurs de norme 1 tels que, pour $1 \leqslant i < j \leqslant n$ on ait $\|u_i - u_j\| = 1$. Établir que $(u_1, ..., u_n)$ est une base de E.

Soit $(e_1, ..., e_n)$ l'orthonormalisée de Schmidt de $(u_1, ..., u_n)$. Montrer qu'il existe des réels $b_1, ..., b_{n-1}$ et $a_1, ..., a_n$ tels que, pour tout j de $[1, n]$, $u_j = a_j e_j + \sum_{1 \leqslant i < j} b_i e_i$.

Calcul des a_j et des b_j.

5.2. Soit E préhilbertien réel.

a) Pour x et y de E, vérifier que $\|x+y\|^2 + \|x-y\|^2 = 2(\|x\|^2 + \|y\|^2)$.

b) Soit C une partie de E, convexe, complète. Montrer que, pour tout x de E il existe un et un seul $p(x)$ dans C tel que :

$$\forall y \in C, \|x-y\| \geqslant \|x-p(x)\|.$$

c) Si C est sous-espace vectoriel de E, noté F, montrer que, pour tout y de F, $\langle x-p(x)|y\rangle = 0$. En déduire la nature de p.

d) Dans le cas général, (C convexe complet), montrer que, pour tout (x, z) de C^2, $\|x-z\| \geqslant \|p(x)-p(z)\|$.

5.3. Soit $P \in \mathbb{R}[X]$, $P(X) = \sum_{k=0}^{n} a_k X^k$.

Montrer que $\int_{-1}^{1} P^2(x)dx = -i \int_0^{\pi} P^2(e^{i\theta})e^{i\theta}d\theta$, et en déduire que $\sum_{0 \leqslant k,l \leqslant n} \frac{a_k a_l}{k+l+1} \leqslant \pi \sum_{k=0}^{n} a_k^2$.

5.4. Soit A dans $\mathcal{M}_{n,p}(\mathbb{R})$, de rang n. Montrer que $A\,{}^tA$ est inversible. Que dire de ${}^tAA$ si A est de rang p.

5.5. Soit Δ l'endomorphisme de $\mathbb{R}^n$ défini par $(\Delta(x))_i = x_i - x_{i-1}$, en posant $x = \sum_{i=1}^{n} x_i e_i$ et $x_0 = 0$, $\{e_1, ..., e_n\}$ base canonique de $\mathbb{R}^n$.

Montrer que Δ est inversible et que :

$$|||\Delta^{-1}||| = \frac{1}{2\sin\dfrac{\pi}{2(2n+1)}}, \text{ où } ||| \cdot ||| \text{ est la norme d'application}$$

linéaire continue associée à la norme euclidienne canonique de $\mathbb{R}^n$.

5.6. Soit E, espace vectoriel euclidien, et $a \in GL(E)$.

1°) Montrer qu'il existe un unique couple (u, s), où u est un automorphisme orthogonal et s un endomorphisme symétrique défini positif, tel que $a = us$.

2°) Déterminer $\underset{v \in O(E)}{\text{Sup}}$ Trace (va).

3°) Déterminer $\underset{v \in O^+(E)}{\text{Sup}}$ Trace (va).

5.7. Soit A matrice carrée réelle d'ordre n, symétrique, de valeurs propres ordonnées $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n$.

Montrer que $\sum_{j=1}^{k} a_{jj} \leqslant \sum_{j=1}^{k} \lambda_j$.

5.8. Soit p et q deux projecteurs orthogonaux d'un espace euclidien E. Montrer que E est somme directe de sous-espaces stables à la fois par p et q, de dimension 1 ou 2.

5.9. Soit E euclidien. Montrer que si f et g sont des éléments de L(E) tels que $f * f = g * g$, il existe s, opérateur orthogonal, tel que $f = sg$.

Soit E euclidien de dimension n, $(u_1, \ldots, u_n)$ une famille de n vecteurs et $\mathcal{G} = (\langle u_i, u_j \rangle)_{1 \leqslant i,j \leqslant n}$, la matrice de Gramm associée. Montrer l'équivalence de :

1°) il existe un projecteur orthogonal p et une base orthonormée $(e_1, \ldots, e_n)$ telle que, pour tout i, $u_i = p(e_i)$;

2°) le spectre de $\mathcal{G}$ est dans $\{0, 1\}$.

5.10. Soit E un espace euclidien de dimension > 0, de sphère unité S. Déterminer l'image de l'application f de S^3 dans $\mathbb{R}$ définie par $f(u, v, w) = \langle u, v \rangle + \langle v, w \rangle + \langle w, u \rangle$.

5.11. Soit A dans $\mathcal{M}_n(\mathbb{R})$, de trace nulle. Montrer qu'il existe U orthogonale telle que $U^{-1}AU$ ait ses termes diagonaux nuls.

5.12. Soit A matrice symétrique réelle d'ordre $n+1$, de valeurs propres indexées en croissant : $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_{n+1}$, de terme général a_{ij}.

Soit B la matrice symétrique réelle d'ordre n des a_{ij} pour $1 \leqslant i, j \leqslant n$ et $\mu_1 \geqslant \mu_2 \geqslant \ldots \geqslant \mu_n$ ses valeurs propres. Montrer que l'on a l'entrelacement :

$$\lambda_1 \geqslant \mu_1 \geqslant \lambda_2 \geqslant \mu_2 \geqslant \ldots \geqslant \lambda_n \geqslant \mu_n \geqslant \lambda_{n+1}.$$

5.13. Soit A une matrice symétrique réelle de valeurs propres $\mu_1, \ldots, \mu_n$. Soit $\lambda_1, \ldots, \lambda_{n+1}$, $n+1$ réels donnés et $c = \sum_{i=1}^{n+1} \lambda_i - \sum_{i=1}^{n} \mu_i$.

Montrer qu'il existe b dans $\mathbb{R}^n$ tel que $\begin{pmatrix} A & b \\ {}^t b & c \end{pmatrix}_{n+1}$ admette $(\lambda_1, \ldots, \lambda_{n+1})$ pour spectre si et seulement si $f(x) = \dfrac{\prod_{i=1}^{n+1} (x - \lambda_i)}{\prod_{i=1}^{n} (x - \mu_i)}$ n'a que des pôles simples, en étant croissante sur son domaine de définition.

5.14. Soit f continue de $[a, b]$ dans $\mathbb{R}$, telle que $\int_a^b f(t) t^n \mathrm{d}t = 0$ pour tout n tel que $0 \leqslant n \leqslant p-1$. Montrer que f change au moins p fois de signe sur $[a, b]$.

5.15. Soit E l'espace vectoriel des suites $x = (x_k)_{k \in \mathbb{N}}$ de réels telles que $\sum_{k=0}^{+\infty} (x_k)^2$ converge. Pour x et y dans E on pose $\langle x, y \rangle = \sum_{k=0}^{\infty} x_k y_k$, et l'on note $\| \ \|$ la norme associée.

Soit $(x^{(n)})_{n \in \mathbb{N}}$ une suite bornée d'éléments de E. Montrer qu'il existe une sous-suite $(y^{(k)})_{k \in \mathbb{N}}$ de la suite $(x^{(n)})_{n \in \mathbb{N}}$ et un élément a de E tels que, pour tout z de E, $\langle y^{(k)}, z \rangle$ tende vers $\langle a, z \rangle$.

5.16. Condition sur f dans $\mathscr{C}^0([a, b], \mathbb{R}^n)$ pour que, pour la norme euclidienne sur $\mathbb{R}^n$, on ait :

$$\int_a^b \|f(t)\| \mathrm{d}t = \left\| \int_a^b f(t) \mathrm{d}t \right\|.$$

5.17. Soit E un espace euclidien de dimension finie, (litote ?), $u \in L(E)$ symétrique défini positif.

Soit $\varphi : E \setminus \{0\} \longrightarrow \mathbb{R}$, définie par : $x \longrightarrow \dfrac{(\langle u(x), x\rangle)^2}{\|u(x)\|^2 \|x\|^2}$.

Montrer que φ est bornée. Atteint-elle ses bornes ?

5.18. Soit E un espace vectoriel normé de dimension finie et a dans E.

a) Γ est un fermé non vide de E. Montrer que l'application d_a de Γ dans $\mathbb{R}$, définie par $d_a(x) = \|x - a\|$ admet un minimum atteint sur Γ.

b) Si Γ est un cône convexe fermé, (donc $\forall (x, y, \lambda) \in \Gamma^2 \times \mathbb{R}_+$, $x + y$ et λx sont dans Γ) dans E supposé euclidien, montrer que d_a admet un minimum atteint en un point unique b de Γ tel que $\langle b - a, b\rangle = 0$ et $\forall x \in \Gamma$, $\langle b - a, x\rangle \geqslant 0$.

5.19. Soit E un espace euclidien de dimension 2 au moins, et f une application continue de E dans E, telle que :

$$\forall (x, y) \in E^2, (x \perp y \Rightarrow f(x + y) = f(x) + f(y)).$$

a) On suppose f paire. Montrer que, pour tout (x, y) de E^2 tel que $\|x\| = \|y\|$, on a $f(x) = f(y)$.

En déduire que f est de la forme $x \longrightarrow \|x\|^2 k$, $k \in E$.

b) Montrer que si f est impaire, elle est linéaire.

c) Étudier le cas général.

5.20. On se place dans le plan euclidien rapporté à une base orthonormée $\{\vec{i}, \vec{j}\}$. Soit p_1, p_2, p_3 les projections orthogonales respectivement sur $\mathbb{R}\vec{i}$, $\mathbb{R}(\vec{i} + \vec{j})$, $\mathbb{R}\vec{j}$. On pose $q = p_3 p_2 p_1$. Image et noyau de q ? Que dire de q^* ?

On généralise à E euclidien de dimension p. Soient $N_1, ..., N_k$ des sous-espaces vectoriels de E, $p_1, ..., p_k$ les projecteurs orthogonaux sur $N_1, ..., N_k$. On pose $q = p_k \dots p_1$ et $N_0 = \bigcap_{i=1}^{k} N_i$.

a) Montrer que, pour tout x de E, $\|q(x)\| = \|x\| \Leftrightarrow x \in N_0$.

b) Montrer que $\operatorname{Ker}(q - \mathrm{id}) = N_0$. En déduire que $\operatorname{Ker}(q^* - \mathrm{id}) = N_0$.

c) Montrer que $E = N_0 \oplus (\mathrm{Im}\,(q - \mathrm{id}))$.

d) Soit $(x_n)_{n \in \mathbb{N}}$ une suite de points de E telle que $\|x_n\| \leqslant 1$ pour tout n, et $\lim_{n \to +\infty} \|q(x_n)\| = 1$.

Montrer que $\lim_{n \to +\infty} \|(q - \mathrm{id})(x_n)\| = 0$.

5.21. Soit A dans $\mathcal{M}_n(\mathbb{R})$, antisymétrique, et $B = (I + A)(I - A)^{-1}$. Montrer que B est orthogonale.

Réciproquement, peut-on toujours décomposer B orthogonale sous la forme $B = (I + A)(I - A)^{-1}$, avec A antisymétrique ?

5.22. Soient A et B deux matrices symétriques réelles positives, q_A et q_B les formes quadratiques associées sur $\mathbb{R}^n$ rapporté à une base. On suppose $q_A \leqslant q_B$. Montrer que $\det A \leqslant \det B$.

5.23. Soit E l'ensemble des matrices symétriques réelles d'ordre n. Soient A et B dans E, on dit que $A \leqslant B$ lorsque, pour tout vecteur colonne X de $\mathcal{M}_{n,1}(\mathbb{R})$, on a ${}^tXAX \leqslant {}^tXBX$.

a) Vérifier que l'on a une relation d'ordre sur E.

b) Soit $(A_k)_{k \in \mathbb{N}}$ une suite d'éléments de E, croissante et majorée au sens de cette relation d'ordre. Montrer qu'elle est convergente dans E.

c) Soit les polynômes P_k, $k \in \mathbb{N}$, définis par la donnée de $P_0 = 0$ et de la relation de récurrence $P_{n+1}(x) = P_n(x) + \frac{1}{2}(x - P_n^2(x))$. Quelle est la limite de la suite de fonctions P_n, sur [0, 1].

Pour A dans E, on pose $B_k = P_k(A)$. Montrer que si chaque valeur propre de A est dans [0, 1], la suite des B_k converge vers un élément de E. Quel est cet élément ?

5.24. Soit E l'ensemble des matrices symétriques réelles d'ordre n.

a) Soit A dans E avec $I_n - A$ définie positive. Montrer que la suite $\left(\sum_{k=0}^{2p-1} (\mathrm{trace}\, A^k)\right)_{p \in \mathbb{N}^*}$ est majorée.

b) On suppose de plus A à coefficients positifs. Montrer que $(I_n - A)^{-1}$ est à coefficients positifs.

5.25. Soit C une matrice symétrique réelle carrée d'ordre n. Montrer que $\rho(C) = \sup\{|\lambda_i| ; \lambda_i \text{ valeur propre de } C\}$ est égal à $|||C||| = \sup\{\|C(x)\| ; \|x\| = 1\}$, la norme de $\mathbb{R}^n$ étant la norme euclidienne canonique.

Montrer que, pour A et B dans $\mathcal{M}_n(\mathbb{R})$, on a :

$$(\rho(AB))^2 \leqslant \rho({}^tAA)\rho({}^tBB).$$

5.26. Soit a et b deux endomorphismes symétriques de l'espace euclidien E. Montrer que :

$$\text{trace}\,(e^a(a-b) - e^a + e^b) \geqslant 0.$$

5.27. Soit q une forme quadratique définie positive sur $\mathbb{R}^n$, de matrice $A = (\alpha_{ij})_{1 \leqslant i,j \leqslant n}$ dans la base canonique.

On définit q' sur $\mathbb{R}^{n-1}$ par :

$$q'(x_1, \ldots, x_{n-1}) = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \begin{vmatrix} \alpha_{nn} & \alpha_{ni} \\ \alpha_{nj} & \alpha_{ij} \end{vmatrix} x_i x_j .$$

Montrer que q' est définie positive.

5.28. Soit ϕ forme quadratique sur E, de forme polaire φ. On fixe a dans E et on définit F par :

$$F(x) = \phi(a)\phi(x) - (\varphi(a, x))^2 .$$

Vérifier que F est une forme quadratique, dont on cherchera le noyau.

5.29. Soit E euclidien de dimension n, et u un endomorphisme de E. On définit une forme quadratique Q sur E par $Q(x) = (\|u(x)\|)^2$.

Soit Q' une autre forme quadratique sur E. Montrer que la restriction de Q' à Ker u est définie positive si et seulement si il existe r réel tel que $Q' + rQ$ soit définie positive.

Solutions

5.1. Pour $1 \leqslant i < j \leqslant n$ on a $\|u_i - u_j\|^2 = 1 = \|u_i\|^2 - 2\langle u_i, u_j\rangle + \|u_j\|^2$, et les vecteurs étant de norme 1, il reste $\langle u_i, u_j\rangle = \frac{1}{2}$.

Si on suppose alors que des scalaires $\lambda_1, ..., \lambda_n$ sont tels que $\sum_{i=1}^{n} \lambda_i u_i = 0$, en prenant le carré de la norme on a :

$$\sum_{i=1}^{n} \lambda_i^2 + 2 \sum_{1 \leqslant i < j \leqslant n} \lambda_i \lambda_j \frac{1}{2} = 0, \text{ mais c'est encore :}$$

$$\frac{1}{2} \sum_{i=1}^{n} \lambda_i^2 + \left(\sum_{i=1}^{n} \frac{\lambda_i}{\sqrt{2}} \right)^2 = 0, \text{ ceci impliquant la nullité de chaque } \lambda_i^2$$

donc de chaque λ_i : on a une famille libre de n vecteurs, donc une base.

Par le procédé d'orthonormalisation de Schmidt, on sait que pour $j = 1, ..., n$, Vect $(u_1, ..., u_j)$ = Vect $(e_1, ..., e_j)$, donc pour tout j, on a des coefficients (λ_{ij}), pour $1 \leqslant i \leqslant j$, tels que $u_j = \sum_{i=1}^{j} \lambda_{i,j} e_i$.

Notre problème, compte tenu des u_j, est de montrer l'indépendance des $\lambda_{i,j}$ par rapport à j, pour $i < j$.

Soient donc $2 \leqslant j < j' \leqslant n$, on pose aussi :

$$u_{j'} = \sum_{i=1}^{j'} \lambda_{i,j'} e_i.$$

On a, pour $i < j$, $\lambda_{i,j} = \langle u_j, e_i\rangle$ et,

$$\lambda_{i,j'} = \langle u_{j'}, e_i\rangle.$$

Or $e_i \in$ Vect $(u_1, ..., u_i)$. Il existe donc des scalaires $\alpha_1, ..., \alpha_i$ tels que $e_i = \sum_{k=1}^{i} \alpha_k u_k$, (ces α_k ne dépendent que de i en fait), et on a :

$$\lambda_{i,j} = \langle u_j, \sum_{k=1}^{i} \alpha_k u_k\rangle = \sum_{k=1}^{i} \alpha_k \langle u_j, u_k\rangle = \frac{1}{2} \sum_{k=1}^{i} \alpha_k,$$

puisque $i<j \Rightarrow j \neq k$ et $\langle u_j, u_k \rangle = \frac{1}{2}$; mais de même on aura :

$$k \neq j' \text{ et } \langle u_{j'}, u_k \rangle = \frac{1}{2} \text{ pour } k \leqslant i \text{ d'où :}$$

$$\lambda_{i,j'} = \langle u_{j'}, e_i \rangle = \sum_{k=1}^{i} \frac{1}{2} \alpha_k \text{ et } \underline{\underline{\lambda_{i,j} = \lambda_{i,j'}}}, \text{ pour } i<j<j'.$$

En posant $a_1 = \lambda_{1,1}$; $b_1 = \lambda_{1,2} = \lambda_{1,3} = \ldots = \lambda_{1,n}$, et plus généralement $a_j = \lambda_{j,j}$; $b_j = \lambda_{j,j+1} = \lambda_{j,j+2}, \ldots = \lambda_{j,n}$ si $j<n$, on trouve $b_1, \ldots, b_{n-1}$ et $a_1, \ldots, a_n$, tels que, pour tout j : $u_j = \sum_{1 \leqslant i<j} b_i e_i + a_j e_j$.

