Quelques classiques d'algèbre

Les exercices qui suivent sont parfois difficiles, et sont choisis suivant les critères suivants : ils sont intéressants, ils se posent à l'oral, on ne perd pas son temps en les cherchant.
Mais faut-il le rappeler ? la priorité, c'est le cours !

1 Arithmétique

Il y a de l'arithmétique à l'oral : parce qu'elle permet de faire du Python facilement (Centrale), parce qu'on peut y faire de petits exercices (Mines), parce qu'on y trouve des problèmes difficiles mais explorables (X-ens).

994.1

Centrale

On appellera fonction multiplicative toute application $f : \mathbf{N}^* \to \mathbf{C}$ telle que

$$\forall m, n \in \mathbf{N}^* \ m \wedge n = 1 \Rightarrow f(mn) = f(m)f(n)$$

1. Programmer une fonction Python pgcd telle que, si $a, b \in \mathbf{N}^*$, pgcd(a,b) renvoie $a \wedge b$.
2. On définit des fonctions $\phi, \tau, \sigma, \mu : \mathbf{N}^* \to \mathbf{C}$ en posant, pour $n \in \mathbf{N}_*$,
   $\phi(n) = |\{x \in [\![1, n]\!] \ ; \ x \wedge n = 1\}|$, $\tau(n) = |\{d \in [\![1, n]\!] \ ; \ d \text{ divise } n\}|$,
   $\sigma(n) = \sum_{d|n} d$,
   $\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier} \\ (-1)^k & \text{si } n \text{ est le produit de } k \text{ nombres premiers distincts} \end{cases}$
   Montrer que ces quatre fonctions sont multiplicatives.
3. Programmer en Python ces quatre fonctions.
4. On note $\mathcal{M}$ l'ensemble des fonctions multiplicatives non nulles. Pour $f, g \in \mathcal{M}$, on définit $f * g : \mathbf{N}_* \to \mathbf{C}$, $n \mapsto \sum_{d|n} f(d)g(n/d)$. On admet que $(\mathcal{M}, *)$ est un groupe abélien. Soit $e : \mathbf{N}_* \to \mathbf{C}$, $n \mapsto \delta_{n,1}$ et $\mathbf{1} : \mathbf{N}_* \to \mathbf{C}$, $n \mapsto 1$. Montrer que e est l'élément neutre de $(\mathcal{M}, *)$ et que $\mathbf{1} * \mu = e$.
5. Soit $H \in \mathcal{M}$. On pose $h : \mathbf{N}_* \to \mathbf{C}$, $n \mapsto \sum_{d|n} H(d)$. Montrer que
   $$\forall n \in \mathbf{N}^* \quad H(n) = \sum_{d|n} \mu(d) h\left(\frac{n}{d}\right)$$
   Expliciter ces relation lorsque $H = \phi$.
6. Soit $f \in \mathcal{M}$, $F = \mu * f$ et $M = (f(i \wedge j))_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbf{R})$. On pose $D = \operatorname{diag}(F(1), \ldots, F(n))$ et $A = (1_{i|j})_{1 \leq i,j \leq n}$. Calculer $A^T D A$ et en déduire $\det(M)$. Calculer $\det(M)$ pour $f = Id$, $f = \sigma$ et $f = \tau$.

C'est tout ?

Cet énoncé, posé à Centrale, beaucoup trop long (en plus il y a du Python), ne contient que des choses intéressantes.

2. Pour ϕ, on a déjà vu cela, comme conséquence du théorème chinois. Rappelons que l'on a un isomorphisme « naturel », quand $m \wedge n = 1$, entre $\mathbf{Z}/mn\mathbf{Z}$ et $\mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/n\mathbf{Z}$:

$$x \bmod mn \longrightarrow (x \bmod m, x \bmod n)$$

Et qu'il induit un isomorphisme entre les groupes multiplicatifs des éléments inversibles dans chacun de ces anneaux, donc un isomorphisme de $(\mathbf{Z}/mn\mathbf{Z})^*$ sur $(\mathbf{Z}/m\mathbf{Z})^* \times (\mathbf{Z}/n\mathbf{Z})^*$, ce qui permet de conclure que ces deux ensembles sont de même cardinal. On peut aussi faire un peu plus simple et dire que c'est un corollaire du théorème de Gauss que $x \wedge mn = 1$ si et seulement si $x \wedge m = x \wedge n = 1$…Il est prudent de savoir redémontrer le théorème chinois, même si la longueur de l'énoncé laisse dubitatif quant à la présence de questions de cours ! Notons maintenant D_n l'ensemble des diviseurs de n compris entre 1 et n. L'application