Cette connaissance des u_j dans une base orthonormée, va permettre de déterminer les b_i et les a_j, (au signe près) en traduisant les relations $\|u_j\|^2 = 1$ et $\langle u_j, u_{j+1} \rangle = \frac{1}{2}$.

Procédons par récurrence.

Pour $j = 1$, $\|u_1\|^2 = a_1^2 = 1$, donc $a_1 = 1$ ou -1.

On se donne une suite finie $(\varepsilon_j)_{1 \leqslant j \leqslant n}$ à valeurs dans $\{-1, 1\}$, et soit $a_1 = \varepsilon_1$.

On a alors $\langle u_1, u_2 \rangle = \frac{1}{2} = a_1 b_1$ donc $b_1 = \frac{\varepsilon_1}{2}$, puis $\|u_2\|^2 = 1 = b_1^2 + a_2^2 = \frac{1}{4} + a_2^2$ d'où $a_2^2 = \frac{3}{4}$ et $a_2 = \varepsilon_2 \sqrt{\frac{3}{4}}$.

Supposons connus $a_1, \ldots, a_{j-1}, a_j$ et $b_1, \ldots, b_{j-1}$, avec : $a_k = \varepsilon_k \sqrt{\frac{k+1}{2k}}$ pour $1 \leqslant k \leqslant j$. (C'est vérifié au rang $j = 2$.)

En écrivant les trois égalités $\|u_j\|^2 = 1, \|u_{j+1}\|^2 = 1$ et $\langle u_j, u_{j+1} \rangle = \frac{1}{2}$, il vient :

$$b_1^2 + \ldots + b_{j-1}^2 + a_j^2 = 1$$

$$b_1^2 + \ldots + b_{j-1}^2 + b_j^2 + a_{j+1}^2 = 1$$

$$b_1^2 + \ldots + b_{j-1}^2 + a_j b_j = \frac{1}{2},$$

d'où l'on tire : $a_{j+1}^2 = a_j^2 - b_j^2$ et $a_j b_j = a_j^2 - \frac{1}{2}$.

On a donc $\varepsilon_j \sqrt{\dfrac{j+1}{2j}}\, b_j = \dfrac{j+1}{2j} - \dfrac{1}{2} = \dfrac{1}{2j}$, d'où l'on tire :

$$b_j = \frac{\varepsilon_j}{\sqrt{2j(j+1)}} \text{ (au passage, c'est vérifié si } j = 1\text{), puis :}$$

$$a_{j+1}^2 = \frac{j+1}{2j} - \frac{1}{2j(j+1)} = \frac{j^2+2j}{2j(j+1)} = \frac{(j+1)+1}{2(j+1)}$$

donc, avec $\varepsilon_{j+1} = 1$ ou -1, on a bien $a_{j+1} = \varepsilon_{j+1}\sqrt{\dfrac{(j+1)+1}{2(j+1)}}$: le calcul se fait par récurrence.

5.2. Le a) est l'identité du parallélogramme : il suffit de développer $\|x+y\|^2 = \|x\|^2 + 2\langle x, y\rangle + \|y\|^2$ et

$\|x-y\|^2 = \|x\|^2 - 2\langle x, y\rangle + \|y\|^2$ et d'ajouter.

b) Complet fait penser à suite de Cauchy. On suppose bien sûr C *non vide*, donc $d = d(x, \mathrm{C}) = \inf\{\|x-y\|, y \in \mathrm{C}\}$ existe, et $\forall n \in \mathbb{N}^*$, $\exists y_n \in \mathrm{C}$, $d \leqslant \|x-y_n\| \leqslant d + \dfrac{1}{n}$.

La suite des y_n est de Cauchy, car le a) appliqué à $x-y_p$ et $x-y_q$, conduit à :

$$\|2x-(y_p+y_q)\|^2 + \|y_q-y_p\|^2 = 2\|x-y_p\|^2 + 2\|x-y_q\|^2 \leqslant$$
$$2\left(d+\frac{1}{p}\right)^2 + 2\left(d+\frac{1}{q}\right)^2,$$

donc, avec $\|2x-(y_p+y_q)\|^2 = 4\left\|x - \dfrac{y_p+y_q}{2}\right\|^2 \geqslant 4d^2$ car $\dfrac{y_p+y_q}{2}$ est dans C, convexe, on obtient :

$$\|y_p-y_q\|^2 \leqslant 2\left(d^2 + \frac{2d}{p} + \frac{1}{p^2} + d^2 + \frac{2d}{q} + \frac{1}{q^2}\right) - 4d^2$$
$$\leqslant 4d\left(\frac{1}{p}+\frac{1}{q}\right) + 2\left(\frac{1}{p^2}+\frac{1}{q^2}\right),$$

majorant rendu arbitrairement petit pour p et q assez grands.

La suite $(y_n)_{n \in \mathbb{N}}$ est de Cauchy dans C complet, donc elle a une limite y, et l'inégalité $d \leqslant \|x-y_n\| \leqslant d + \dfrac{1}{n}$, jointe à la continuité de la norme, donne $d = \|x-y\|$.

Si d était aussi atteinte en y' dans C, dans le triangle isocèle de sommets x, y, y', le milieu $\frac{y+y'}{2}$ du côté $[y, y']$ serait plus près, (par Pythagore) du sommet x, que y ou y', ce qui est absurde, d'où $y = y'$. *On note $p(x)$ cet unique élément de C.*

c) Soit y quelconque dans F, pour tout t de $\mathbb{R}$, $z = p(x) + ty$ est dans F, donc $\|x - p(x)\|^2 \leqslant \|x - p(x) - ty\|^2$, ce qui, en développant et après simplification par $\|x - p(x)\|^2$, conduit à :

$$0 \leqslant -2t\langle x - p(x), y\rangle + t^2\|y\|^2.$$

En simplifiant par $t > 0$, et en faisant tendre t vers 0^+, on obtient :

$\langle x - p(x), y\rangle \leqslant 0$, et ce pour y quelconque de F, donc aussi pour $-y$, d'où $-\langle x - p(x), y\rangle \leqslant 0$ et finalement : $\langle x - p(x), y\rangle = 0, \forall y \in F$.

Ceci traduit l'appartenance de $x - p(x)$ à $F^\perp$. Comme on a $x = (x - p(x)) + p(x)$, décomposé dans $F^\perp + F$, et que $F \cap F^\perp = \{0\}$, on a $E = F \oplus F^\perp$.

Si x de E se décompose alors en $x = u + v$, $u \in F$, $v \in F^\perp$, pour y quelconque de F on aura :

$\|x - y\|^2 = \|(u - y) + v\|^2 = \|u - y\|^2 + \|v\|^2 \geqslant \|v\|^2$, borne inférieure atteinte en $y = u$, donc $p(x) = u$ est le projeté orthogonal de x sur F, d'où p linéaire, (et même continue car $\|p(x)\|^2 = \|u\|^2 \leqslant \|u\|^2 + \|v\|^2 = \|x\|^2$: p est 1.lipschitzienne.

d) Pour C convexe, on reprend le c), pour justifier que, pour tout y de C, on a $\langle p(x) - x, p(x) - y\rangle \leqslant 0$.

En effet $p(x)$ et y sont dans C convexe, donc $z = p(x) + t(y - p(x))$ aussi, pour $0 \leqslant t \leqslant 1$, on a donc :

$\|x - p(x)\|^2 \leqslant \|x - p(x) - t(y - p(x))\|^2$, ce qui se développe et donne, après simplification par $\|x - p(x)\|^2$, l'inégalité :

$$0 \leqslant -2t\langle x - p(x), y - p(x)\rangle + t^2\|p(x) - y\|^2,$$

d'où le résultat en simplifiant par $t > 0$ et en faisant tendre t vers 0^+.

Partant alors de x et z dans E, et de $p(z)$ et $p(x)$ dans C, on aura :

$\langle p(x) - x, p(x) - p(z)\rangle \leqslant 0$ et,

$\langle p(z) - z, p(z) - p(x)\rangle \leqslant 0$ soit encore,

$\langle z - p(z), p(x) - p(z)\rangle \leqslant 0$.

On en déduit que :

$\langle z - x + p(x) - p(z), p(x) - p(z)\rangle \leqslant 0$, d'où l'on tire :

$$\|p(x) - p(z)\|^2 \leqslant - \langle z - x, p(x) - p(z)\rangle$$
$$\leqslant \|z - x\| \|p(x) - p(z)\| \text{ par Cauchy-Schwarz.}$$

Si $p(x) - p(z) = 0$, l'inégalité cherchée est vérifiée, et sinon, en simplifiant par $\|p(x) - p(z)\|$ on obtient bien :

$$\|p(x) - p(z)\| \leqslant \|z - x\| .$$

5.3. L'application $\phi : P \rightsquigarrow \int_{-1}^{1} P^2(x)dx$ est une forme quadratique sur $E = \mathbb{R}[X]$, de forme bilinéaire symétrique associée : $\varphi(P, Q) = \int_{-1}^{1} P(x)Q(x)dx$.

Si on vérifie que $\varphi(P, Q) = -i \int_0^{\pi} P(e^{i\theta})Q(e^{i\theta})e^{i\theta}d\theta$, pour $P = Q$ on aura le résultat.

Comme les deux membres de l'égalité dépendent cette fois linéairement de P et de Q, il suffit de vérifier cette égalité pour P et Q pris dans la base canonique de E.

Avec $P(x) = x^k$ et $Q(x) = x^l$, en posant $n = k + l$, on doit vérifier que $\int_{-1}^{1} x^n dx = \dfrac{1 - (-1)^{n+1}}{n+1} = -i \int_0^{\pi} e^{in\theta} e^{i\theta} d\theta$

$$= \frac{-i}{i(n+1)} \left[e^{i(n+1)\theta}\right]_0^{\pi}$$

$$= -\frac{(-1)^{n+1} - 1}{n+1}, \text{ ce qui me semble vrai.}$$

On a alors :

$$\int_{-1}^{1} P^2(x)dx = \int_{-1}^{1} \left(\sum_{0 \leqslant k, l \leqslant n} a_k a_l x^{k+l} \right) dx = \sum_{0 \leqslant k, l \leqslant n} \frac{a_k a_l}{k + l + 1}, \text{ et}$$

comme c'est un réel positif, c'est aussi :

$$\left| -i \int_0^{\pi} P^2(e^{i\theta}) e^{i\theta} d\theta \right| \leqslant \int_0^{\pi} \left| P^2(e^{i\theta}) \right| d\theta$$

$$\leqslant \int_0^{\pi} \sum_{k=0}^{n} a_k e^{ik\theta} \sum_{l=0}^{n} a_l e^{-il\theta} d\theta,$$

d'où

$$\sum_{0 \leqslant k, l \leqslant n} \frac{a_k a_l}{k + l + 1} \leqslant \sum_{0 \leqslant k, l \leqslant n} a_k a_l \int_0^{\pi} e^{i(k-l)\theta} d\theta ,$$

ce qui n'aboutit pas ! On ne jette pas le manche après la cognée : il faudrait intégrer entre 0 et 2π pour récupérer $\int_0^{2\pi} e^{i(k-l)\theta}d\theta = 0$ si $k \neq l$, 1 si $k = l$. Or, on a considéré en fait $I = \int_0^{\pi} P(e^{i\theta})P(e^{-i\theta})d\theta$. En posant $t = -\theta$, on a :

$$I = \int_0^{-\pi} P(e^{-it})P(e^{it})(-dt) = \int_{-\pi}^{0} P(e^{-i\theta})P(e^{i\theta})d\theta$$

donc $2I = \int_{-\pi}^{\pi} P(e^{i\theta})P(e^{-i\theta})d\theta$ et cette fois on va aboutir à la majoration :

$$\sum_{0 \leqslant k,\, l \leqslant n} \frac{a_k a_l}{k+l+1} \leqslant \frac{1}{2} \sum_{0 \leqslant k,\, l \leqslant n} a_k a_l \underbrace{\int_{-\pi}^{\pi} e^{i(k-l)\theta}d\theta}_{= 0 \text{ si } k \neq l,\ 2\pi \text{ si } k = l}$$

$$\leqslant \pi \sum_{k=0}^{n} a_k^2.$$

5.4. La matrice $B = A\,{}^tA$ est carrée d'ordre n, symétrique, associée à une forme quadratique ϕ positive sur $\mathbb{R}^n$, car si x de $\mathbb{R}^n$ est associé à la matrice colonne X on a :

$$\phi(x) = {}^tX(A\,{}^tA)X = {}^t({}^tAX)({}^tAX) = {}^tYY,$$

avec $Y = {}^tAX$, matrice colonne de p éléments $y_1, \ldots, y_p$, soit encore :

$$\phi(x) = \sum_{i=1}^{p} y_i^2 \geqslant 0.$$

La matrice B sera inversible si et seulement si ϕ est définie, donc si et seulement si $\phi(x) = 0 \Leftrightarrow x = 0$.

Or $\phi(x) = 0 \Leftrightarrow Y = 0 \Leftrightarrow X \in \text{Ker}\,({}^tA)$.

Mais ${}^tA$ est une matrice de rang n, d'une application linéaire de $\mathbb{R}^n$ dans $\mathbb{R}^p$: on a $n = \dim \mathbb{R}^n = \text{rang}\,{}^tA + \dim(\text{Ker}\,{}^tA)$, d'où $\text{Ker}\,{}^tA = \{0\}$ et finalement $\phi(x) = 0 \Leftrightarrow x = 0$: c'est dans la poche !

Le résultat est acquis pour $A\,{}^tA$, avec rang (A) = nombre de lignes de A, il le sera donc pour ${}^tAA = {}^tA({}^tA)$ si le rang de

${}^tA$ = rang (A) = nombre de lignes de ${}^tA = p$, donc si A de $\mathcal{M}_{n,p}(\mathbb{R})$ est de rang p, la matrice ${}^tAA$ est inversible.

5.5. La matrice A de Δ dans la base canonique donnée est triangulaire inférieure, avec des 1 sur la diagonale et des – 1 qui bordent la diagonale, « en dessous », tout le reste étant nul donc det A = 1 : Δ *est inversible.*

On sait, (quitte à rejustifier), que $|||\Delta^{-1}|||^2$ est le rayon spectral de l'endomorphisme $(\Delta^{-1})^*\Delta^{-1}$, endomorphisme de matrice symétrique ${}^tA^{-1}A^{-1} = (A{}^tA)^{-1}$, matrice diagonalisable de valeurs propres les inverses des valeurs propres de $A{}^tA$. Finalement, $|||\Delta^{-1}|||$ est $1/(\text{inf des valeurs propres de } A{}^tA)^{1/2}$, les valeurs propres de $A{}^tA$ étant > 0.

Soit :

$$B_n = A{}^tA = \begin{pmatrix} 1 & 0 & & \\ -1 & 1 & \ddots & \\ & \ddots & \ddots & 0 \\ & & -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 & & \\ 0 & 1 & \ddots & 0 \\ & \ddots & \ddots & -1 \\ 0 & & & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & -1 & & \\ -1 & 2 & \ddots & \\ & \ddots & 2 & -1 \\ & & -1 & 2 \end{pmatrix}.$$

La première ligne est à part, et pour tenir compte de ce particularisme, on calcule le polynôme caractéristique, $P_n(\lambda) = \det(B_n - \lambda I_n)$ en partant de la dernière ligne.

On obtient, pour $n \geqslant 3$, la relation :

$$P_n(\lambda) = (2-\lambda)P_{n-1}(\lambda) - P_{n-2}(\lambda),$$

qui, jointe aux égalités $P_1(\lambda) = 1-\lambda$ et $P_2(\lambda) = (1-\lambda)(2-\lambda)-1$, détermine les P_n.

Pour un λ complexe fixé, on a une suite récurrente double, d'équation caractéristique $r^2 - (2-\lambda)r + 1 = 0$, de discriminant $(2-\lambda)^2 - 4 = -4\left(1 - \left(\frac{2-\lambda}{2}\right)^2\right)$.

En posant $\frac{2-\lambda}{2} = \cos\theta$, (sur $\mathbb{C}$, c'est possible), ce discriminant vaut $-4\sin^2\theta$, et les racines de l'équation caractéristique s'écrivent $\frac{2-\lambda \pm 2i\sin\theta}{2} = \cos\theta \pm i\sin\theta$, et par cette « astuce », (à méditer), on obtient $P_n(\lambda)$ du type $P_n(\lambda) = ae^{in\theta} + be^{-in\theta}$, λ étant relié à θ par l'égalité $2-\lambda = 2\cos\theta$.

On calcule a et b en résolvant le système obtenu pour $n = 1$ et 2.

On a $P_1(\lambda) = 1-\lambda = e^{i\theta} + e^{-i\theta} - 1$, puis :

$$P_2(\lambda) = (1-\lambda)(2-\lambda) - 1 = (e^{i\theta} + e^{-i\theta} - 1)(e^{i\theta} + e^{-i\theta}) - 1$$
$$= (e^{i\theta} + e^{-i\theta})^2 - e^{i\theta} - e^{-i\theta} - 1 = e^{2i\theta} + e^{-2i\theta} - e^{i\theta} - e^{-i\theta} + 1,$$

d'où le système :

$$\begin{cases} ae^{i\theta} + be^{-i\theta} = e^{i\theta} + e^{-i\theta} - 1 \\ ae^{2i\theta} + be^{-2i\theta} = e^{2i\theta} + e^{-2i\theta} - e^{i\theta} - e^{-i\theta} + 1 \end{cases} \left| \begin{matrix} -e^{-i\theta} \\ 1 \end{matrix} \right., \quad \left| \begin{matrix} -e^{i\theta} \\ 1 \end{matrix} \right.,$$

qui conduit aux solutions :

$$\begin{cases} a(e^{2i\theta} - 1) = -1 - e^{-2i\theta} + e^{-i\theta} + e^{2i\theta} + e^{-2i\theta} - e^{i\theta} - e^{-i\theta} + 1 = e^{2i\theta} - e^{i\theta} \\ b(e^{-2i\theta} - 1) = -e^{2i\theta} - 1 + e^{i\theta} + e^{2i\theta} + e^{-2i\theta} - e^{i\theta} - e^{-i\theta} + 1 = e^{-2i\theta} - e^{-i\theta}, \end{cases}$$

ou : $a = \dfrac{e^{3i\frac{\theta}{2}}\left(e^{i\frac{\theta}{2}} - e^{-i\frac{\theta}{2}}\right)}{e^{i\theta}(e^{i\theta} - e^{-i\theta})} = \dfrac{\sin\frac{\theta}{2}}{\sin\theta} e^{i\frac{\theta}{2}}$ et

$b = \dfrac{e^{-3i\frac{\theta}{2}}\left(e^{-i\frac{\theta}{2}} - e^{i\frac{\theta}{2}}\right)}{e^{-i\theta}(e^{-i\theta} - e^{i\theta})} = \dfrac{\sin\frac{\theta}{2}}{\sin\theta} e^{-i\frac{\theta}{2}}$, ce qui conduit à une expression du polynôme caractéristique valant :

$$P_n(\lambda) = \frac{\sin\frac{\theta}{2}}{\sin\theta}\left(e^{i(2n+1)\frac{\theta}{2}} + e^{-i(2n+1)\frac{\theta}{2}}\right) = 2\frac{\sin\frac{\theta}{2}}{\sin\theta}\cos(2n+1)\frac{\theta}{2}.$$

Cette expression s'annule pour $\theta_k = \dfrac{(1+2k)\pi}{2n+1}$, $0 \leqslant k \leqslant n-1$ ce qui correspond à $\lambda_k = 2\left(1 - \cos\dfrac{(1+2k)\pi}{2n+1}\right)$ et vu les variations (monoto-

nie) de la fonction cosinus, on a n valeurs distinctes de λ qui annulent un polynôme de degré n : inutile d'aller plus loin, on a les valeurs propres de $B_n = A\,{}^tA$.

La plus petite est $\lambda_1 = 2\left(1 - \cos\dfrac{\pi}{2n+1}\right) = 4\sin^2\dfrac{\pi}{2(2n+1)}$ donc $|||\Delta^{-1}||| = \dfrac{1}{2\sin\dfrac{\pi}{2(2n+1)}}$, ce que l'on voulait.

5.6. Le 1°) consiste à mettre a de GL(E) sous sa forme de décomposition polaire. Comme l'intérêt de u orthogonale est de vérifier ${}^tu = u^{-1}$, et d'intervenir dans les réductions des matrices symétriques, on va considérer ${}^taa$, et même, si on suppose que $a = us$, ceci donnera ${}^taa = {}^ts\,{}^tuus = s^2$: la matrice symétrique s, (ou l'opérateur...) doit vérifier l'équation $s^2 = {}^taa$.

Partant de a, on vérifie que ${}^taa$ est symétrique, positive, ($\forall x$ vecteur colonne de $\mathbb{R}^n$, ${}^tx({}^taa)x = {}^tyy = \sum_{j=1}^{n} (y_j)^2 \geqslant 0$, avec des notations évidentes, si $y = ax$). De plus ${}^taa$ est régulière, (comme la matrice a), donc ${}^taa$ est symétrique définie positive.

Il existe alors $q \in O(E)$ telle que $q^{-1}({}^taa)q = {}^tq\,{}^taaq$ soit une matrice diagonale, $D = \text{diag}\,(\lambda_1, ..., \lambda_n)$ avec des $\lambda_j > 0$.

En posant $\mu_j = \sqrt{\lambda_j}$ et $\Delta = \text{diag}\,(\mu_1, ..., \mu_n)$, on a ${}^taa = q\Delta^2\,{}^tq = (q\Delta\,{}^tq)^2$: avec $s = q\Delta\,{}^tq$, on a trouvé s endomorphisme défini positif, (ou matrice définie positive) telle que ${}^taa = s^2$.

S'il existe s', défini positif vérifiant $s'^2 = {}^taa = s^2$, on a forcément $s' = s$.

En effet, avec d valeur propre de s' et x vecteur propre associé, on a $s'^2(x) = d^2x = ({}^taa)(x)$, donc d^2 est l'un des λ_j, et d, (> 0), est l'un des μ_j.

De plus, avec j tel que $d^2 = \lambda_j$ et x dans $\text{Ker}\,(s' - d\text{id}_E)$, on a $s^2(x) = \lambda_j x$, donc $\text{Ker}\,(s' - d\text{id}_E) \subset \text{Ker}\,(s^2 - \lambda_j\text{id}_E)$.

Mais alors en notant $\lambda_1, ..., \lambda_k$ les valeurs propres distinctes de ${}^t aa = s^2$, de multiplicités respectives $\alpha_1, ..., \alpha_k$; puis $d_1, ..., d_r$ les valeurs propres distinctes de s', on a une injection σ de $\{d_1, ..., d_r\}$ dans $\{\lambda_1, ..., \lambda_k\}$, définie par $\sigma(i) =$ le seul indice j tel que $(d_i)^2 = \lambda_j$, d'où déjà l'inégalité $r \leqslant k$, et, avec $(d_i)^2 = \lambda_{\sigma(i)}$ pour $1 \leqslant i \leqslant r$, on a, ($s'$ symétrique étant diagonalisable) :

$$E = \bigoplus_{i=1}^{r} \operatorname{Ker}(s' - d_i \mathrm{id}_E), \text{ avec } \operatorname{Ker}(s' - d_i \mathrm{id}_E) \subset \operatorname{Ker}(s^2 - \lambda_{\sigma(i)} \mathrm{id}_E),$$

et aussi $E = \bigoplus_{j=1}^{k} \operatorname{Ker}(s^2 - \lambda_j \mathrm{id}_E)$: forcément $r = k$ et $\operatorname{Ker}(s' - d_i \mathrm{id}_E) = \operatorname{Ker}(s^2 - \lambda_{\sigma(i)} \mathrm{id}_E)$.

Mais alors, sur le sous-espace propre de ${}^t aa$, de valeur propre λ, s' est l'homothétie de rapport $\sqrt{\lambda}$: elle est parfaitement déterminée, donc s' l'est sur E, somme directe des sous-espaces propres de ${}^t aa$.

Si on pose alors, avec s symétrique défini positif tel que ${}^t aa = s^2$, $u = as^{-1}$, on aura ${}^t uu = {}^t(s^{-1}){}^t aas^{-1} = s^{-1}s^2s^{-1} = \mathrm{id}_E$, (car s^{-1} est symétrique, comme s), donc u est orthogonal et on obtient bien $a = us$, avec s unique, donc u aussi est unique.

2°) On écrit $a = us$, avec, on l'a vu, $s^2 = {}^t aa$, u orthogonal et s symétrique défini positif.

Si v parcourt le groupe orthogonal, $w = vu$ le parcourt aussi, et comme $va = (vu)s$, on a :

$$\operatorname*{Sup}_{v \in O(E)} \operatorname{Trace}(va) = \operatorname*{Sup}_{w \in O(E)} \operatorname{Trace}(ws).$$

Mais s, symétrique, est diagonalisable dans le groupe orthogonal : soit $\mathscr{B} = (e_1, ..., e_n)$ une base orthonormée de vecteurs propres pour s, pour les valeurs propres, distinctes ou non, $\lambda_1, ..., \lambda_n$, on aura $\langle ws(e_i), e_i \rangle = \langle \lambda_i w(e_i), e_i \rangle = \lambda_i \langle w(e_i), e_i \rangle$, terme diagonal de la matrice de ws dans la base $\mathscr{B}$, et $\operatorname{Trace}(ws) = \sum_{i=1}^{n} \lambda_i \langle w(e_i), e_i \rangle$.

Comme w est orthogonal, et $\mathscr{B}$ orthonormée $\langle w(e_i), e_i \rangle \leqslant \|w(e_i)\| \|e_i\| = 1$, et :

$$\operatorname{Trace}(ws) \leqslant \sum_{i=1}^{n} \lambda_i \text{ ; et pour } w = \mathrm{id}_E, \text{ on a :}$$

Trace $(\mathrm{id}_E s) = \sum_{i=1}^{n} \lambda_i$ d'où finalement :

$$\sup_{v \in O(E)} (\text{Trace } va) = \sum_{i=1}^{n} \lambda_i = \text{trace } s, \text{ avec } s^2 = {}^t aa .$$

3°) On repart de $a = us$, avec $u \in O(E)$, donc il y a deux cas suivant que u est dans $O^+(E) = SO(E)$ ou non.

Si $u \in SO(E)$, si v parcourt le sous-groupe $SO(E)$, $w = vu$ le parcourt aussi, le raisonnement précédent s'applique et conduit à $\sup_{v \in SO(E)} (\text{Trace } va) = \text{trace } s$, puisque $\mathrm{id}_E \in SO(E)$.

On peut remarquer que $\det a = \det u \det s$, avec $\det s > 0$, donc $u \in SO(E) \Leftrightarrow \det u = 1 \Leftrightarrow \det a > 0$.

Si maintenant $\det a < 0$, $\det u = -1$, et avec $va = (vu)s = ws$, cette fois w parcourt $O^-(E)$, et en prenant une base orthonormée directe dans laquelle $s = \mathrm{diag}(\lambda_1, ..., \lambda_n)$, avec $0 < \lambda_1 \leqslant \lambda_2 \leqslant ... \leqslant \lambda_n$, on cherche

$$\sup_{w \in O^-(E)} \text{Trace } (w \cdot \mathrm{diag}(\lambda_1, ..., \lambda_n)) .$$

Comme -1 est valeur propre de l'isométrie indirecte w, on a trace $w \leqslant -1 + (n-1)$, car, en notant $\mu_2, ..., \mu_n$ les autres valeurs propres, réelles ou complexes, mais de module 1, et de somme réelle, on a :

Trace w = un nombre réel $= -1 + \mu_2 + ... + \mu_n$, avec

$$\mu_2 + ... + \mu_n \leqslant |\mu_2 + ... + \mu_n| \leqslant |\mu_2| + ... + |\mu_n| = n - 1 .$$

C'est encore $\sum_{i=1}^{n} w_{ii} \leqslant n - 2$, donc :

$$1 + w_{11} \leqslant \sum_{i=2}^{n} (1 - w_{ii}), \text{ d'où :}$$

$$\text{trace } (w \text{ diag } (\lambda_1, ..., \lambda_n)) = \sum_{i=1}^{n} \lambda_i w_{ii}$$

$$\leqslant \lambda_1 \left(-1 + \sum_{i=2}^{n} (1 - w_{ii}) \right) + \sum_{i=2}^{n} w_{ii} \lambda_i .$$

Or, $-1 \leqslant w_{ii} \leqslant 1$, (dans une matrice orthogonale, les termes sont de module inférieur ou égal à 1), et comme $\lambda_1 \leqslant \lambda_i$, on a $\lambda_1(1-w_{ii}) \leqslant \lambda_i(1-w_{ii})$ pour $i \geqslant 2$, d'où finalement

$$\begin{aligned}\text{trace}\,(w\ \text{diag}\,(\lambda_1, ..., \lambda_n)) &\leqslant -\lambda_1 + \sum_{i=2}^{n} (1 - w_{ii} + w_{ii})\lambda_i \\ &\leqslant -\lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_n.\end{aligned}$$

Pour $w = \text{diag}\,(-1, 1, 1, ..., 1)$, ce sup est atteint et finalement, si $\det a < 0$, le sup est $-\lambda_1 + \lambda_2 + \lambda_3 + ... + \lambda_n$.

J'ai bien cru ne pas l'achever celui-là !

5.7. On considère $\mathbb{R}^n$ euclidien canonique, la base $\mathscr{B} = (e_1, ..., e_n)$ canonique étant donc orthonormée.

L'endomorphisme α de matrice symétrique A dans la base $\mathscr{B}$ est auto-adjoint, donc diagonalisable dans le groupe orthogonal : il existe une base orthonormée $\mathscr{C} = (\varepsilon_1, ..., \varepsilon_n)$ de vecteurs propres pour α, l'indexation étant telle que ε_i soit vecteur propre pour la valeur propre λ_i.

On a alors :

$a_{jj} = \langle e_j, \alpha(e_j)\rangle$ puisque $\alpha(e_j) = \sum_{i=1}^{n} a_{ij} e_i$ et que la base $\mathscr{B}$ est orthonormée.

Avec $P = (p_{uv})_{1 \leqslant u, v \leqslant n}$, matrice de passage de la base $\mathscr{B}$ à $\mathscr{C}$, on a $P^{-1} = {}^tP$, donc $e_j = \sum_{u=1}^{n} p_{ju}\varepsilon_u$, (on se promène dans la $j^{\text{ième}}$ colonne de P^{-1}, donc la $j^{\text{ième}}$ ligne de P), avec $p_{ju} = \langle e_j, \varepsilon_u\rangle$ puisque $\mathscr{C}$ est orthonormée.

$$\begin{aligned}\text{Donc } a_{jj} &= \langle e_j, \sum_{u=1}^{n} p_{ju}\alpha(\varepsilon_u)\rangle \\ &= \sum_{u=1}^{n} p_{ju}\langle e_j, \lambda_u\varepsilon_u\rangle \\ &= \sum_{u=1}^{n} \lambda_u p_{ju}\langle e_j, \varepsilon_u\rangle = \sum_{u=1}^{n} \lambda_u \langle e_j, \varepsilon_u\rangle^2,\end{aligned}$$

et, vu l'indexation décroissante des valeurs propres, on a :

$$a_{jj} \leqslant \sum_{u=1}^{k} \lambda_u \langle e_j, \varepsilon_u \rangle^2 + \lambda_k \sum_{u=k+1}^{n} \langle e_j, \varepsilon_u \rangle^2 .$$

Or, comme on a remarqué que $\langle e_j, \varepsilon_u \rangle = p_{ju}$ est, (si u varie), le terme générique de la $j^{\text{ième}}$ ligne de P, matrice orthogonale, on a :

$$\sum_{u=1}^{n} \langle e_j, \varepsilon_u \rangle^2 = 1 \text{ d'où :}$$

$$\sum_{u=k+1}^{n} \langle e_j, \varepsilon_u \rangle^2 = 1 - \sum_{u=1}^{k} \langle e_j, \varepsilon_u \rangle^2 .$$

Il en résulte l'inégalité :

$$a_{jj} \leqslant \lambda_k + \sum_{u=1}^{k} (\lambda_u - \lambda_k) \langle e_j, \varepsilon_u \rangle^2, \text{ donc}$$

$$\sum_{j=1}^{k} a_{jj} \leqslant k\lambda_k + \sum_{j=1}^{k} \sum_{u=1}^{k} (\lambda_u - \lambda_k) \langle e_j, \varepsilon_u \rangle^2$$

$$\leqslant k\lambda_k + \sum_{u=1}^{k} (\lambda_u - \lambda_k) \left(\sum_{j=1}^{k} \langle e_j, \varepsilon_u \rangle^2 \right).$$

Mais, pour u fixé, $\sum_{j=1}^{n} \langle e_j, \varepsilon_u \rangle^2 = 1$, (somme des carrés des termes de la $u^{\text{ième}}$ colonne de la matrice orthogonale P), donc $\sum_{j=1}^{k} \langle e_j, \varepsilon_u \rangle^2 \leqslant 1$, et $\lambda_u - \lambda_k$ étant $\geqslant 0$ pour $u \leqslant k$, il vient :

$$\sum_{j=1}^{k} a_{jj} \leqslant k\lambda_k + \sum_{u=1}^{k} (\lambda_u - \lambda_k) = \lambda_1 + \lambda_2 + \ldots + \lambda_k .$$

On se demande toujours comment on obtient cela !

5.8. La propriété est évidente si dim E = 1 ou 2. On la justifie par récurrence sur n, en la supposant vraie pour dim E $\leqslant n$ et en considérant E de dimension $n+1$, $(n \geqslant 2)$.

Comme p et q sont autoadjoints, (p projection orthogonale sur F, parallèlement à $G = F^{\perp}$ admet F et G comme sous-espaces propres orthogonaux, pour les valeurs propres 1 et 0, d'où une base orthonormée de E dans laquelle la matrice de p est diagonale), on a $p-q$ autoadjoint, donc diagonalisable dans le groupe orthogonal.

En particulier il existe $x \neq 0$ et s réel tels que $(p-q)(x) = sx$. Soit $A = \text{Vect}(x, p(x))$, (plan ou droite), comme $p(p(x)) = p(x)$, on a $p(A) \subset A$; mais on a aussi, pour $y = \alpha x + \beta p(x)$ dans A :

$q(y) = \alpha q(x) + \beta q(p(x))$, avec $p(x) = q(x) + sx$, donc :

$$\begin{aligned} q(y) &= \alpha q(x) + \beta q^2(x) + s\beta q(x) = (\alpha + (1+s)\beta) q(x) \\ &= (\alpha + (1+s)\beta)(p(x) - sx) \in A, \ (\alpha, s \text{ et } \beta \text{ scalaires}). \end{aligned}$$

On a donc le sous-espace A, de dimension 1 ou 2, stable par p et q, donc $A^{\perp}$ l'est par $p^* = p$ et $q^* = q$, avec $A^{\perp}$ euclidien de dimension $n + 1 - (1 \text{ ou } 2) \leqslant n$: l'hypothèse de récurrence s'applique pour $A^{\perp}$.

En fait on a même obtenu une somme directe orthogonale de sous-espaces stables par p et q, de dimension 1 ou 2.

5.9. Pour tout couple (x, y) de E^2, on a :

$$\langle f(x), f(y) \rangle = \langle x, f^* f(y) \rangle = \langle x, g * g(y) \rangle = \langle g(x), g(y) \rangle .$$

Mais alors, $x \in \text{Ker } f \Leftrightarrow \langle f(x), f(x) \rangle = 0$

$$\Leftrightarrow \langle g(x), g(x) \rangle = 0$$

$$\Leftrightarrow x \in \text{Ker } g,$$

donc f et g ont même noyau, et aussi même rang r.

Soit alors $\{e_1, ..., e_r\}$ une base orthonormée de Im g, et $x_1, ..., x_r$ tels que, pour $1 \leqslant i \leqslant r$, $g(x_i) = e_i$.