$$(a, b) \longmapsto ab$$

est une application de $D_m \times D_n$ dans D_{nm}. Sa bijectivité est une application du théorème de Gauss (on peut aussi, si on se sent plus à l'aise avec cela, la justifier avec les décompositions en facteurs premiers de m et de n). Donc τ est multiplicative.

Le fait que σ soit multiplicative s'en déduit, via le développement par distributivité :

$$\left(\sum_{d\in D_m} d\right)\left(\sum_{\delta\in D_n} \delta\right) = \sum_{(d,\delta)\in D_m\times D_n} d\delta$$

La mutliplicativité de μ est enfin, sans doute, la plus facile des quatre.

4. A noter : l'associativité de $*$ est un exercice d'écriture pas forcément inintéressant.

La neutralité de e est assez simple. Facilement, $(\mathbf{1} * \mu)(1) = 1$ (on a $\mu(1) = 1$, car 1 est le produit de 0 nombres premiers distincts). Si $n > 1$, n a au moins un diviseur premier. Soit $p_1, \dots, p_r$ les diviseurs premiers de n (comptés chacun une seule fois). Alors les seuls diviseurs de n ayant une image non nulle par μ sont les $p_1^{\epsilon_1} \dots p_r^{\epsilon_r}$ avec chaque ϵ_k égal à 0 ou 1. Et donc

$$\mathbf{1} * \mu(n) = \sum_{(\epsilon_1,\dots,\epsilon_r)\in\{0,1\}^r} (-1)^{\epsilon_1+\dots+\epsilon_r}$$

Il suffit de faire dans cette somme deux paquets, les termes pour lesquels $\epsilon_1 = 0$ et ceux pour lesquels $\epsilon_1 = 1$, pour voir qu'elle est nulle, puisqu'elle vaut

$$\left(\sum_{(\epsilon_2,\dots,\epsilon_r)\in\{0,1\}^{r-1}} (-1)^{\epsilon_2+\dots+\epsilon_r}\right) - \left(\sum_{(\epsilon_2,\dots,\epsilon_r)\in\{0,1\}^{r-1}} (-1)^{\epsilon_2+\dots+\epsilon_r}\right)$$

5. h=**1***H, donc $\mu * h = (\mu * \mathbf{1}) * H = e * H = H$. Mais

$$\sum_{d|n} \phi(d) = n$$

(en classant les éléments de $\mathbf{U}_n$ suivant le $\mathbf{U}_d$ qu'ils engendrent, exercice classique mais dont on ne se souviendra pas forcément ! L'examinateur ne sera pas là offusqué de devoir mettre un peu le candidat sur la piste). Donc

$$\phi(n) = \sum_{d|n} \left(\frac{n}{d}\right) \mu(d)$$

6. Le coefficient (i, j) de $A^T DA$ est

$$\sum_{k=1}^{n} 1_{k|i} F(k) 1_{k|j} = \sum_{k=1}^{n} 1_{k|i\wedge j} F(k) = f(i \wedge j)$$

(par la question précédente). Mais A est triangulaire, avec une diagonale de 1, donc

$$\det(M) = F(1) \dots F(n)$$

Pour $f = Id$, $F = \phi$ a déjà été vu. De plus $\sigma = \mathbf{1} * id$, donc $\mu * \sigma = Id$, $\tau = \mathbf{1} * \mathbf{1}$, donc $\mu * \tau = \mathbf{1}$, ce qui donne les résultats demandés.

994.2

Soit p un nombre premier. On note Z_p l'ensemble des a/b où $(a,b) \in \mathbf{Z} \times \mathbf{N}^*$ et p ne divise pas b. On note J_p l'ensemble des a/b où $(a,b) \in \mathbf{Z} \times \mathbf{N}^*$, p divise a et p ne divise pas b.

1. Montrer que Z_p est un sous-anneau de $\mathbf{Q}$.
2. Montrer que J_p est un idéal de Z_p et que tout idéal de Z_p autre que Z_p est inclus dans J_p.
3. Déterminer tous les idéaux de Z_p.

---

1. ne pose pas de difficulté particulière.
2. Pas tellement non plus de problème pour montrer que J_p est un idéal de Z_p. Soit I un idéal de Z_p non inclus dans J_p. Soit $a/b \in I$ avec p ne divisant ni a ni b. Alors $b/a \in Z_p$; donc par absorbance $1 = (a/b)(b/a) \in I$. Et, toujours par absorbance, un idéal qui contient 1 contient tout. Donc $I = Z_p$, ce qui conclut par contraposition.
3. On note J_{p^k} l'ensemble des a/b où $(a,b) \in \mathbf{Z} \times \mathbf{N}^*$, p^k divise a et p ne divise pas b ($k \in \mathbf{N}$). Il est assez simple de montrer que les J_{p^k} sont des idéaux de Z_p. Soit I un idéal de Z_p. Il existe un k_0 minimal tel que I ne soit pas inclus dans $J_{p^{k_0}}$ (car l'intersection de tous les J_{p^k} est vide). On a alors $I = J_{p^{k_0-1}}$, de la même manière que ci-dessus. On a donc trouvé tous les idéaux.

994.3

Formule de Legendre

Soit $n \geq 2$, p premier.
Exprimer $\nu_p(n!)$ à l'aide des $\lfloor \frac{n}{p^k} \rfloor$, $k \geq 1$.
Par combien de 0 se termine l'écriture décimale de 2025! ?

On a

$$\nu_p(n!) = \sum_{m=2}^{n} \nu_p(m)$$

Il y a dans $[\![2,n]\!]$ un nombre de multiples de p^k égal à $\lfloor \frac{n}{p^k} \rfloor$ (pour $k \geq 1$). Si on est multiple de p^{k+1} on est multiple de p^k, on obtient donc :

$$\nu_p(n!) = \sum_{k=1}^{+\infty} k \left(\lfloor \frac{n}{p^k} \rfloor - \lfloor \frac{n}{p^{k+1}} \rfloor \right)$$

(la somme est finie). Coupant la somme en deux, réindexant l'une des deux sommes obtenues, on parvient à

$$\nu_p(n!) = \sum_{k=1}^{+\infty} \lfloor \frac{n}{p^k} \rfloor$$

Comme $\nu_5(2018!) < \nu_2(2025)$, le nombre de 0 cherchés est $\nu_5(2025!)$, c'est-à-dire

$$\sum_{k=1}^{+\infty} \lfloor \frac{2025}{5^k} \rfloor$$

qui vaut $403 + 80 + 16 + 3$ c'est-à-dire 502.

994.4

Résoudre le système

$$\begin{cases} \overline{3}x + \overline{7}y &= \overline{3} \\ \overline{6}x - \overline{7}y &= \overline{0} \end{cases}$$

dans $\mathbf{Z}/36\mathbf{Z}$ puis dans $\mathbf{Z}/37\mathbf{Z}$.

On a irrésistiblement envie d'ajouter les équations, pour supprimer la deuxième inconnue. D'où $\overline{9}x = \overline{3}$. La multiplication par $\overline{4}$, dans $\mathbf{Z}/36\mathbf{Z}$, donne une contradiction. En revanche, dans $\mathbf{Z}/37\mathbf{Z}$ qui est un corps, pas d'astuce ni de surprise : on calcule le déterminant, qui vaut $-\overline{26}$ et donc est non nul. Il y a donc une solution unique. La multiplication par $\overline{4}$ de $\overline{9}x = \overline{3}$ donne $x = -\overline{12}$, puis il ne reste qu'à trouver $\overline{7}^{-1}$ pour déterminer y. Ce qui peut se faire systématiquement à l'aide d'un algorithme d'Euclide entre 37 et 7 :

$$37 = 5 \times 7 + 2$$

$$7 = 3 \times 2 + 1$$

Donc $1 = 16 \times 7 - 3 \times 37$ et $\overline{7}^{-1} = \overline{16}$. D'où

$$y = \overline{16} \times \overline{3} \times (\overline{1} - \overline{-12}) = \overline{-5} = \overline{32}$$

(sauf erreur de calcul).