Pour $1 \leqslant i \leqslant r$ et $1 \leqslant j \leqslant r$, on a :

$\langle f(x_i), f(x_j) \rangle = \langle g(x_i), g(x_j) \rangle = \langle e_i, e_j \rangle$, donc la famille des $f(x_i)$ est orthonormée, donc libre et de cardinal r dans Im f de dimension r : c'est une base de Im f.

On peut alors compléter les deux familles orthonormées des $f(x_i)$ d'une part, et des $g(x_i)$ d'autre part, en deux bases orthonormées de E :

$\mathscr{B}_1 = \{g(x_1), ..., g(x_r) \ ; \ e_{r+1}, ..., e_n\}$ et,

$\mathscr{B}_2 = \{f(x_1), ..., f(x_r) \ ; \ \varepsilon_{r+1}, ..., \varepsilon_n\}$.

Avoir $f = sg$, impose les égalités $f(x_j) = s(g(x_j))$.

On définit donc l'opérateur linéaire s, tout simplement par :

$s(g(x_j)) = f(x_j)$, pour $1 \leqslant j \leqslant r$ et,

$s(e_{r+p}) = \varepsilon_{r+p}$, pour $1 \leqslant p \leqslant n-r$.

On a s opérateur orthogonal, (envoie une base orthonormée sur une autre base orthonormée).

Il reste à voir si, pour tout x de E, $f(x) = sg(x)$.

Soit x dans E, $g(x) \in \text{Im } g = \text{Vect } \{g(x_1), ..., g(x_r)\}$, donc il existe r scalaires $\alpha_1, ..., \alpha_r$ tels que $g(x) = \alpha_1 g(x_1) + ... + \alpha_r g(x_r)$ soit encore $g(x - \alpha_1 x_1 - ... - \alpha_r x_r) = 0$.

Mais alors, (Ker f = Ker g), on a aussi :

$f(x - \alpha_1 x_1 - ... - \alpha_r x_r) = 0$, soit encore :

$$\begin{aligned} f(x) &= \alpha_1 f(x_1) + ... + \alpha_r f(x_r) \\ &= \alpha_1 s(g(x_1)) + ... + \alpha_r s(g(x_r)) \\ &= s(\alpha_1 g(x_1) + ... + \alpha_r g(x_r)) = s(g(x)), \end{aligned}$$

d'où $f = s \circ g$ et le résultat.

Soit maintenant une famille $\{u_1, ..., u_n\}$ de n vecteurs dans E euclidien de dimension n, et sa matrice de Gramm, $\mathcal{G}$.

On suppose qu'il existe une base orthonormée $\mathcal{B} = \{e_1, ..., e_n\}$ et un projecteur orthogonal p tel que $u_i = p(e_i)$, pour $i = 1, ..., n$.

En se plaçant dans une base orthonormée de vecteurs propres pour p, (vérifiant $p^2 = p$), on a une matrice diagonale, donc ${}^t p = p$, et réciproquement, si p vérifie $p^2 = p$ et ${}^t p = p^* = p$, c'est un projecteur orthogonal.

La $j^{\text{ième}}$ colonne de la matrice P de p dans la base $\mathcal{B}$ est celle des composantes de $p(e_j)$ dans $\mathcal{B}$, orthonormée, c'est donc celle des

$$\begin{aligned} \langle e_i, p(e_j) \rangle &= \langle e_i, p^2(e_j) \rangle = \langle e_i, p * p(e_j) \rangle \\ &= \langle p(e_i), p(e_j) \rangle = \langle u_i, u_j \rangle : \end{aligned}$$

c'est la matrice $\mathcal{G}$, qui a donc pour seules valeurs propres possibles 0 et 1, (p projecteur).

Réciproquement, on suppose que la matrice de Gramm, $\mathcal{G}$, qui est symétrique réelle, a son spectre contenu dans $\{0, 1\}$. Soit une base orthonormée $\mathcal{B} = \{\varepsilon_1, ..., \varepsilon_n\}$ de E, et g l'opérateur de matrice $\mathcal{G}$ dans $\mathcal{B}$.

Comme ses sous-espaces propres sont orthogonaux et en somme directe, ($\mathscr{G}$ symétrique), pour les valeurs propres 0 et 1, g est un projecteur orthogonal.

On définit l'application linéaire f sur E par les relations : $f(\varepsilon_i) = u_i$, pour $1 \leqslant i \leqslant n$.

Le terme général, $\langle u_i, u_j \rangle$ de la matrice $\mathscr{G}$ de g dans la base orthonormée $\mathscr{B}$ vérifie :

$$\langle u_i, u_j \rangle = \langle \varepsilon_i, g(\varepsilon_j) \rangle = \langle f(\varepsilon_i), f(\varepsilon_j) \rangle = \langle \varepsilon_i, f^* f(\varepsilon_j) \rangle .$$

Mais $g = g^2 = g * g$, (g projecteur orthogonal), donc l'égalité :

$\langle u_i, u_j \rangle = \langle \varepsilon_i, g(\varepsilon_j) \rangle$ donne :

$\langle \varepsilon_i, g * g(\varepsilon_j) \rangle = \langle \varepsilon_i, f^* f(\varepsilon_j) \rangle$, et c'est valable pour tout i, j dans $\{1, ..., n\}$, d'où en fait $g * g$ et $f * f$ égales, car ayant même matrice dans la base $\mathscr{B}$.

Il existe alors s, opérateur orthogonal, tel que $f = sg$.

En prenant $p = sgs^{-1}$, p est semblable à g donc c'est un projecteur orthogonal, et en posant $e_i = s(\varepsilon_i)$, on a une base orthonormée $\{e_1, ..., e_n\}$ telle que, pour tout i, $p(e_i) = s \circ g \circ s^{-1} \circ s(\varepsilon_i)$

$$= s(g(\varepsilon_i)) = f(\varepsilon_i) = u_i,$$

c'est gagné !

5.10. Le produit scalaire étant continu de $E \times E$ dans $\mathbb{R}$, f est continue. Comme on est en dimension finie, S est un fermé borné de E, donc un compact, l'espace produit S^3 est un compact de E^3, d'image continue un compact de $\mathbb{R}$.

Si dim $E \geqslant 2$, S est de plus connexe par arcs, (si u et v sont de norme 1, dans tout plan, euclidien, contenant 0, u et v, il existe un arc de cercle Γ, joignant u et v, contenu dans S). Donc S^3 est aussi connexe par arcs, et $f(S^3)$ est un connexe compact de $\mathbb{R}$: c'est un segment.

Or $\|u\| = \|v\| = \|w\|$ donne $f(u, v, w) \leqslant 3$, maximum atteint pour $u = v = w$.

De plus $f(u, v, w) = \frac{1}{2}(\|u + v + w\|^2 - 3) \geqslant -\frac{3}{2}$, minimum atteint pour tout point, (de S^3), tel que $u + v + w = 0$, et il y en a car dans un plan euclidien assimilé à $\mathbb{C}$, si $\|u\| = 1$, u, ju et $j^2 u$ vérifient cette égalité, donc $f(S^3) = [-3/2, 3]$, *si* dim $E \geqslant 2$.

Si dim E = 1, S n'est plus connexe, mais formé de deux vecteurs, e et $-e$, donc $\langle u, v\rangle = 1$ ou -1 et on a le triplet (u, v, w) du type (e, e, e) ou $(e, e, -e)$, ou leurs opposés, mais tout ceci donne $f(S^3) = \{-1, 3\}$.

5.11. Pour A dans $\mathcal{M}_n(\mathbb{R})$, on a $A = \frac{1}{2}(A + {}^tA) + \frac{1}{2}(A - {}^tA)$, et la matrice $B = \frac{1}{2}(A - {}^tA)$ est antisymétrique, donc pour U matrice orthogonale, on aura $U^{-1}BU = {}^tUBU$ encore antisymétrique, donc à éléments diagonaux nuls. Si on a trouvé U telle que $U^{-1}A'U$, avec $A' = \frac{1}{2}(A + {}^tA)$, ait ses termes diagonaux nuls, il en sera de même pour $U^{-1}(A' + B)U$ et le problème sera résolu.

De plus trace (A) = trace $\left(\frac{1}{2}(A + {}^tA)\right) = 0$, donc on résoud le problème avec A symétrique de trace nulle, et là, on travaille par récurrence sur n.

Si $n = 1$, A = (0), matrice (1, 1) et le problème est résolu.

On le suppose aussi résolu à l'ordre $n - 1$.

Soit A symétrique réelle d'ordre n, de trace nulle. Elle est diagonalisable dans le groupe orthogonal et si $\lambda_1, ..., \lambda_n$ sont les valeurs propres, on a, soit $\lambda_1 = \lambda_2 = ... = \lambda_n = 0$, auquel cas $A = 0$ et le problème est résolu ; soit il existe des $\lambda_i \neq 0$, mais alors, (trace nulle), on a des $\lambda_i > 0$ et d'autres < 0 et la forme quadratique de matrice A admet des vecteurs isotropes non nuls.

On introduit $E = \mathbb{R}^n$, euclidien canonique, $\mathcal{B} = (e_1, ..., e_n)$ la base orthonormée canonique, et ϕ forme quadratique de matrice A dans cette base : elle admet ε_1, vecteur isotrope non nul, de norme euclidienne 1.

On prend une base orthonormée $\mathcal{C}$ de $\{\varepsilon_1\}^\perp$, (orthogonal pour la structure euclidienne), donc $\mathcal{B}_1 = \{\varepsilon_1\} \cup \mathcal{C}$ est base orthonormée de E et P_1, matrice de passage de $\mathcal{B}$ à $\mathcal{B}_1$ est orthogonale.

La matrice $A_1 = P_1^{-1}AP_1$, semblable à A est de trace nulle, et comme $P_1^{-1} = {}^tP_1$, c'est $A_1 = {}^tP_1AP_1$, symétrique comme A. De plus

le terme de la première ligne première colonne vaut $\varphi(\varepsilon_1, \varepsilon_1) = \phi(\varepsilon_1) = 0$, donc on a une écriture « blocs » de A_1 en :

$$A_1 = \left(\begin{array}{c|c} 0 & L \\ \hline {}^tL & A' \end{array}\right), \text{ avec A' symétrique d'ordre } n-1, \text{ de trace nulle car trace } A_1 = 0 = \text{trace A'}.$$

L'hypothèse de récurrence s'applique, donc il existe P'_2 orthogonale d'ordre $n-1$ telle que $P'^{-1}_2 A' P'_2$ soit à coefficients diagonaux nuls.

Il reste à vérifier que $P_2 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P'_2 \end{array}\right)$ est orthogonale réelle d'ordre n, (vrai car P'_2 est orthogonale), et que :

$$P_2^{-1} A_1 P_2 = \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P'^{-1}_2 \end{array}\right) \left(\begin{array}{c|c} 0 & L \\ \hline {}^tL & A' \end{array}\right) \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P'_2 \end{array}\right)$$

$$= \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & P'^{-1}_2 \end{array}\right) \left(\begin{array}{c|c} 0 & LP'_2 \\ \hline {}^tL & A'P'_2 \end{array}\right) = \left(\begin{array}{c|c} 0 & LP'_2 \\ \hline P'^{-1}_2 {}^tL & P'^{-1}_2 A' P'_2 \end{array}\right)$$

est bien à éléments diagonaux nuls, ce qui est vrai pour $P'^{-1}_2 A' P'_2$.

Avec $A_1 = P_1^{-1} A P_1$, on a finalement $(P_1 P_2)^{-1} A (P_1 P_2)$ à termes diagonaux nuls, avec $P_1 P_2$ matrice orthogonale.

5.12. Il s'agit de relier les polynômes caractéristiques de A et de B, or $\det(B - \lambda I_n)$ est le cofacteur de l'élément de la dernière ligne et dernière colonne de $A - \lambda I_{n+1}$, cofacteur qui intervient, pour λ non valeur propre de A, dans la matrice $(A - \lambda I_{n+1})^{-1}$, que nous allons considérer, après avoir diagonalisé A. Allons-y !

Il existe P orthogonale d'ordre $n+1$ telle que :

$P^{-1} A P = {}^tP A P = \text{diag}(\lambda_1, \lambda_2, ..., \lambda_{n+1}) = D$, donc :

$A - \lambda I_{n+1} = PDP^{-1} - \lambda I_{n+1} = P(D - \lambda I_{n+1}) P^{-1}$, et

$(A - \lambda I_{n+1})^{-1} = P(D - \lambda I_{n+1})^{-1} P^{-1}$, ceci, pour tout λ non valeur propre de A bien sûr.

C'est donc encore :

$$\frac{1}{\det(A-\lambda I_{n+1})} \cdot {}^t(\text{com}(A-\lambda I_{n+1})) = P \operatorname{diag}\left(..., \frac{1}{\lambda_i-\lambda}, ...\right) {}^tP,$$

puisque P est orthogonale.

Comme $A-\lambda I_{n+1}$ est symétrique, il en est de même de sa comatrice, donc il y a une transposition de matrice en trop, et, en prenant l'élément de la $(n+1)^{\text{ième}}$ ligne, $(n+1)^{\text{ième}}$ colonne, et en notant $p_1, p_2 \dots p_{n+1}$ la dernière ligne de P on a :

$$\frac{\det(B-\lambda I_n)}{\det(A-\lambda I_{n+1})} = \begin{pmatrix} & & \\ & & \\ & & \\ p_1 & \cdots & p_{n+1} \end{pmatrix} \begin{pmatrix} \frac{p_1}{\lambda_1-\lambda} \\ \vdots \\ \frac{p_{n+1}}{\lambda_{n+1}-\lambda} \end{pmatrix},$$

soit finalement, en notant $\chi_A(\lambda)$ et $\chi_B(\lambda)$ les polynômes caractéristiques de A et B :

$$\frac{\chi_B(\lambda)}{\chi_A(\lambda)} = \sum_{i=1}^{n+1} \frac{(p_i)^2}{\lambda_i-\lambda} = f(\lambda),$$

relation valable pour tout λ non valeur propre de A.

Sur $\mathbb{R}-\{\lambda_i\}$, la fonction $\lambda \rightsquigarrow \frac{1}{\lambda_i-\lambda}$, de dérivée $\frac{1}{(\lambda_i-\lambda)^2}$ est croissante.

Si on suppose tous les λ_i distincts et les $p_i \neq 0$, la fonction f est croissante sur les n intervalles $]\lambda_{i+1}, \lambda_i[$ pour i variant de 1 à n, avec $\lim_{\lambda \to \lambda_{i+1}^+} f(\lambda) = -\infty$, (c'est ce que fait $\frac{(p_{i+1})^2}{\lambda_{i+1}-\lambda}$, les autres termes ayant une limite finie), alors que $\lim_{\lambda \to \lambda_i^-} f(\lambda) = +\infty$.

Dans ce cas la fonction f admet n zéros, $\mu_1, ..., \mu_n$ avec, vu l'indexation adoptée, $\mu_1 \in]\lambda_2, \lambda_1[$, $\mu_2 \in]\lambda_3, \lambda_2[$...

Comme f est une fraction rationnelle de numérateur le polynôme caractéristique de B, de degré n, on a bien trouvé les n valeurs propres de B, entrelacées avec celles de A.

Si les λ_i sont tous distincts, mais si $p_i = 0$, le terme en $\frac{1}{\lambda_i-\lambda}$ ne figure pas dans la décomposition en éléments simples de $\frac{\chi_B(\lambda)}{\chi_A(\lambda)}$, or c'est un

pôle simple, donc λ_i est zéro de $\chi_B(\lambda)$, de plus, si p_{i-1} et p_{i+1} sont non nuls, la fonction f est encore croissante de $-\infty$ à $+\infty$ sur $]\lambda_{i+1}, \lambda_{i-1}[$ avec $\lim_{\lambda \to \lambda_i} f(\lambda)$ existe et est $\neq 0$ si λ_i zéro simple de $\chi_B(\lambda) = 0$, (nulle si zéro multiple). Dans le cas d'un zéro simple, f s'annule encore sur $]\lambda_{i+1}, \lambda_{i-1}[$, ailleurs qu'en λ_i, on a donc 2 zéros de χ_B, et si λ_i est zéro double au moins de χ_B, on aura $\lambda_{i+1} \leqslant \mu_i = \lambda_i = \mu_{i-1} \leqslant \lambda_{i-1}$: les inégalités sont préservées.

Si λ_i est zéro multiple, d'ordre α, comme la décomposition en éléments simples de f fait intervenir $\dfrac{(p_i)^2}{\lambda_i - \lambda}$, c'est que :

si $p_i \neq 0$, λ_i est zéro d'ordre $\alpha - 1$ de $\chi_B(\lambda)$,

si $p_i = 0$, λ_i est zéro d'ordre α au moins de $\chi_B(\lambda)$.

Finalement, on a dans tous les cas l'entrelacement voulu.

5.13. La matrice A est diagonalisable dans le groupe orthogonal. On suppose ses valeurs propres indexées en croissant : $\mu_1 \leqslant \mu_2 \leqslant \ldots \leqslant \mu_n$. Il existe donc P dans $O_n(\mathbb{R})$ telle que $P^{-1}AP = {}^tPAP = \Delta = \text{diag}(\mu_1, \ldots, \mu_n)$.

Soit Q la matrice blocs $Q = \left(\begin{array}{c|c} P & 0 \\ \hline 0 & 1 \end{array}\right)$: elle est orthogonale d'ordre $n+1$, et on a :

$$ {}^tQ = \left(\begin{array}{c|c} {}^tP & 0 \\ \hline 0 & 1 \end{array}\right) = \left(\begin{array}{c|c} P^{-1} & 0 \\ \hline 0 & 1 \end{array}\right) = Q^{-1}. $$

Posons $A_1 = \left(\begin{array}{c|c} A & b \\ \hline {}^tb & c \end{array}\right)$, avec b matrice colonne d'ordre n, inconnue,

$$ \text{et } B = Q^{-1}A_1Q = \left(\begin{array}{c|c} P^{-1} & 0 \\ \hline 0 & 1 \end{array}\right)\left(\begin{array}{c|c} A & b \\ \hline {}^tb & c \end{array}\right)\left(\begin{array}{c|c} P & 0 \\ \hline 0 & 1 \end{array}\right) $$

$$ = \left(\begin{array}{c|c} P^{-1} & 0 \\ \hline 0 & 1 \end{array}\right)\left(\begin{array}{c|c} AP & b \\ \hline {}^tbP & c \end{array}\right) = \left(\begin{array}{c|c} P^{-1}AP & P^{-1}b \\ \hline {}^tbP & c \end{array}\right) $$

$$ = \left(\begin{array}{c|c} \Delta & d \\ \hline {}^td & c \end{array}\right), $$

avec $d = P^{-1}b = {}^tPb$, vecteur colonne de $\mathbb{R}^n$, et A_1 et B ayant même spectre.