994.5

1. Montrer que tout sous-groupe d'un groupe cyclique est cyclique.
2. Soit d, n entiers tels que $d|n$. Montrer que $\mathbf{Z}/n\mathbf{Z}$ a un unique sous-groupe d'ordre d.
3. Montrer que $n = \sum_{d|n} \phi(d)$, où ϕ désigne l'indicateur d'Euler.

---

1. Méthode 1 : (Inspirée par l'observation de $\mathbf{U}_{12}$ par exemple) : soit $(G, *)$ un groupe cyclique d'ordre n, g un générateur de G. On a alors

$$G = \{g^k \ ; \ k \in \mathbf{Z}\} \ = \ \{g^k \ ; \ 0 \leq k \leq n-1\}$$

Soit H un sous-groupe de $(G, *)$ autre que $\{e\}$ (ce dernier est clairement cyclique). Comme H est fini, il suffit d'en trouver un générateur. Considérons

$$k_0 = \min(\{k \in [\![1, n-1]\!] \ / \ g^k \in H\})$$

(un dessin dans $\mathbf{U}_{12}$ justifie ce choix). Alors $h_0 = g^{k_0} \in H$ et donc

$$\langle h_0 \rangle = \{h_0^k \ ; \ k \in \mathbf{Z}\} \subset H$$

($\langle h_0 \rangle$ est le sous-groupe de $(G, *)$ engendré par h_0). Soit réciproquement h un élément de H. Soit $k \in \mathbf{Z}$ tel que $h = g^k$. Il existe q, r entiers tels que $k = k_0 q + r$, $0 \leq r < k_0$. Donc

$$h = g^k = g^{k_0 q} * g^r = \left(g^{k_0}\right)^q * g^r = h_0^q * g^r$$

Donc $g^r = h_0^{-q} * h \in H$. Et la définition de k_0 fait que $r = 0$. On en déduit que $h = h_0^q$.
Conclusion : $H = \langle h_0 \rangle$ est cyclique.

Méthode 2 : Le morphisme ϕ_g permet de transférer des résultats de $(\mathbf{Z}, +)$ sur $(G, *)$.
Les sous-groupes de $(\mathbf{Z}, +)$ sont les $n\mathbf{Z}$, $n \in \mathbf{N}$; résultat qui n'est plus au programme de mpsi, mais qui se démontre comme le résultat analogue sur les idéaux.

> soit H un sous-groupe de $(\mathbf{Z}, +)$. Si $H = \{0\}$, c'est fini : $H = 0\mathbf{Z}$. Sinon, $H \cap \mathbf{N}_* \neq \emptyset$ (en effet, si h est un élément non nul de H, $-h \in H$, et $h > 0$ ou $-h > 0$).
> Soit $h_0 = \text{Min}\,(H \cap \mathbf{N}_*)$; comme $h_0 \in H$ et $(H, +)$ est un groupe, $\forall q \in \mathbf{Z} \quad qh_0 \in H$ (*Il faut voir que qh_0 n'est pas du tout, ici, le « produit » de la « multiplication » (????) de q par h_0*).
> Réciproquement, si $h \in H$, on divise
>
> $$h = qh_0 + r \quad , \quad 0 \leq r < h_0$$
>
> et $r = h - qh_0 \in H$ donc nécessairement $r = 0$. On a donc $H = h_0\mathbf{Z}$.

Notons que les sous-groupes de $\mathbf{K}[X]$ *ne sont en revanche pas tous des idéaux.*
Soit donc $(G,*)$ un groupe cyclique d'ordre n, g un générateur de $(G,*)$. Considérons le morphisme $\phi_g : z \mapsto g^z$ de $(\mathbf{Z},+)$ dans $(G,*)$. Ce morphisme est surjectif. Son noyau est $n\mathbf{Z}$ (cours).
Si H est un sous-groupe de $(G,*)$, $\phi_g^{-1}(H)$ est un sous-groupe de $\mathbf{Z}$, donc il existe m entier naturel tel que $\phi_g^{-1}(H) = m\mathbf{Z}$. Or $\phi_g\big(\phi_g^{-1}(H)\big) = H$ (évidence ? pas tout-à-fait, c'est vrai seulement parce que ϕ_g est surjective). Donc

$$H = \phi_g(m\mathbf{Z}) = \langle g^m \rangle$$

Méthode 3 : On peut se contenter de résoudre le problème pour les sous-groupes de $(\mathbf{U}_n,\times)$, le résultat se transporte par isomorphisme…voir paragraphe suivant !