On est donc ramené à traiter l'exercice avec Δ matrice diagonale, et B matrice dont on peut calculer facilement le polynôme caractéristique, $\chi_B(\lambda)$.

On a, en développant par rapport à la dernière ligne :

$$\chi_B(\lambda) = \begin{vmatrix} \mu_1 - \lambda & & & d_1 \\ & \ddots & & \vdots \\ & & \mu_n - \lambda & d_n \\ d_1 & \cdots & d_n & c - \lambda \end{vmatrix}$$

$$= (c-\lambda)\prod_{i=1}^{n}(\mu_i - \lambda) +$$

$$\sum_{i=1}^{n}(-1)^{n+1+i}d_i \underbrace{\begin{vmatrix} \mu_1 - \lambda & & 0 & 0 & & d_1 \\ & \ddots & & & & \\ 0 & & \mu_{i-1} - \lambda & & & d_{i-1} \\ \hline & & & 0 & \cdots & d_i \\ & 0 & & \mu_{i+1} - \lambda & & 0 \\ & & & & \ddots & \\ & & & & & \mu_n - \lambda \end{vmatrix}}_{\text{on développe par rapport à la } i^{\text{ième}} \text{ ligne,}}$$

$$\text{en } (-1)^{n+i}d_i\prod_{j\neq i}(\mu_j - \lambda).$$

Avec $\chi_A(\lambda) = \prod_{i=1}^{n}(\mu_i - \lambda)$, on a donc :

$$\chi_B(\lambda) = (c-\lambda)\chi_A(\lambda) + \sum_{i=1}^{n}(-1)^{n+1+i+n+i}(d_i)^2\frac{\chi_A(\lambda)}{\mu_i - \lambda}$$

$$= \chi_A(\lambda)\left(c - \lambda - \sum_{i=1}^{n}\frac{d_i^2}{\mu_i - \lambda}\right),$$

donc, pour tout λ distinct des μ_i, on a :

$$\frac{\chi_B(\lambda)}{\chi_A(\lambda)} = c - \lambda - \sum_{i=1}^{n} \frac{d_i^2}{\mu_i - \lambda}.$$

La fonction f de l'énoncé étant $f(x) = \dfrac{(-1)^{n+1}\chi_B(x)}{(-1)^n \chi_A(x)}$ c'est encore :

$$\text{①} \qquad f(x) = x - c - \sum_{i=1}^{n} \frac{d_i^2}{x - \mu_i}.$$

Si b existe, donc si d existe, la fraction rationnelle f admet la décomposition en éléments simples donnée par ① : elle n'a que des pôles simples, et sa dérivée étant positive, elle est croissante.

Réciproquement, si les λ_j sont tels que f soit croissante en n'ayant que des pôles simples, ceux-ci sont certains des μ_j, et $f(x)$ admet une décomposition du type :

$$\text{②} \qquad f(x) = \frac{\prod_{i=1}^{n+1}(x - \lambda_i)}{\prod_{i=1}^{n}(x - \mu_i)} = x + \alpha - \sum_{i=1}^{n} \frac{\beta_i}{x - \mu_i},$$

certains β_i pouvant être nuls, le coefficient de x étant 1 car :

$$f(x) = \frac{x^{n+1} - \left(\sum_{i=1}^{n+1} \lambda_i\right) x^n + \ldots}{x^n - \left(\sum_{i=1}^{n} \mu_i\right) x^{n-1} + \ldots}, \quad \text{ce qui montre aussi que}$$

$$\alpha = \sum_{i=1}^{n} \mu_i - \sum_{i=1}^{n+1} \lambda_i = -c.$$

De plus, pour $\beta_i \neq 0$, sur un voisinage de μ_i la fonction $f(x) + \dfrac{\beta_i}{x - \mu_i}$ est bornée ; donc si β_i était négatif, la fonction $x \rightsquigarrow \dfrac{-\beta_i}{x - \mu_i}$ tendrait vers $-\infty$ si $x \to \mu_i^-$, et vers $+\infty$ si $x \to \mu_i^+$, d'où pour f une asymptote verticale pour $x = \mu_i$.

Mais alors, les limites trouvées lorsque x tend vers μ_i^- et x tend vers μ_i^+, ne sont pas compatibles avec la croissance de f sur $\mathbb{R}$ privé des μ_i.

Donc les β_i qui sont non nuls sont > 0.

On peut alors justifier l'existence de $d = (d_1, ..., d_n)$, tel que ① soit la décomposition en éléments simples de $f(x)$. En effet, avec l'indexation donnée des μ_i, les d_i doivent être tels que :

si μ, valeur propre d'ordre r de A, associée aux indices $i+1, i+2, ..., i+r$, est effectivement pôle de f, de coefficient $-\beta$, $\beta > 0$, on doit avoir

$$(d_{i+1})^2 + (d_{i+2})^2 + ... + (d_{i+r})^2 = \beta,$$

et cette équation a des solutions,

alors que si μ n'est pas pôle de f, on doit avoir $(d_{i+1})^2 + ... + (d_{i+r})^2 = 0$, mais là encore il y a une solution, nulle.

5.14. On munit $E = \mathscr{C}^0([a, b], \mathbb{R})$ du produit scalaire :

$$\langle u, v\rangle = \int_a^b u(t)v(t)\mathrm{d}t.$$

Pour ce produit scalaire, f est orthogonale au sous-espace F des polynômes de degré $p-1$ au plus, (fonctions polynômes restreintes à $[a, b]$). De plus, $\int_a^b f(t)\mathrm{d}t = 0$, donc f, continue, n'est pas de signe constant sur $]a, b[$: elle change de signe (ou elle est nulle, cas que nous écarterons).

Si f ne changeait que r fois de signe sur $]a, b[$, en $\alpha_1, ..., \alpha_r$, avec $a < \alpha_1 < ... < \alpha_r < b$, la fonction $t \rightsquigarrow f(t) \prod_{i=1}^{r} (t - \alpha_i) = g(t)$ serait continue, non identiquement nulle, (sinon, comment parler de changement de signe), de signe constant là où elle est non nulle, donc $\int_a^b f(t) \prod_{i=1}^{r} (t - \alpha_i)\mathrm{d}t$ serait non nul.

En posant $P(t) = \prod_{i=1}^{r} (t - \alpha_i)$, si la fonction P est dans F on devrait avoir $\langle f, P\rangle = 0$: c'est gênant. C'est que P n'est pas dans F, d'où $r \geqslant p$, et f s'annule au moins p fois.

5.15. D'abord, justifions la convergence de la série des $x_k y_k$, pour x et y dans E : on a $2|x_k||y_k| \leqslant (x_k)^2 + (y_k)^2$, donc $\langle x, y\rangle$ existe, et on vérifie que $E = l^2(\mathbb{R})$ est un espace préhilbertien pour ce produit scalaire, espace complet en fait.

Dans cet espace, la famille des $(e^{(n)})_{n \in \mathbb{N}}$, ($e^{(n)}$ étant la suite de terme général nul, sauf celui d'indice n qui vaut 1), est totale, car en notant :

$F = \text{Vect}\{e^{(n)}, n \in \mathbb{N}\}$, si $x = (x_n)_{n \in \mathbb{N}}$ est dans E, les $x^{(n)}$ définis par $x^{(n)} = \sum_{i=0}^{n} x_i e^{(i)}$ sont dans F et $\|x - x^{(n)}\|^2 = \sum_{i=n+1}^{\infty} (x_i)^2$, tend vers 0 si n tend vers l'infini. On comprend bien que pour vérifier la condition finale pour tout z de E, on pourra la vérifier pour les $e^{(n)}$, l'étendre à F par linéarité et conclure sur E par densité.

Or, si $a = (a_i)_{i \in \mathbb{N}}$, $\langle a, e^{(n)}\rangle = a_n$, et l'élément a de E cherché, et la suite extraite des $y^{(k)}$, doivent être tels que, pour tout n de $\mathbb{N}$,

$$\langle a, e^{(n)}\rangle = a_n = \lim_{k \to +\infty} \langle y^{(k)}, e^{(n)}\rangle$$

$$= \lim_{k \to +\infty} y_n^{(k)}$$

on est ramené à une « convergence simple » par rapport aux indices des termes généraux des suites et là, le procédé de la suite diagonale va servir.

D'abord, il existe une constante $M > 0$ telle que :

$\forall k \in \mathbb{N}$, $\sum_{n=0}^{+\infty} (x_n^{(k)})^2 \leqslant M$, (c'est $\|x^{(k)}\|^2 \leqslant M$) ; donc, *a fortiori*, $\forall k \in \mathbb{N}$, $\forall n \in \mathbb{N}$, $|x_n^{(k)}| \leqslant \sqrt{M}$.

La suite des $(x_0^{(k)})_{k \in \mathbb{N}}$ est bornée, à valeurs dans $K = [-\sqrt{M}, \sqrt{M}]$ compact, donc admet une suite extraite convergente, notée $(x_0^{\varphi_0(k)})_{k \in \mathbb{N}}$ et on pose $a_0 = \lim_{k \to +\infty} x_0^{\varphi_0(k)}$.

Puis, la suite des $(x_1^{\varphi_0(k)})_{k \in \mathbb{N}}$ est à son tour à valeurs dans $[-\sqrt{M}, \sqrt{M}]$ compact, donc admet une suite extraite convergente, notée $(x_1^{\varphi_0 \circ \varphi_1(k)})_{k \in \mathbb{N}}$, et on pose $a_1 = \lim_{k \to +\infty} x_1^{\varphi_0 \circ \varphi_1(k)}$.

On peut itérer ce raisonnement, et, en partant de la suite des $(x_p^{\varphi_0 \circ \varphi_1 \circ \ldots \circ \varphi_{p-1}(k)})_{k \in \mathbb{N}}$, à valeurs dans le même compact $[-\sqrt{M}, \sqrt{M}]$, en extraire la suite des $(x_p^{\varphi_0 \circ \ldots \circ \varphi_p(k)})_{k \in \mathbb{N}}$, qui converge vers a_p.

Considérons alors la suite $a = (a_p)_{p \in \mathbb{N}}$ ainsi construite, et la suite des $(y^{(p)})_{p \in \mathbb{N}}$, extraite de la suite initiale, par le procédé de la suite diagonale, en posant $y^{(p)} = x^{\varphi_0 \circ \varphi_1 \circ \ldots \circ \varphi_p(p)}$.

Pour tout $k \geqslant p$, on a $y^{(k)} = x^{\varphi_0 \circ \varphi_1 \circ \ldots \circ \varphi_p(\varphi_{p+1} \circ \ldots \circ \varphi_k(k))}$, et, en posant $k' = \varphi_{p+1} \circ \ldots \circ \varphi_k(k)$, comme les φ_j sont strictement croissantes, (suites extraites), on a $\lim_{k \to +\infty} k' = +\infty$, et le $p^{\text{ième}}$ terme de $y^{(k)}$ est tel que

$$\lim_{k \to +\infty} y_p^{(k)} = \lim_{k \to +\infty} x_p^{\varphi_0 \circ \ldots \circ \varphi_p(\varphi_{p+1} \circ \ldots \circ \varphi_k(k))},$$

$$= \lim_{k' \to +\infty} x_p^{\varphi_0 \circ \ldots \circ \varphi_p(k')} = a_p,$$

soit, avec les notations du produit scalaire :

$$\lim_{k \to +\infty} \langle y^{(k)}, e^{(p)} \rangle = \langle a, e^{(p)} \rangle .$$

Si on *justifie l'appartenance* de a à E, on aura aussi la condition finale vérifiée pour les $(e^{(p)})_{p \in \mathbb{N}}$.

Si on repart de l'inégalité :

$$\forall k \in \mathbb{N}, \sum_{n=0}^{+\infty} (x_n^{(k)})^2 \leqslant M, \text{ on a, } a \textit{ fortiori} :$$

$$\forall k \in \mathbb{N}, \forall N \in \mathbb{N}, \sum_{n=0}^{N} (x_n^{(k)})^2 \leqslant M,$$

donc, avec $k = \varphi_0 \circ \varphi_1 \circ \ldots \circ \varphi_N(l)$, l étant quelconque dans $\mathbb{N}$, on a :

$$\forall l \in \mathbb{N}, \forall N \in \mathbb{N}, \sum_{n=0}^{N} (x_n^{\varphi_0 \circ \varphi_1 \circ \ldots \circ \varphi_N(l)})^2 \leqslant M,$$

et, dans cette somme finie, on peut faire tendre l vers $+\infty$, mais alors :

$x_0^{\varphi_0(\varphi_1 \circ \ldots \circ \varphi_N(l))}$ tend vers a_0 ;

$x_1^{\varphi_0 \circ \varphi_1(\varphi_2 \circ \ldots \circ \varphi_N(l))}$ tend vers a_1 ;

et plus généralement, pour chaque $n \leqslant N$,

$x_n^{\varphi_0 \circ \dots \circ \varphi_n(\varphi_{n+1} \circ \dots \circ \varphi_N(l))}$ tend vers a_n.

A la limite on obtient : $\sum_{n=0}^{N} (a_n)^2 \leqslant M$, et ceci pour tout N de $\mathbb{N}$, donc la suite a est bien dans $E = l^2(\mathbb{R})$.

Il reste à conclure. Avec la suite a ainsi définie, et les $y^{(k)}$ de E, tels que $y^{(k)} = x^{\varphi_0 \circ \dots \circ \varphi_k(k)}$, nous avons justifié que, pour chaque élément $e^{(p)}$ de E, on a :

$$\lim_{k \to +\infty} \langle y^{(k)}, e^{(p)} \rangle = \langle a, e^{(p)} \rangle .$$

Par bilinéarité du produit scalaire, on a également :

$$\lim_{k \to +\infty} \langle y^{(k)}, z \rangle = \langle a, z \rangle ,$$

pour tout z de $F = \text{Vect}\{e^{(p)}, p \in \mathbb{N}\}$.

Enfin, on a vu que l'adhérence de F est E, donc, avec $z \in E$, on a : $\forall \varepsilon > 0$, $\exists z' \in F$ tel que $\|z - z'\| \leqslant \varepsilon$; on a alors :

$$\forall k \in \mathbb{N}, \langle y^{(k)} - a, z \rangle = \langle y^{(k)} - a, z - z' \rangle + \langle y^{(k)} - a, z' \rangle , \text{ d'où :}$$

$$\begin{aligned} |\langle y^{(k)}, z \rangle - \langle a, z \rangle| &= |\langle y^{(k)} - a, z \rangle| \\ &\leqslant \|y^{(k)} - a\| \|z - z'\| + |\langle y^k - a, z' \rangle| \\ &\leqslant (\|y^{(k)}\| + \|a\|)\varepsilon + |\langle z^k, z' \rangle - \langle a, z' \rangle| . \end{aligned}$$

Or, au même $\varepsilon > 0$, on associe k_0 tel que, $\forall k \geqslant k_0$, on ait $|\langle y^k, z' \rangle - \langle a, z' \rangle| \leqslant \varepsilon$, (propriété finale vérifiée pour les z' de F), et comme $\|y^{(k)}\| \leqslant M$, finalement on a :

$\forall z \in E, \forall \varepsilon > 0, \exists k_0 \in \mathbb{N}, \forall k \geqslant k_0, |\langle y^{(k)}, z \rangle - \langle a, z \rangle| \leqslant (1 + M + \|a\|)\varepsilon$: ceci traduit bien l'égalité :

$$\lim_{k \to +\infty} \langle y^{(k)}, z \rangle = \langle a, z \rangle ,$$

valable maintenant pour tout z de E.

5.16. On peut s'attendre à trouver une condition du type : $f(t)$, (vecteur) doit avoir une direction fixe. On note $\langle\ ,\ \rangle$ et $\|\ \|$ le produit scalaire de $\mathbb{R}^n$, et la norme associée.

Pour t dans $[a, b]$, on pose $f(t) = (f_1(t), ..., f_n(t))$, et on suppose que l'on a $\left\|\int_a^b f(t)\mathrm{d}t\right\| = \int_a^b \|f(t)\|\,\mathrm{d}t$.

Si on introduit un vecteur unitaire $u = (u_1, ..., u_n)$, tel que $\int_a^b f(t)\mathrm{d}t = \left\|\int_a^b f(t)\mathrm{d}t\right\| u = \left(\int_a^b \|f(t)\|\,\mathrm{d}t\right)u$, ce vecteur u est unique si $\int_a^b f(t)\mathrm{d}t \neq 0$, quelconque unitaire sinon, mais dans ce cas, $\int_a^b \|f(t)\|\,\mathrm{d}t = 0$, avec $t \rightsquigarrow \|f(t)\|$ continue, donc la fonction f est identiquement nulle. On la suppose non nulle par la suite. On a :

$$\left\langle \int_a^b f(t)\mathrm{d}t, u\right\rangle = \left\|\int_a^b f(t)\mathrm{d}t\right\| \langle u, u\rangle = \left\|\int_a^b f(t)\mathrm{d}t\right\|$$

$$= \int_a^b \|f(t)\|\,\mathrm{d}t \text{ d'une part, mais aussi :}$$

$$= \sum_{i=1}^{n} \left(\int_a^b f_i(t)\mathrm{d}t\right) \cdot u_i$$

$$= \int_a^b \left(\sum_{i=1}^{n} f_i(t)u_i\right)\mathrm{d}t, \text{ par linéarité de l'intégrale,}$$

d'où en fait l'égalité :

$$\int_a^b \|f(t)\|\,\mathrm{d}t = \int_a^b \langle f(t), u\rangle\,\mathrm{d}t, \text{ ou mieux :}$$

$$\int_a^b (\|f(t)\| - \langle f(t), u\rangle)\mathrm{d}t = 0.$$

Comme u est unitaire, par l'inégalité de Cauchy Schwarz on a $\varphi(t) = \|f(t)\| - \langle f(t), u\rangle = \|f(t)\|\|u\| - \langle f(t), u\rangle$ qui est fonction continue de t, à valeurs positives ou nulles, d'intégrale nulle, donc cette fonction est nulle et, pour tout t de $[a, b]$, $\|f(t)\|\|u\| = \langle f(t), u\rangle$, donc les vecteurs $f(t)$ et u sont liés, et comme u est unitaire, il existe, pour tout t de $[a, b]$, un scalaire $\lambda(t)$ tel que $f(t) = \lambda(t)u$.

On a alors $\|f(t)\| = |\lambda(t)| = \|f(t)\|\|u\| = \langle f(t), u\rangle$,

$$= \langle \lambda(t)u, u\rangle = \lambda(t)\|u\|^2 = \lambda(t),$$

donc $\lambda(t)$ est à valeurs positives ou nulles, d'où $\lambda(t) = \|f(t)\|$, avec u vecteur unitaire choisi au départ.

Réciproquement, si la fonction f est du type $t \rightsquigarrow \|f(t)\|u$, avec u vecteur unitaire, on aura :

$\int_a^b f(t)\mathrm{d}t = \left(\int_a^b \|f(t)\|\,\mathrm{d}t\right)u$, avec u vecteur unitaire, d'où $\left\|\int_a^b f(t)\mathrm{d}t\right\| = \int_a^b \|f(t)\|\,\mathrm{d}t$, puisque ce scalaire est positif.

5.17. L'opérateur u étant symétrique défini positif est injectif, donc pour $x \neq 0$, on a $u(x) \neq 0$ et $\varphi(x)$ existe.

Comme $\langle u(x), x\rangle$ est la valeur prise par la forme quadratique ϕ de matrice U celle de u dans une base orthonormée de E, donc U définie positive, cette valeur est strictement positive.

Par Cauchy Schwartz, $(\langle u(x), x\rangle)^2 \leqslant \|u(x)\|^2\|x\|^2$, on a $\varphi(x) \leqslant 1$, borne supérieure atteinte pour n'importe quel vecteur propre de u.

Enfin, en divisant numérateur et dénominateur par $\|x\|^4$, on obtient $\varphi(x) = \varphi\left(\frac{x}{\|x\|}\right)$: les valeurs de φ sont celles prises sur la sphère unité S de E, compact de E, (fermé borné en dimension finie). Comme φ est continue sur S, (finalement, c'est une fraction rationnelle par rapport aux coordonnées de x dans une base, fraction dont le dénominateur ne s'annule pas pour $x \neq 0$), la fonction φ est bornée sur S, (donc sur $E\backslash\{0\}$), elle atteint ses bornes, en particulier sa borne inférieure, atteinte, est strictement positive, et sa borne supérieure vaut 1 et est atteinte aussi.

5.18. a) Qui dit minimum atteint pense continuité sur un compact. Soit donc a fixé dans E, et x_0 dans Γ, $A = \Gamma \cap \mathscr{B}_f(a, \|x_0 - a\|)$ est un fermé, (Γ fermé, donc A intersection de fermés), borné puisque la boule fermée l'est, donc un compact de E, espace vectoriel normé de dimension finie.

Comme $x \rightsquigarrow \|x - a\| = d_a(x)$ est continue, (1.lipschitzienne grâce à l'inégalité triangulaire), d_a atteint sa borne inférieure sur A, compact en un point b de A, (donc de Γ), et cette borne inférieure est aussi celle de d_a sur Γ, les x exclus étant plus loin de a que x_0.

b) Vérifions d'abord que, si Γ est un cône convexe fermé, le point b où la borne inférieure est atteinte est unique. Si on avait b et b' de Γ tels que $\|b - a\| = \|b' - a\| = d(a, \Gamma)$, le milieu $c = \frac{1}{2}(b + b')$ du segment

$[b, b']$ est dans Γ, et dans un plan affine contenant a, b et b', on a, (triangle isocèle oblige) :

$$\|a-c\|^2 = \|a-b\|^2 - \frac{1}{4}\|b-b'\|^2 < (d(a,\Gamma))^2, \text{ ce qui est exclu.}$$

Le reste est une propriété des convexes en euclidien.

Supposons $d(a, \Gamma)$ atteinte en b de Γ, convexe.

Soit u dans Γ, pour tout t de $[0, 1]$, $(1-t)b + tu = b + t(u-b)$ est dans Γ, donc :

$$\|a-b\|^2 \leqslant \|a-b-t(u-b)\|^2$$

$$\leqslant \|a-b\|^2 - 2t\langle a-b, u-b\rangle + t^2\|u-b\|^2, \text{ d'où}$$

$$2t\langle a-b, u-b\rangle \leqslant t^2\|u-b\|^2.$$

On simplifie par $t > 0$ et on fait tendre t vers 0^+, d'où :

$$\langle a-b, u-b\rangle \leqslant 0,$$

et ceci pour tout u de Γ.

Comme de plus Γ est un cône, si $x \in \Gamma$, $\frac{b+x}{2}$ est dans Γ, et, par homothétie positive, $b + x = 2 \cdot \frac{b+x}{2} = u$ est dans Γ ; avec ce u particulier, $u - b = x$, d'où $\langle a-b, x\rangle \leqslant 0$ ou $\langle b-a, x\rangle \geqslant 0$, pour tout x de Γ.

Par ailleurs, l'inégalité $\langle a-b, u-b\rangle \leqslant 0$, valable pour tout u de Γ donne $\langle a-b, b\rangle \leqslant 0$, $(u = 2b)$ et aussi $\langle a-b, -b\rangle \leqslant 0$, $(u = 0)$ d'où $\langle a-b, b\rangle = 0$.

Réciproquement, si Γ est un convexe tel qu'il existe b dans Γ vérifiant $\langle b-a, b\rangle = 0$ et, $\forall x \in \Gamma$, $\langle b-a, x\rangle \geqslant 0$, Γ étant un cône, montrons que la distance du point a et de Γ est atteinte en b. Soit x dans Γ, on a :

$$\langle a-b, b-x\rangle = \langle a-b, b\rangle - \langle a-b, x\rangle \geqslant 0, \text{ d'où :}$$

$$\|a-x\|^2 = \|a-b+b-x\|^2$$

$$= \|a-b\|^2 + 2\langle a-b, b-x\rangle + \|b-x\|^2 \geqslant \|a-b\|^2,$$

et la distance de Γ au point a est bien atteinte en b.

5.19. a) Si x et y sont de même norme, $\frac{x+y}{2}$ et $\frac{x-y}{2}$ sont orthogonaux, donc $f\left(\frac{x+y}{2} + \frac{x-y}{2}\right) = f(x) = f\left(\frac{x+y}{2}\right) + f\left(\frac{x-y}{2}\right)$. Mais on a aussi, f étant paire, $f\left(\frac{x-y}{2}\right) = f\left(\frac{y-x}{2}\right)$ d'où :

$$f\left(\frac{y-x}{2}+\frac{y+x}{2}\right) = f(y) = f\left(\frac{x-y}{2}\right)+f\left(\frac{x+y}{2}\right) = f(x).$$

Les bases orthonormées jouant un rôle important dans les espaces euclidiens, soit $\mathscr{B} = (e_1, e_2, ..., e_n)$ une base orthonormée de E et $x = \sum_{i=1}^{n} x_i e_i$, décomposé dans cette base.

Les $x_i e_i$ étant deux à deux orthogonaux, on a déjà : $f(x) = \sum_{i=1}^{n} f(x_i e_i)$, et, les e_i étant tous de norme 1, les images $f(e_i)$ sont égales : notons $\vec{k}$ cette image. On sent qu'en ayant $f(x_i e_i) = x_i^2 f(e_i) = x_i^2 \vec{k}$, on récupère $\|x\|^2$ en facteur, donc on va justifier que, pour λ réel, $f(\lambda e_i) = \lambda^2 f(e_i)$.

Pour cela, on va utiliser la continuité de f, (un réel est limite de rationnels) et la dimension $\geqslant 2$.

Soit λ réel et q entier naturel, montrons que : $f(\sqrt{q}\lambda e_i) = q f(\lambda e_i)$, pour tout $i \leqslant n$, en procédant par récurrence.

Si $q = 0$, c'est $f(0) = 0$, vrai car $\forall x \in E$, $\langle x, 0\rangle = 0$ donc $f(x) = f(x+0) = f(x)+f(0)$.

L'égalité cherchée est aussi évidente si $q = 1$.

On la suppose vérifiée pour q. Soit un indice $j \neq i$, les vecteurs $\sqrt{q+1}\lambda e_i$ et $\sqrt{q}\lambda e_i + \lambda e_j$ sont tous deux de même norme, de carré $(q+1)\lambda^2$ par Pythagore, donc ont même image, avec $\sqrt{q}\lambda e_i$ et λe_j orthogonaux, d'où :

$$\begin{aligned} f(\sqrt{q+1}\lambda e_i) &= f(\sqrt{q}\lambda e_i + \lambda e_j) = f(\sqrt{q}\lambda e_i) + f(\lambda e_j) \\ &= q f(\lambda e_i) + f(\lambda e_j) \end{aligned}$$

par hypothèse de récurrence.

Puis, λe_i et λe_j, de même norme, ont même image, d'où : $f(\sqrt{q+1}\lambda e_i) = (q+1) f(\lambda e_i)$.

On a bien $f(\sqrt{q}\lambda e_i) = q f(\lambda e_i)$, pour tout q entier naturel, pour tout λ réel. Avec $\lambda = \frac{1}{\sqrt{q}}$, ceci conduit à l'égalité $f\left(\frac{e_i}{\sqrt{q}}\right) = \frac{1}{q} f(e_i)$, pour q dans $\mathbb{N}^*$.

Mais alors, si r est un rationnel positif, écrit sous la forme $r = \frac{p}{q}$, $(p, q) \in \mathbb{N} \times \mathbb{N}^*$, on a :

$$f(\sqrt{r}e_i) = f\left(\sqrt{p}\left(\frac{1}{\sqrt{q}}e_i\right)\right) = pf\left(\frac{1}{\sqrt{q}}e_i\right) = \frac{p}{q}f(e_i) = rf(e_i),$$

et pour $\sqrt{\lambda}$ réel positif, avec $(r_k)_{k \in \mathbb{N}}$, suite de rationnels convergeant vers λ, par continuité de f, on aura :

$$f(\sqrt{\lambda}e_i) = \lim_{k \to +\infty} f(\sqrt{r_k}e_i) = \lim_{k \to +\infty} r_k f(e_i) = \lambda f(e_i).$$

En posant $\sqrt{\lambda} = \mu$, on a finalement, pour tout μ réel positif, $f(\mu e_i) = \mu^2 f(e_i)$, et par parité, (en μ) des deux membres, pour tout μ réel, $f(\mu e_i) = \mu^2 f(e_i)$.

Avec $x = \sum_{i=1}^{n} x_i e_i$, et $\vec{k} = f(e_i)$, vecteur constant par rapport à i, on obtient alors :

$$f(x) = \sum_{i=1}^{n} f(x_i e_i), \text{ (orthogonalité des } x_i e_i),$$

$$= \sum_{i=1}^{n} (x_i)^2 \vec{k} = \|x\|^2 \vec{k}.$$

b) On va cette fois, prouver par récurrence sur q, que pour tout x de E et q de $\mathbb{N}$, $f(qx) = qf(x)$. C'est vrai si $q = 0$ ou 1. Si on suppose $f(qx) = qf(x)$, soit y orthogonal à x, de norme $\|y\| = \sqrt{q}\|x\|$, (y existe dans l'orthogonal de x car dim (E) $\geqslant 2$).

On a :

$$f(qx + y) = f(qx) + f(y) = qf(x) + f(y),$$

et aussi, (x et $-y$ orthogonaux) :

$$f(x - y) = f(x) + f(-y) = f(x) - f(y) \text{ car } f \text{ est impaire.}$$

Or $\langle qx + y, x - y \rangle = q\|x\|^2 - \|y\|^2$, car $\langle x, y \rangle = 0$,

$= 0$, puisque $\|y\| = \sqrt{q}\|x\|$,

donc :

$f((qx + y) + (x - y)) = f(qx + y) + f(x - y) = (q + 1)f(x)$, soit :

$f((q + 1)x) = (q + 1)f(x)$, la propriété est récurrente.

Comme f est impaire, pour tout q de $\mathbb{N}$ on a :

$f((-q)x) = -f(qx) = -qf(x)$, d'où $f(qx) = qf(x)$ pour tout q de $\mathbb{Z}$.

Avec q dans $\mathbb{Z}^*$, $f\left(q \cdot \frac{x}{q}\right) = f(x) = qf\left(\frac{x}{q}\right)$, d'où $f\left(\frac{x}{q}\right) = \frac{1}{q} f(x)$; puis, si $r = \frac{p}{q}$ est dans $\mathbb{Q}$, on a :

$$f(rx) = f\left(p \frac{x}{q}\right) = pf\left(\frac{x}{q}\right) = p\left(\frac{1}{q} f(x)\right) = rf(x),$$

et par continuité de f et densité de $\mathbb{Q}$ dans $\mathbb{R}$, on a :

$$\forall(\lambda, x) \in \mathbb{R} \times \mathrm{E}, f(\lambda x) = \lambda f(x).$$

Soient alors x et y dans E, non tous deux nuls, $x \neq 0$ par exemple, alors $z = y - \frac{\langle x, y\rangle}{\|x\|^2} x$ est tel que $\langle z, x\rangle = 0$, donc

$$\begin{aligned} f(x+y) &= f\left(\left(1 + \frac{\langle x, y\rangle}{\|x\|^2}\right) x + z\right) \\ &= f\left(\left(1 + \frac{\langle x, y\rangle}{\|x\|^2}\right) x\right) + f(z) \\ &= \left(1 + \frac{\langle x, y\rangle}{\|x\|^2}\right) f(x) + f(z) \\ &= f(x) + \frac{\langle x, y\rangle}{\|x\|^2} f(x) + f(z) \\ &= f(x) + f\left(\frac{\langle x, y\rangle}{\|x\|^2} x\right) + f(z), \end{aligned}$$

avec $\frac{\langle x, y\rangle}{\|x\|^2} x$ et z orthogonaux, donc tels que :

$$f\left(\underbrace{\frac{\langle x, y\rangle}{\|x\|^2} x + z}_{= y}\right) = f\left(\frac{\langle x, y\rangle}{\|x\|^2} x\right) + f(z).$$

On obtient finalement l'égalité $f(x+y) = f(x) + f(y)$, ce qui justifie la linéarité de f.

c) En décomposant f en $g + h$, avec $g(x) = \frac{f(x) + f(-x)}{2}$, fonction paire, et $h(x) = \frac{f(x) - f(-x)}{2}$, fonction impaire, on peut constater que

g et h vérifient la même hypothèse que f. En effet, pour h par exemple, si $\langle x, y\rangle = 0$, on a

$$\begin{aligned} 2h(x+y) &= f(x+y) - f(-x-y) \\ &= f(x) + f(y) - (f(-x) + f(-y)), \text{ car } \langle -x, -y\rangle = 0, \\ &= f(x) - f(-x) + (f(y) - f(-y)) = 2(h(x) + h(y)). \end{aligned}$$

Il en est de même de g.

Mais alors f est du type $f(x) = u(x) + \vec{k}\|x\|^2$, avec u application linéaire de E dans E.

5.20. On a $q(x\vec{i} + y\vec{j}) = p_3p_2(p_1(x\vec{i} + y\vec{j})) = p_3p_2(x\vec{i})$

$$= p_3\left(\frac{x}{\sqrt{2}}\vec{i} + \frac{x}{\sqrt{2}}\vec{j}\right) = \frac{x}{\sqrt{2}}\vec{j}.$$

Donc $\operatorname{Im} q = \mathbb{R}\vec{j}$, $\operatorname{Ker} q = \{y\vec{j}\ ;\ y \in \mathbb{R}\} = \mathbb{R}\vec{j}$.

Comme l'adjoint q^* est $p_1^*\ p_2^*\ p_3^* = p_1p_2p_3$, les projections orthogonales étant des applications auto-adjointes, car de matrice symétrique dans une base orthonormée réunion d'une base orthonormée de l'image et du noyau), on a, en échangeant les places de p_1 et p_3,

$\operatorname{Im} q^* = \mathbb{R}\vec{i} = \operatorname{Ker} q^* = (\operatorname{Ker} q)^\perp = (\operatorname{Im} q)^\perp$.

Généralisation

a) Si $x \in \mathrm{N}_0 = \bigcap_{i=1}^{k} \mathrm{N}_i = \bigcap_{i=1}^{k} \operatorname{Ker}(p_i - \mathrm{id})$, on a $p_i(x) = x$ pour tout i, donc $q(x) = p_k \circ p_{k-1} \circ \ldots \circ p_1(x) = x$ et $\|q(x)\| = \|x\|$.

Soit p un projecteur orthogonal, on décompose x en : $x = u + v$, $u \in \operatorname{Ker} p$, $v \in \operatorname{Im} p = (\operatorname{Ker} p)^\perp$.

Alors $\|p(x)\|^2 = \|v\|^2 \leqslant \|x\|^2 = \|u\|^2 + \|v\|^2$, et il y a égalité si et seulement si $x = v \in \operatorname{Im} p$.

Si on suppose que $x \notin \mathrm{N}_0$, on peut introduire le plus petit indice i_0 tel que $x \notin \mathrm{N}_{i_0}$. Pour $i < i_0$, s'il y en a, $p_i(x) = x$ et on a :

$q(x) = p_k \circ \ldots \circ p_{i_0+1}(p_{i_0}(x))$,

avec $\|p_{i_0}(x)\| < \|x\|$, puis, en posant $x' = p_{i_0}(x)$, $\|p_{i_0+1}(x')\| \leqslant \|x'\|$ et, finalement, $\|q(x)\| \leqslant \|x'\| < \|x\|$. On a bien $(x \in N_0) \Leftrightarrow \|q(x)\| = \|x\|$.

b) On a vu que $x \in N_0 \Rightarrow q(x) = x$, d'où $N_0 \subset \text{Ker}\,(q - \text{id}_E)$.