2. Méthode 1 : Déplaçons le problème vers le groupe $(\mathbf{U}_n,\times)$. Soit donc d un diviseur de n ; $(\mathbf{U}_d,\times)$ est un sous-groupe d'ordre d, il y a donc existence, reste à voir l'unicité. Soit H un sous-groupe d'ordre d de $\mathbf{U}_n$. Si $h \in H$, h est d'ordre m, et m divise d (cours !). Donc $h^d = 1$. Donc $h \in \mathbf{U}_d$.
Donc $H \subset \mathbf{U}_d$ et, comme $\mathrm{Card}(H) = \mathrm{Card}(\mathbf{U}_d)$, $H = \mathbf{U}_d$.
On a démontré que $(\mathbf{U}_n,\times)$ avait un unique sous-groupe d'ordre d. On a aussi démontré que les sous-groupes de $\mathbf{U}_n$ sont les $\mathbf{U}_d$ où $d|n$, ce qui répond aux deux premières questions !
[Soit ϕ un isomorphisme de $(\mathbf{Z}/n\mathbf{Z},+)$ sur $(\mathbf{U}_n,\times)$. ϕ transforme un sous-groupe d'ordre d de l'un en sous-groupe d'ordre d de l'autre, ce qui conclut.]

Méthode 2 : On reprend la méthode 2 précédente. De $e \in H$ on déduit que $\phi_g^{-1}(H)$ contient $\mathrm{Ker}(\phi_g)$. Et donc $n\mathbf{Z} \subset m\mathbf{Z}$. Et donc $m|n$. Or si $n = md$, on voit que l'ordre de g^m est d. Donc H est d'ordre d si et seulement si il est engendré par $g^{n/d}$. Et donc le seul sous-groupe d'ordre d est celui engendré par $g^{n/d}$.
3. L'indexation $d|n$, couramment utilisée en arithmétique, peut sembler vague. Elle désigne tous les diviseurs positifs de n, depuis 1 (compris) jusqu'à n (compris). Par exemple, si n est premier, la formule à démontrer est

$$p = \phi(p) + \phi(1)$$

qui n'est pas très difficile à voir !
Soit, si $d|n$, H_d l'unique sous-groupe d'ordre d de $(\mathbf{Z}/n\mathbf{Z},+)$. Soit A_d l'ensemble des générateurs de H_d. Comme H_d est cyclique, le cours dit que $\mathrm{Card}(H_d) = \phi(d)$.
Si $d \neq d'$, $A_d \cap A_{d'} = \emptyset$ (autrement dit : on ne peut pas engendrer deux groupes différents !)
Soit $g \in \mathbf{Z}/n\mathbf{Z}$, $\langle g \rangle$ le sous-groupe qu'il engendre. Ce sous-groupe est l'un des H_d. Donc g est dans l'un des A_d.
En conclusion on a une partition de $\mathbf{Z}/n\mathbf{Z}$:

$$\mathbf{Z}/n\mathbf{Z} = \bigcup_{d|n} A_d$$

et la réunion étant disjointe,

$$\mathrm{Card}(\mathbf{Z}/n\mathbf{Z}) = \sum_{d|n} \mathrm{Card}(A_d)$$

qui est le résultat attendu.
On peut bien entendu tout rédiger dans $\mathbf{U}_n$.

994.6

Indicatrice d'Euler : méthode probabiliste

Soit $n \geq 2$, on munit $\Omega = \{1,2,\ldots,n\}$ de la probabilité uniforme P. On note $\{p_1,\ldots,p_r\}$ l'ensemble des diviseurs premiers de n. On désigne par ϕ l'indicatrice d'Euler.

1. Soit d un diviseur de n ($d \geq 1$), A_d l'ensemble des multiples de d dans Ω. Calculer $P(A_d)$.
2. (a) Montrer que les évènements A_{p_i} $(1 \leq i \leq r)$ sont mutuellement indépendants.
   (b) En déduire que

$$\frac{\phi(n)}{n} = \prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)$$

(c) Calculer $\phi(36)$

---

1. Comme P est la probabilité uniforme sur Ω,

$$P(A_d) = \frac{\text{Card}(A_d)}{\text{Card}(\Omega)}$$

Or $A_d = \left\{d, 2d, \ldots, \frac{n}{d}d\right\}$. Donc $\text{Card}(A_d) = \frac{n}{d}$, et

$$P(A_d) = \frac{1}{d}$$

2.a. Attention à ne pas se contenter de montrer qu'ils sont indépendants deux à deux. Soit $\{i1, \ldots, im\}$ $(1 \leq m \leq r)$ une partie finie de $\{1, \ldots, r\}$. On a (c'est une conséquence du théorème de Gauss) :

$$\bigcap_{k=1}^{m} A_{p_{ik}} = A_{p_{i1} \ldots p_{im}}$$

(les p_{ik} sont des nombres premiers distincts, être divisible par leur produit c'est être divisible par chacun d'eux) ; donc

$$P\left(\bigcap_{k=1}^{m} A_{p_{ik}}\right) = \frac{1}{p_{i1} \cdots p_{im}} = \prod_{k=1}^{m} P\left(A_{p_{ik}}\right)$$

On en déduit l'indépendance mutuelle. Soit alors B l'ensemble des éléments de Ω premiers avec n. Ecrivant

$$B = \bigcap_{i=1}^{r} \overline{A_{p_i}}$$

et utilisant le fait que des complémentaires d'événements indépendants le sont, on trouve la formule. Et donc

$$\phi(36) = 36 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{3}\right) = 12$$

994.7

Théorème de Wolstenholme

Soit p un nombre premier, $S_p = \sum_{k=1}^{p-1} \frac{(p-1)!}{k(p-k)}$. On écrit $\sum_{k=1}^{p-1} \frac{1}{k} = \frac{a_p}{b_p}$ où a_p et b_p sont deux entier naturels premiers entre eux. La classe de $a \in \mathbf{Z}$ modulo p est notée $\overline{a}$.

1. Montrer que $(p-1)! \equiv -1$ $[p]$.
2. Montrer : $\overline{S_p} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^{-2} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^2$.
3. Montrer que, pour $p \geq 5$, p divise S_p.
4. Montrer que, pour $p \geq 5$, p^2 divise a_p.

---

1. La congruence de Wilson est un classique. On fait le produit des éléments de $\mathbf{Z}/p\mathbf{Z}^*$ en regroupant chaque classe avec son inverse. Deux classes restent seules : $\overline{1}$ et $\overline{-1}$.
2. Remarquons d'abord que $k(p-k)$ divise $(p-1)!$ pour tout k entre 1 et $p-1$; en effet, $(p-1)!$ est un produit de facteurs dont k et $p-k$ font partie (et ces deux facteurs sont bien distincts : $k = p-k$ donnerait p pair, d'où $p = 2$, cas trop évident pour être intéressant). Notons alors m_k le quotient de la division de $(p-1)!$ par $k(p-k)$:

$$(p-1)! = k(p-k)m_k$$

Alors, en prenant les classes modulo p (c'est-à-dire dans $\mathbf{Z}/p\mathbf{Z}$) :

$$\overline{(p-1)!} = \overline{k} \times \overline{p-k} \times \overline{m_k}$$

ou encore, tenant compte de la congruence de Wilson,

$$\overline{-1} = \overline{k} \times (\overline{-k}) \times \overline{m_k}$$

ce qui donne $\overline{m_k} = \overline{k}^{-2}$ et la formule attendue :

$$\overline{S_p} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^{-2}$$

Mais l'application $x \mapsto x^{-1}$ est une permutation de $(\mathbf{Z}/p\mathbf{Z})^*$, on a donc bien

$$\overline{S_p} = \sum_{x \in (\mathbf{Z}/p\mathbf{Z})^*} x^{2}$$

Il importe dans cette question de supprimer les fractions pour bien faire de l'arithmétique avec des entiers, c'est ce qui motive l'introduction des m_k

3. La formule précédente montre :

$$\overline{S_p} = \sum_{k=1}^{p-1} \overline{k}^2 = \overline{\Big(\frac{(p-1)p(2p-1)}{6}\Big)}$$

grâce à une formule sommatoire « connue » (mais qu'il faut savoir démontrer…). En notant que, si m est un entier, $\overline{6m} = 6\,\overline{m}$, on en déduit que $\overline{6} \times \overline{S_p} = \overline{p-1} \times \overline{p} \times \overline{2p-1} = \overline{0}$ Mais p ne vaut ici ni 2 ni 3, donc est premier avec 6, on conclut bien $\overline{S_p} = \overline{0}$, donc p divise S_p.