Si $x \in \text{Ker}\,(q - \text{id}_E)$, $q(x) = x$, donc $\|q(x)\| = \|x\|$, et l'équivalence du a) donne alors $x \in N_0$.

Donc $N_0 = \text{Ker}\,(q - \text{id}_E)$.

Comme $q^* = p_1^* \circ \ldots \circ p_k^* = p_1 \circ \ldots \circ p_k$, les N_i étant les images des projections orthogonales p_i, on a $\text{Ker}\,(q^* - \text{id}_E) = \bigcap_{i=k}^{1} N_i$, et l'indexation décroissante ne change pas l'intersection, d'où $\text{Ker}\,(q^* - \text{id}_E) = N_0$ aussi.

c) On sait que $\text{Ker}\,(q^* - \text{id}_E) = (\text{Im}\,(q - \text{id}_E))^\perp = N_0$, puis que :

$$\begin{aligned} E &= \text{Im}\,(q - \text{id}_E) \oplus (\text{Im}\,(q - \text{id}_E))^\perp \\ &= \text{Im}\,(q - \text{id}_E) \oplus N_0 = \text{Im}\,(q - \text{id}_E) \oplus \text{Ker}\,(q - \text{id}_E). \end{aligned}$$

d) Soit une suite $(x_n)_{n \in \mathbb{N}}$ d'éléments de E, avec $\|x_n\| \leqslant 1$ et $\lim_{n \to +\infty} \|q(x_n)\| = 1$.

On a vu au a), que pour tout x, $\|q(x_n)\| \leqslant \|x_n\|$. On a ici $\|q(x_n)\| \leqslant \|x_n\| \leqslant 1$, d'où également $\lim_{n \to +\infty} \|x_n\| = 1$.

Supposons que l'on n'ait pas $\lim_{n \to +\infty} \|(q - \text{id})(x_n)\| = 0$. Alors $\exists \alpha > 0$, $\forall n_0, \exists n \geqslant n_0, \|q(x_n) - x_n\| \geqslant \alpha$. On peut extraire une suite $x'_n = x_{\varphi(n)}$ telle que, pour tout n, $\|q(x'_n) - x'_n\| \geqslant \alpha$.

Cette suite $(x'_n)_{n \in \mathbb{N}}$, dans le compact $\mathscr{B}_f(0, 1)$, admet une suite extraite des $x''_n = x'_{\psi(n)} = x_{\varphi \circ \psi(n)}$, qui converge vers y, de norme 1 car $\lim_{n \to +\infty} \|x''_n\| = \lim_{n \to +\infty} \|x_{\varphi \circ \psi(n)}\| = 1$.

Comme q, linéaire en dimension finie est continue, on a aussi $\|q(y)\| = \lim_{n \to +\infty} \|q(x_{\varphi \circ \psi(n)})\| = 1$, donc $\|q(y)\| = \|y\|$ et y est dans N_0, (d'après le a), avec $N_0 = \text{Ker}\,(q - \text{id})$, (voir b), donc $q(y) = y$.

Mais, pour tout n on a :

$\|q(x''_n) - x''_n\| = \|q(x'_{\psi(n)}) - x'_{\psi(n)}\| \geqslant \alpha$, à la limite $\|q(y) - y\| \geqslant \alpha > 0$, ce qui contredit $q(y) = y$.

On a justifié, par l'absurde, que $\lim_{n \to +\infty} \|(q - \mathrm{id})(x_n)\| = 0$.

5.21. Il y a d'abord un problème d'existence de B : il faut justifier que $I - A$ est inversible, donc que A, antisymétrique n'admet pas 1 pour valeur propre.

On peut par exemple dire que $H = iA$ est hermitienne, donc de valeurs propres réelles, d'où les valeurs propres de A du type ia avec a réel, ce qui exclut 1.

On peut aussi, directement, remarquer que si λ est valeur propre de A, avec X vecteur colonne tel que $AX = \lambda X$, en transposant on a ${}^tX(-A) = \lambda {}^tX = -{}^tXA$, d'où : ${}^tXAX = {}^tX(AX) = {}^tX(\lambda X) = \lambda({}^tXX)$, mais c'est aussi : $({}^tXA)X = -\lambda {}^tXX$, d'où $2\lambda {}^tXX = 0$, et comme ${}^tXX = \|X\|^2$, (norme euclidienne canonique de $\mathbb{R}^n$), c'est non nul pour $X \neq 0$, d'où $\lambda = 0$ seule valeur propre réelle.

Si on forme alors ${}^tBB$, on a :

$$\begin{aligned} {}^tBB &= {}^t(I-A)^{-1}\,{}^t(I+A)(I+A)(I-A)^{-1} \\ &= (I+A)^{-1}(I-A)(I+A)(I-A)^{-1}, \end{aligned}$$

et comme $I - A$ et $I + A$, polynômes en A, commutent, il reste ${}^tBB = (I+A)^{-1}(I+A)(I-A)(I-A)^{-1} = I$, d'où B orthogonale.

Réciproquement, si B est orthogonale, et si on peut trouver A antisymétrique telle que $B = (I+A)(I-A)^{-1}$, c'est équivalent à avoir : $B(I-A) = I+A$ ou encore : $B - I = (I+B)A$.

Supposons $I + B$ *régulière*, et soit $A = -(I+B)^{-1}(I-B)$. La matrice A est antisymétrique, car :

${}^tA = -(I - {}^tB)(I + {}^tB)^{-1}$, avec B orthogonale, donc telle que ${}^tB = B^{-1}$, d'où :

$(I+B)(I-{}^tB) = I + B - {}^tB - B{}^tB = B - {}^tB$, et aussi :

$-(I-B)(I+{}^tB) = -I + B - {}^tB + B{}^tB = B - {}^tB$.

Mais l'égalité :

$$(I+B)(I-{}^tB) = -(I-B)(I+{}^tB) \text{ conduit à :}$$

$$(I-{}^tB)(I+{}^tB)^{-1} = -(I+B)^{-1}(I-B), \text{ soit encore à :}$$

$$-{}^tA = A.$$

Si $I+B$ n'*est pas régulière on ne peut pas conclure*, par exemple avec $B = -I$, orthogonale, si A antisymétrique vérifie l'égalité $B = (I+A)(I-A)^{-1}$, on est conduit à $-(I-A) = I+A$ soit à $2I = 0$, ce qui est curieux.

Donc, si B est orthogonale, telle que $I+B$ est régulière, on peut trouver A antisymétrique, $(A = -(I+B)^{-1}(I-B))$, telle que $B = (I+A)(I-A)^{-1}$.

5.22. L'inégalité $q_A \leqslant q_B$ signifie que, pour tout x de $\mathbb{R}^n$, on a $q_A(x) \leqslant q_B(x)$, ou encore, si X est la matrice colonne des coordonnées de x dans la base $\mathscr{B}$ fixée dans $\mathbb{R}^n$ pour associer q_A et q_B aux matrices A et B, que ${}^tXAX \leqslant {}^tXBX$.

Les matrices symétriques étant positives, leurs déterminants, (produit des valeurs propres) le sont d'où, si $\det A = 0$, l'inégalité $0 = \det A \leqslant \det B$ vérifiée.

Si $\det A > 0$, A, définie positive, définit un produit scalaire, et on peut réduire simultanément A et B : il existe P régulière telle que ${}^tPAP = I_n$ et ${}^tPBP = \operatorname{diag}(\lambda_1, ..., \lambda_n)$ avec, si $\mathscr{C} = \{\varepsilon_1, ..., \varepsilon_n\}$ est la nouvelle base, $\lambda_i = q_B(\varepsilon_i) \geqslant q_A(\varepsilon_i) = 1$.

Donc, on a $(\det P)^2 \det B = \prod_{i=1}^{n} \lambda_i \geqslant 1 = (\det P)^2 \det A$, d'où, comme $(\det P)^2 > 0$, l'inégalité voulue : $\det B \geqslant \det A$.

5.23. a) La réflexivité $(A \leqslant A)$ et la transitivité, $(A \leqslant B$ et $B \leqslant C \Rightarrow A \leqslant C)$ sont faciles à vérifier. Justifions l'antisymétrie.

Si, pour A et B de E, on a $A \leqslant B$ et $B \leqslant A$, pour tout vecteur colonne X de $\mathscr{M}_{n,1}(\mathbb{R})$ on a ${}^tXAX \leqslant {}^tXBX$ et ${}^tXBX \leqslant {}^tXAX$, d'où ${}^tX(A-B)X = 0$ en fait, et la forme quadratique de matrice symétrique $A-B$ étant nulle, c'est que $A-B = 0$, d'où $A = B$.

b) Soit $B \in E$, une matrice symétrique qui majore les A_k. Pour une matrice colonne fixée dans $\mathcal{M}_{n,1}(\mathbb{R})$, en posant :

$\phi_k(X) = {}^tXA_kX$, la suite des réels $(\phi_k(X))_{k \in \mathbb{N}}$ est croissante, majorée par ${}^tXBX$, donc convergente. On note $\phi(X)$ sa limite.

En fait ϕ est une forme quadratique car, $\forall \lambda \in \mathbb{R}, \forall X \in \mathcal{M}_{n,1}(\mathbb{R})$, $\phi(\lambda X) = \lim\limits_{k \to +\infty} \phi_k(\lambda X) = \lim\limits_{k \to +\infty} \lambda^2 \phi_k(X) = \lambda^2 \lim\limits_{k \to +\infty} \phi_k(X) = \lambda^2 \phi(X)$, et φ définie par :

$$\varphi(X, Y) = \frac{1}{4}(\phi(X+Y) - \phi(X-Y)),$$

est bilinéaire, car c'est encore :

$$\varphi(X, Y) = \lim_{k \to +\infty} \frac{1}{4}(\phi_k(X+Y) - \phi_k(X-Y)) = \lim_{k \to +\infty} \varphi_k(X, Y), \text{ si}$$

φ_k est la forme bilinéaire symétrique associée à ϕ_k. Le côté bilinéaire de φ_k étant préservé par le passage à la limite, le résultat en découle.

Mais alors ϕ est une forme quadratique, et si A est sa matrice, en notant $(e_1, ..., e_n)$ la base canonique de $\mathbb{R}^n$, on aura $\alpha_{ij} = \varphi(e_i, e_j) = \lim\limits_{k \to +\infty} \varphi_k(e_i, e_j) = \lim\limits_{k \to +\infty} \alpha_{ij}^{(k)}$, en notant $\alpha_{ij}^{(k)}$ le terme de la $i^{\text{ième}}$ ligne, $j^{\text{ième}}$ colonne de A_k. Donc, dans la topologie induite sur E par celle de $\mathbb{R}^{n^2}$, (espace vectoriel normé), on a $\lim\limits_{k \to +\infty} A_k = A$, avec A matrice symétrique.

c) Pour $x \in [0, 1]$, on vérifie par récurrence que $P_n^2(x) \leqslant x$ et que la suite est croissante.

Comme $P_0 = 0, x - P_0^2(x) = x \geqslant 0$ donc $P_1(x) \geqslant P_0(x)$, et

$$\sqrt{x} - P_1(x) = \sqrt{x} - P_0(x) - \frac{1}{2}(\sqrt{x} - P_0(x))(\sqrt{x} + P_0(x))$$

$$= (\sqrt{x} - P_0(x))\left(1 - \frac{\sqrt{x} + P_0(x)}{2}\right).$$

On a $0 \leqslant P_0(x) \leqslant \sqrt{x} \leqslant 1 \Rightarrow \frac{\sqrt{x} + P_0(x)}{2} \leqslant 1$, et $\sqrt{x} - P_1(x)$ est produit de deux nombres positifs, sur [0, 1].

Si on suppose $0 \leqslant P_n(x) \leqslant \sqrt{x} \leqslant 1$, on a $P_n^2(x) \leqslant x$, d'où :

$$P_{n+1}(x) = P_n(x) + \frac{1}{2}(x - P_n^2(x)) \geqslant P_n(x), \text{ puis :}$$

$$\sqrt{x} - P_{n+1}(x) = \sqrt{x} - P_n(x) - \frac{1}{2}(\sqrt{x} - P_n(x))(\sqrt{x} + P_n(x))$$

$$= (\sqrt{x} - P_n(x))\left(1 - \frac{\sqrt{x} + P_n(x)}{2}\right),$$

c'est encore un produit de deux nombres positifs puisque :

$$\frac{\sqrt{x} + P_n(x)}{2} \leqslant \frac{2\sqrt{x}}{2} = \sqrt{x} \leqslant 1.$$

La suite $P_n(x)$, croissante majorée converge, sur [0, 1], et la limite vérifie $l(x) = l(x) + \frac{1}{2}(x - l^2(x))$, donc $l(x) = \sqrt{x}$. On retrouve une étape classique d'une justification du Théorème de Stone Weierstrass.

d) Comme A, dans E, est diagonalisable dans le groupe orthogonal, il existe Q orthogonale d'ordre n sur $\mathbb{R}$ telle que $A = QDQ^{-1}$ avec $D = \text{diag}(\lambda_1, ..., \lambda_n)$, les λ_i étant dans [0, 1].

Comme $A^r = QD^rQ^{-1}$, il est facile de voir que $P_k(A) = QP_k(D)Q^{-1}$ avec $P_k(D) = \text{diag}(P_k(\lambda_1), ..., P_k(\lambda_n))$, qui a pour limite, si k tend vers l'infini, la matrice diag $(\sqrt{\lambda_1}, ..., \sqrt{\lambda_n})$, vu le c).

$$\text{Donc } \lim_{k \to +\infty} P_k(A) = Q \text{ diag } (\sqrt{\lambda_1}, ..., \sqrt{\lambda_n})Q^{-1}$$

$$= Q \text{ diag } (\sqrt{\lambda_1}, ..., \sqrt{\lambda_n})^tQ = B,$$

est symétrique, positive, et $B^2 = QDQ^{-1} = A$: la suite des $P_k(A)$ a pour limite « $\sqrt{A}$ » si l'on peut dire.

5.24. a) La matrice A, symétrique réelle, est diagonalisable. Si $\lambda_1, ..., \lambda_n$ sont les valeurs propres distinctes ou non de A, celles de $I_n - A$ sont les $1 - \lambda_i$, et on a $1 - \lambda_i > 0$ pour tout i. De plus $I_n - A$ est inversible, et on a l'identité :

$$(I_n + A + A^2 + ... + A^{2p-1})(I_n - A) = (I_n - A^{2p}), \text{ d'où :}$$

$$I_n + A + A^2 + ... + A^{2p-1} = (I_n - A)^{-1} - A^{2p}(I_n - A)^{-1}.$$

Le nombre réel $u_p = \sum_{k=0}^{2p-1} (\text{trace } A^k)$ est donc, (linéarité de la trace), trace $(I_n - A)^{-1}$ – trace $A^{2p}(I_n - A)^{-1}$.

Mais, (invariance de la trace pour des matrices semblables), dans une base de diagonalisation de A, A est semblable à $A' = \text{diag}(\lambda_1, ..., \lambda_n)$, donc $I_n - A$ est semblable à $I_n - A' = \text{diag}(1-\lambda_1, ..., 1-\lambda_n)$, et $(I_n - A)^{-1}$ à $\text{diag}\left(..., \frac{1}{1-\lambda_i}, ...\right)$ et A^{2p} à $A'^{2p} = \text{diag}(\lambda_1^{2p}, ..., \lambda_n^{2p})$, d'où en fait :

$$u_p = \text{trace } (I_n - A)^{-1} - \sum_{i=1}^{n} \frac{\lambda_i^{2p}}{1-\lambda_i} \leqslant \text{trace } (I_n - A)^{-1}.$$

La suite des u_p est donc majorée.

b) On suppose cette fois A à coefficients positifs. Donc les traces des A^k sont des nombres positifs, la suite des sommes partielles $S_q = \sum_{k=0}^{q} (\text{trace } A^q)$ est croissante, majorée, ($S_q \leqslant u_{2q+1}$ par exemple), donc la série des trace (A^k) converge, et son terme général tend vers 0.

En particulier $\lim_{k \to +\infty} \left(\sum_{i=1}^{n} (\lambda_i)^{2k} \right) = 0$, donc chaque $|\lambda_i|$ est strictement inférieur à 1.

Le rayon spectral $\rho(A)$ étant < 1, il suffit alors de savoir que $(I_n - A)^{-1} = \sum_{k=0}^{+\infty} A^k$, (passez à la limite dans l'identité $(I_n - A)(I_n + A + ... + A^q) = I_n - A^{q+1}$, avec A^{q+1} du type $A^{q+1} = Q(\text{ diag } (\lambda_1^{q+1}, ..., \lambda_i^{q+1}))Q^{-1}$, Q orthogonale), pour en déduire, chaque A^k étant à coefficients positifs, que $(I_n - A)^{-1}$ est à coefficients positifs.

5.25. Soit $\mathscr{B} = (e_1, ..., e_n)$ une base orthonormée de vecteurs propres de C, (symétrique réelle), pour les valeurs propres $\lambda_1, ..., \lambda_n$.

Si $x = \sum_{i=1}^{n} x_i e_i$ est de norme 1, on a $\sum_{i=1}^{n} x_i^2 = 1$, et $C(x) = \sum_{i=1}^{n} \lambda_i x_i e_i$ étant connu dans une base orthonormée, on a :

$$\|C(x)\|^2 = \sum_{i=1}^{n} (\lambda_i)^2 (x_i)^2 \leqslant (\rho(C))^2 \sum_{i=1}^{n} (x_i)^2 = (\rho(C))^2,$$

d'où $|||C||| = \sup \{\|C(x)\| ; \|x\| = 1\} \leqslant \rho(C)$.

Puis, si $\rho(C) = |\lambda_{i_0}|$, on a $\|C(e_{i_0})\| = |\lambda_{i_0}| \leqslant |||C|||$, d'où l'égalité cherchée.

En fait, il faut faire un détour par les espaces hermitiens pour la suite, en remarquant que, pour le produit scalaire hermitien canonique sur $\mathbb{C}^n$, et pour H matrice hermitienne, on a, avec la même justification : $\rho(H) = |||H|||$.