4. Remarquons la décomposition en éléments simples :

$$\frac{1}{k(p-k)} = \frac{1}{p}\big(\frac{1}{k} + \frac{1}{p-k}\big)$$

d'où l'on déduit

$$pS_p = \sum_{k=1}^{p-1} (p-1)!\Big(\frac{1}{k} + \frac{1}{p-k}\Big) = 2(p-1)!\frac{a_p}{b_p}$$

ou encore (toujours pour supprimer les fractions)

$$b_p p S_p = 2(p-1)! a_p$$

p^2 divise le membre de gauche (car S_p est multiple de p), et donc celui de droite, et est premier avec $2(p-1)!$ (qui est produit de nombre premiers avec p, donc avec p^2). Le théorème de Gauss permet alors de conclure.

---

2 Groupes

Peu de choses sont au programme sur les groupes.
Il faut connaître la définition, bien sûr, qui permet à elle seule de résoudre un classique :

994.8

oit H, K deux sous-groupes d'un groupe $(G,\ )$. On définit

$$HK = \{hk\ ;\ (h,k) \in H \times K\}$$

Montrer que HK est un sous-groupe de $(G,\ )$ si et seulement si $HK = KH$.

…solution plus loin. On connaît les groupes cycliques, il est conseillé, en plus du cours, de **savoir montrer que tout sous-groupe d'un groupe cyclique est cyclique, que si G est un groupe cyclique d'ordre n et si d est un diviseur de n alors G admet un unique sous-groupe d'ordre** d (rappel : l'ordre d'un groupe, c'est son cardinal). Comme une majorité d'exercices posés à l'oral sur les groupes concernent les groupes cycliques, c'est bien de refaire ces exercices déjà vus en début d'année. Rappelons une **idée importante** : ce qu'on fait pour $(\mathbf{U}_n, \times)$, on le fait pour n'importe quel groupe cyclique d'ordre n. Ce groupe $\mathbf{U}_n$ se représente graphiquement, ce qui aide à réfléchir et fait plaisir à l'interrogateur. On a intérêt à préférer la description

$$\mathbf{U}_n = \{\omega^k\ ;\ 0 \leq k \leq n-1\} \qquad (\omega = \exp(2i\pi/n))$$

à la description

$$\mathbf{U}_n = \{\exp(2ik\pi/n)\ ;\ 0 \leq k \leq n-1\}$$

pour au moins deux raisons : les écritures seront plus simples, et la transposition à un groupe cyclique quelconque sera plus évidente, puisqu'un tel groupe peut s'écrire $\{g^k\ ;\ 0 \leq k \leq n-1\}$.
Ce n'est pas parce que $(\mathbf{U}_n, \times)$ est (souvent) la bonne représentation d'un groupe cyclique qu'il faut oublier $(\mathbf{Z}/n\mathbf{Z}, +)$.

Les groupes cycliques sont les groupes commutatifs finis les plus simples. Il y a bien sûr des groupes infinis, mais il y a aussi des groupes finis non commutatifs. On révise donc bien le groupe $(\Sigma_n, \circ)$ qui montre une structure de groupe non commutative et beaucoup plus compliquée.

Un nombre significatif d'exercices s'intéressent à l'ordre d'un élément d'un groupe fini, en lien souvent avec le cardinal du groupe. Il faut donc rappeler quelques points importants : dans un groupe fini, tout élément est d'ordre fini, cet ordre divisant l'ordre du groupe. La preuve dans le cas commutatif est à connaître. Dans le cas non commutatif, il n'y a pas de preuve plus élémentaire que le passage par le célèbre théorème de Lagrange, hors programme mais fort intéressant : dans un groupe fini, abélien ou non, l'ordre d'un sous-groupe divise l'ordre du groupe.