Soient A et B dans $\mathcal{M}_n(\mathbb{R})$, et λ une valeur propre, (réelle ou complexe), de AB, et $X \in \mathcal{M}_{n,1}(\mathbb{C})$ un vecteur colonne tel que $ABX = \lambda X$. On a :

$$|\lambda|^2 \|X\|^2 = \bar{\lambda}\, {}^t\overline{X}(\lambda X) = \langle ABX, ABX\rangle$$
$$= \langle BX, {}^t\overline{A}A(BX)\rangle = \langle BX, {}^tAA(BX)\rangle,$$

car A est matrice réelle.

Comme $H = {}^tAA$ est symétrique réelle, donc hermitienne, on a :

$$|\lambda|^2 \|X\|^2 \leqslant \|BX\| \|{}^tAA(BX)\| \leqslant \|BX\| |||{}^tAA||| \|BX\| ;$$

or $|||{}^tAA||| = \rho({}^tAA)$, et $\|BX\|^2 = \langle BX, BX\rangle = \langle X, {}^t\overline{B}BX\rangle$, d'où :

$$|\lambda|^2 \|X\|^2 \leqslant \rho({}^tAA)\langle X, ({}^tBB)X\rangle \leqslant \rho({}^tAA)\|X\| |||{}^tBB||| \|X\|,$$

car B aussi est réelle, et finalement, on a :

$$|\lambda|^2 \|X\|^2 \leqslant \rho({}^tAA)\rho({}^tBB)\|X\|^2.$$

Comme on peut prendre X non nul, il vient $|\lambda|^2 \leqslant \rho({}^tAA)\rho({}^tBB)$, et en passant au sup des modules des valeurs propres, on a bien :

$$(\rho(AB))^2 \leqslant \rho({}^tAA)\rho({}^tBB).$$

5.26. Sur E euclidien, les endomorphismes symétriques étant diagonalisables dans le groupe orthogonal, on peut déjà choisir une base orthonormée de vecteurs propres pour b. En notant A et B les matrices

de a et b dans cette base, on prendra $B = \text{diag}(\mu_1, ..., \mu_n)$, d'où $e^B = \text{diag}(e^{\mu_1}, ..., e^{\mu_n})$.

De plus, il existe P matrice orthogonale, de terme général p_{ij}, telle que $P^{-1}AP = \text{diag}(\lambda_1, ..., \lambda_n)$, d'où $P^{-1}e^AP = \text{diag}(e^{\lambda_1}, ..., e^{\lambda_n})$, et $P^{-1}(e^A A)P = \text{diag}(e^{\lambda_1}\lambda_1, ..., e^{\lambda_n}\lambda_n)$. Par linéarité de la trace, on a :

$$\text{trace}\,(e^a(a-b) - e^a + e^b) = \text{trace}\, e^a a - \text{trace}\, e^a b - \text{trace}\, e^a + \text{trace}\, e^b$$

$$= \sum_{i=1}^{n} e^{\lambda_i}(\lambda_i - 1) - \text{trace}\, e^a b + \text{trace}\, e^b,$$

et il nous reste à évaluer les traces de $e^a b$ et de e^b.

La dernière, c'est $\sum_{j=1}^{n} e^{\mu_j}$, le travail sérieux va concerner la trace de $e^a b$. On a :

$$\text{trace}\,(e^a b) = \text{trace}\,(e^A \text{ diag}(\mu_1, ..., \mu_n))$$

$$= \text{trace}\,[P^{-1}(e^A P P^{-1} \text{ diag}(\mu_1, ..., \mu_n))P]$$

$$= \text{trace}\,(\text{diag}(e^{\lambda_1}, ..., e^{\lambda_n})P^{-1} \text{ diag}(\mu_1, ..., \mu_n)P).$$

Si on note respectivement : $\text{diag}(\mu_1, ..., \mu_n)P = (\alpha_{ij})$;

$P^{-1} \text{ diag}(\mu_1, ..., \mu_n)P = {}^tP \text{ diag}(\mu_1, ..., \mu_n)P = (\beta_{ij})$;

et $\text{diag}(e^{\lambda_1}, ..., e^{\lambda_n})P^{-1} \text{ diag}(\mu_1, ..., \mu_n)P = (\gamma_{ij})$, on doit évaluer la somme des γ_{ii}.

$$\text{On a } \gamma_{ii} = e^{\lambda_i}\beta_{ii} = e^{\lambda_i}\sum_{k=1}^{n} p_{ki}\alpha_{ki}$$

$$= e^{\lambda_i}\sum_{k=1}^{n} p_{ki}(\mu_k p_{ki})$$

$$= e^{\lambda_i}\sum_{k=1}^{n} (p_{ki})^2\mu_k, \text{ d'où :}$$

$$\text{trace}\, e^a b = \sum_{i=1}^{n} e^{\lambda_i}\left(\sum_{k=1}^{n} (p_{ki})^2\mu_k\right).$$

On comprend bien qu'il faut éliminer les p_{ki}, ce qui peut se faire parce que la matrice P est orthogonale, et pour cela il faudrait factoriser μ_k : pas possible, ou e^{λ_i} si on intervertit les sommations : pas possible. Mais en fait on peut se rappeler qu'on cherche une inégalité, donc on va minorer l'expression cherchée. On a :

$$\text{trace}\,(e^a(a-b)-e^a+e^b) = \sum_{i=1}^{n} e^{\lambda_i}(\lambda_i-1) + \sum_{k=1}^{n} e^{\mu_k} - \sum_{i=1}^{n} e^{\lambda_i} \sum_{k=1}^{n} \mu_k (p_{ki})^2 .$$

Pour faire intervenir l'aspect « matrice orthogonale » qui nous donne $\sum_{k=1}^{n} (p_{ki})^2 = 1$, et comme, pour comparer deux sommes, c'est plus facile si elles sont indexées de la même façon, on va écrire, (P étant orthogonale) :

$$\begin{aligned}
&\sum_{k=1}^{n} e^{\mu_k} - \sum_{i=1}^{n} e^{\lambda_i} \sum_{k=1}^{n} \mu_k (p_{ki})^2 \\
&\quad = \sum_{k=1}^{n} e^{\mu_k} \sum_{i=1}^{n} (p_{ki})^2 - \sum_{i=1}^{n} e^{\lambda_i} \sum_{k=1}^{n} \mu_k (p_{ki})^2 \\
&\quad = \sum_{i=1}^{n} \sum_{k=1}^{n} (p_{ki})^2 (e^{\mu_k} - \mu_k e^{\lambda_i}),
\end{aligned}$$

et étudier les variations de la fonction $f_i : x \rightsquigarrow e^x - xe^{\lambda_i}$, de dérivée $f'_i = e^x - e^{\lambda_i}$, positive pour $x > \lambda_i$, négative si $x < \lambda_i$, ce qui nous donne un minimum valant $f_i(\lambda_i)$, soit $e^{\lambda_i} - \lambda_i e^{\lambda_i}$.

On a donc $e^{\mu_k} - \mu_k e^{\lambda_i} \geqslant e^{\lambda_i}(1-\lambda_i)$, inégalité que l'on multiplie par $(p_{ki})^2$, d'où, en sommant :

$$\begin{aligned}
\sum_{k=1}^{n} e^{\mu_k} - \sum_{i=1}^{n} e^{\lambda_i} \sum_{k=1}^{n} \mu_k (p_{ki})^2 &\geqslant \sum_{i=1}^{n} e^{\lambda_i}(1-\lambda_i) \underbrace{\left(\sum_{k=1}^{n} (p_{ki})^2 \right)}_{=1} \\
&\geqslant \sum_{i=1}^{n} e^{\lambda_i}(1-\lambda_i),
\end{aligned}$$

d'où l'on déduit :

$$\text{trace}\,(e^a(a-b)-e^a+e^b) \geqslant \sum_{i=1}^{n} e^{\lambda_i}(\lambda_i-1) + \sum_{i=1}^{n} e^{\lambda_i}(1-\lambda_i) = 0 \text{ : il s'en est fallu de peu !}$$

5.27. Il s'agit d'une question de calculs. On a :

$$q'(x_1, ..., x_{n-1}) = \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} (\alpha_{nn}\alpha_{ij} - \alpha_{nj}\alpha_{ni}) x_i x_j,$$ expression que l'on coupe en deux, en factorisant α_{nn} dans la première pour obtenir :

$$q'(x_1, ..., x_{n-1}) = \alpha_{nn} \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \alpha_{ij} x_i x_j - \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} \alpha_{nj}\alpha_{ni} x_i x_j.$$

La première somme, si on introduit $X = (x_1, ..., x_{n-1}, 0)$, vecteur de $\mathbb{R}^n$, c'est exactement :

$$\alpha_{nn} \sum_{i=1}^{n} \sum_{j=1}^{n} \alpha_{ij} x_i x_j,$$

puisque, si $i = n$, (ou $j = n$), $x_i = 0$, (ou $x_j = 0$).

En notant $\{e_1, ..., e_n\}$ la base canonique de $\mathbb{R}^n$, c'est donc encore $q(e_n)q(X)$.

La deuxième somme se calcule en :

$$\sum_{i=1}^{n-1} \alpha_{ni} x_i \left(\sum_{j=1}^{n-1} \alpha_{nj} x_j \right) = \left(\sum_{j=1}^{n-1} \alpha_{nj} x_j \right) \left(\sum_{i=1}^{n-1} \alpha_{ni} x_i \right).$$

Si on note φ la forme polaire de q, on a $\alpha_{nj} = \varphi(e_n, e_j)$, donc cette somme est encore, avec $x_n = 0$:

$$\left(\sum_{j=1}^{n} x_j \varphi(e_n, e_j) \right)^2 = \left(\varphi\left(e_n, \sum_{j=1}^{n} x_j e_j\right) \right)^2$$

$$= (\varphi(e_n, X))^2,$$

si bien qu'avec $X = (x_1, ..., x_{n-1}, 0)$, on obtient :

$$q'(x_1, ..., x_{n-1}) = q(e_n)q(X) - (\varphi(e_n, X))^2.$$

C'est le moment d'aller chercher Cauchy-Schwarz par la main, et de se rappeler que $(\varphi(e_n, X))^2 \leqslant q(e_n)q(X)$, puisque q est positive, pour obtenir q' positive.

De plus, si $q'(x_1, ..., x_{n-1}) = 0$, on a égalité dans l'inégalité de Cauchy pour q définie positive, c'est que $X = (x_1, ..., x_{n-1}, 0)$ et

$e_n = (0, ..., 0, 1)$ sont liés, donc avec $X = \alpha \cdot e_n$ il n'y a pas le choix : $\alpha = 0$, d'où $x_1 = x_2 = ... = x_{n-1} = 0$.

En conclusion, q' est bien définie positive sur $\mathbb{R}^{n-1}$.

5.28. Si, pour x et y dans E, on pose :

$$f(x, y) = \phi(a)\varphi(x, y) - \varphi(a, x)\varphi(a, y),$$

il est clair que f est bilinéaire symétrique et que $F(x) = f(x, x)$, d'où F forme quadratique de forme polaire f.

On aura x dans le noyau de F si et seulement si, pour tout y de E, on a :

$$\phi(a)\varphi(x, y) - \varphi(a, x)\varphi(a, y) = 0.$$

Commençons par le plus simple. *Si a est dans le noyau* E^0 de ϕ, on a $\phi(a) = 0$, et $\varphi(a, y) = 0$ pour tout y, donc la condition est vérifiée pour tout x de E : *le noyau de F est E entier.* D'ailleurs dans ce cas F est nulle, ce qui se voit dès le départ.

Puis, si a est isotrope, sans être dans le noyau de ϕ, il existe y_0 dans E tel que $\varphi(a, y_0) \neq 0$, et si x est dans le noyau de F, on doit avoir $-\varphi(a, x)\varphi(a, y_0) = 0$, d'où $\varphi(a, x) = 0$. Mais réciproquement, si $\varphi(a, x) = 0$, pour tout y de E on a bien :

$$f(x, y) = -\varphi(a, x)\varphi(a, y) = 0,$$

donc dans ce cas, le noyau de F est $\{a\}^0$, conjugué pris pour ϕ.

Enfin, si a est non isotrope, la droite vectorielle $D = Ka$, (K corps de base) est alors sous-espace vectoriel de dimension finie, non isotrope, donc $E = Ka \oplus \{a\}^0$.

Si $\mathscr{B} = (e_i)_{i \in I}$ est une base de $\{a\}^0$, $\mathscr{B} \cup \{a\}$ en est une de E, et on aura x dans le noyau de F, si et seulement si, pour tout élément y de $\mathscr{B} \cup \{a\}$, on a :

$$\phi(a)\varphi(x, y) - \varphi(a, x)\varphi(a, y) = 0,$$

ceci par linéarité en y de l'expression.

Pour $y = a$, on doit avoir $\phi(a)\varphi(x, a) - \varphi(a, x)\phi(a) = 0$, ce qui est vérifié, et si y est l'un des e_i, on aura $\varphi(a, e_i) = 0$, donc il reste la condition $\phi(a)\varphi(x, e_i) = 0$, avec $\phi(a) \neq 0$, soit $\varphi(x, e_i) = 0$, ceci pour tout e_i de la base $\mathscr{B}$ de $\{a\}^0$.

Finalement, dans ce cas le noyau de F est $(\{a\}^0)^0$, (conjugué pour ϕ à chaque fois).

5.29. S'il existe r tel que $Q' + rQ$ soit définie positive, en particulier, sa restriction à Ker u sera aussi définie positive, or, pour x dans Ker u, on a :

$$(Q' + rQ)(x) = Q'(x) + r(\|u(x)\|)^2,$$

avec $u(x) = 0$: la restriction est celle de Q' à Ker u, qui est donc définie positive.

Réciproquement, on suppose la restriction de Q' à Ker u définie positive. De ce fait, Ker u est non isotrope pour Q', car si $x \in \text{Ker } u \cap (\text{Ker } u)^0$, conjugué pris pour Q', on aura, avec φ' forme bilinéaire symétrique associée à Q' :

$$Q'(x) = \varphi'(x, x) = 0, \text{ puisque } x \in \text{Ker } u \text{ et } x \in (\text{Ker } u)^0.$$

Mais alors x est nul, ($Q'|_{\text{Ker } u}$ définie).

Soit $\mathscr{B}_1$ une base de Ker u, supposé de dimension p, et $\mathscr{B}_2$ une base de $(\text{Ker } u)^0$. Comme Ker u est non isotrope, de dimension finie, (E étant de dimension n), on a E somme directe de Ker u et de $(\text{Ker } u)^0$, conjugué pour Q'.

Comme $Q'|_{\text{Ker } u}$ est définie positive, on prend $\mathscr{B}_1$ orthonormée pour Q'.

Par ailleurs, la restriction de Q à $(\text{Ker } u)^0$ est définie positive, car, pour x dans $(\text{Ker } u)^0$, on a $Q(x) = \|u(x)\|^2 \geqslant 0$, et si c'est nul, $u(x) = 0$, donc $x \in \text{Ker } u$. Comme on a vu que $\text{Ker } u \cap (\text{Ker } u)^0 = \{0\}$, x est nul.

On peut alors choisir $\mathscr{B}_2$ orthonormée pour la restriction de Q à $(\text{Ker } u)^0$.

Soit $\mathscr{B}_1 = \{e_1, ..., e_p\}$ et $\mathscr{B}_2 = \{e_{p+1}, ..., e_n\}$, et φ et φ' les formes bilinéaires symétriques associées à Q et Q' respectivement.

On a $\varphi(x, y) = \langle u(x), u(y) \rangle$, (ce qui au passage justifie le côté forme quadratique de Q), donc si $i \leqslant p$ ou $j \leqslant p$, on aura $\varphi(e_i, e_j) = 0$ car alors $u(e_i)$ sera nul, (ou $u(e_j) = 0$).

Comme $\mathscr{B}_2$ est orthonormée pour φ, la matrice A de Q dans la base $\mathscr{B} = \mathscr{B}_1 \cup \mathscr{B}_2$ est la matrice bloc :

$$A = \left(\begin{array}{c|c} 0 & 0 \\ \hline 0 & I_{n-p} \end{array}\right).$$

Soit A' la matrice de Q' dans la base $\mathscr{B}$. On a déjà $\mathscr{B}_1$ base orthonormée pour Q', et pour tout e_i de Ker u, et e_j de $(\text{Ker } u)^0$, (conjugué pour Q'), on a $\varphi'(e_i, e_j) = 0$, donc A' est une matrice bloc du type :

$$A' = \left(\begin{array}{c|c} I_p & 0 \\ \hline 0 & D \end{array}\right),$$

avec D matrice symétrique réelle.

Mais alors, $Q' + rQ$ a pour matrice dans la base $\mathscr{B}$, A" avec :

$$A'' = \left(\begin{array}{c|c} I_p & 0 \\ \hline 0 & D + rI_{n-p} \end{array}\right),$$

de valeurs propres 1 et les $\lambda_j + r$, avec λ_j valeur propre de D. Il est évident que si $r > \sup\{-\lambda_j\}$, la matrice A" sera définie positive comme ayant toutes ses valeurs propres strictement positives.

Imprimé en France
Imprimerie des Presses Universitaires de France
73, avenue Ronsard, 41100 Vendôme
Septembre 1997 — N° 44 448

Je me suis efforcé, en rédigeant ces exercices, de répondre à la question qui se pose à tous les candidats aux concours de grandes écoles : comment organiser rationnellement la recherche de la solution d'un problème ?

Une réflexion sur l'énoncé doit d'abord permettre au candidat de se situer dans telle ou telle partie des mathématiques.

Si les notions intervenant dans le problème sont proches de mécanismes constructifs déjà rencontrés dans telle ou telle partie mathématique du cours, on pourra alors s'y référer pour la justification de résultats (bases des espaces vectoriels, parties génératrices d'une structure...).

Dans cet esprit, le présent ouvrage ne se limite pas à l'énoncé d'une collection de résultats à connaître, mais se veut constituer un essai d'exposition par l'exemple d'une méthode de travail.

La partie Algèbre générale est renforcée, conformément aux nouveaux programmes des classes MP*.

198 FF 22412579/9/97