Voici quelques exercices donnés récemment à Centrale, Mines, X :

994.9

n désigne par G un groupe abélien. Soit g un élément de G d'ordre fini n, g' un élément de G d'ordre fini n', on suppose n et n' premiers entre eux. Montrer que $g * g'$ est d'ordre fini nn'.

Montrer que $g * g'$ est d'ordre nn', c'est montrer que

$$(g * g')^k = e \ \Leftrightarrow \ nn' \mid k$$

D'abord, le plus facile :

$$(g * g')^{nn'} = g^{nn'} * (g')^{nn'} = (g^n)^{n'} * \left((g')^{n'}\right)^n = e$$

par commutativité de la loi $*$. On sait donc que $g * g'$ est d'ordre fini divisant nn'. Supposons maintenant

$$(g * g')^m = e$$

qui s'écrit par commutativité $g^m * (g')^m = e$. En élevant à la puissance n, on obtient $(g')^{mn} = e$, donc $n' \mid mn$, et par théorème de Gauss, $n' \mid m$. De même $n \mid m$. Et encore par corollaire du théorème de Gauss, $nn' \mid m$.
La conclusion s'ensuit.

994.10

oit $(G, .)$ un groupe fini dont tout élément est d'ordre 1 ou 2. Montrer que le cardinal de G est une puissance de 2.

Cet exercice est nettement plus délicat que le précédent. On peut constater qu'un groupe vérifie les hypothèses de l'énoncé :

$$\left((\mathbf{Z}/2\mathbf{Z})^n, +\right)$$

et qu'il est bien de cardinal 2^n. On peut (c'est à la fois d'une façon générale une bonne idée en math, et une démarche qui paît aux examinateurs) commencer humblement par de tous petits groupes : un groupe $\{e, g\}$ où $g^2 = e$ vérifie bien sûr les hypothèses.
Si on rajoute un élément : on a un groupe dans lequel figurent l'élément neutre e, deux éléments g_1 et g_2 tels que $g_1^2 = g_2^2 = e$. Il faut qu'il y ait aussi $g_1 g_2$ et $g_2 g_1$. Remarquons que $g_1 g_2$ ne peut être égal ni à g_1, ni à g_2 (sinon, on aurait $g_1 = e$ ou $g_2 = e$). Ni à e. En effet, si $g_1 g_2 = e$, alors $g_1 = g_2$ (en composant à gauche par g_1 ou à droite par g_2).
La question qui se pose est alors : aurait-on $g_1 g_2 = g_2 g_1$? mais oui, rappelons qu'on veut que tous les éléments soient d'ordre 1 ou 2. Donc, si g_1 et g_2 sont deux éléments d'un tel groupe, de deux choses l'une : ou bien $g_1 g_2 = e$, alors $g_1 = g_2$ et évidemment g_1 et g_2 commutent. Ou bien $g_1 g_2$ est d'ordre 2, et alors

$$g_1 g_2 g_1 g_2 = e$$

relation qu'il suffit de composer par g_1 à gauche et par g_2 à droite pour obtenir

$$g_2 g_1 = g_1 g_2$$

On a donc la commutativité des groupes considérés, et l'étude des petits, du type $\{e, g\}$ ou $\{e, g_1, g_2, g_1 g_2\}$. C'est bien parti ! L'étape suivante serait de voir qu'on a l'impression qu'un tel groupe serait, pour des g_k bien choisis, l'ensemble des $g_1^{\epsilon_1} \dots g_r^{\epsilon_r}$, les ϵ_k dans $\{0, 1\}$. Donc, finalement : un tel groupe G est commutatif. Soit $A = \{g_1, \dots, g_r\}$ une partie génératrice de cardinal minimal (il en existe nécessairement, puisque l'ensemble des cardinaux des parties qui engendrent G est une partie non vide de $\mathbf{N}_*$ donc a un plus petit élément). Soit

$$H = \{g_1^{\epsilon_1} \dots g_r^{\epsilon_r} \ ; \ (\epsilon_1, \dots, \epsilon_r) \in \{0, 1\}^r$$

On montre facilement que H est un sous-groupe de G, qu'il contient A et que si un sous-groupe de G contient A il contient H. Bref, $H = G$.

Reste à constater que H a bien, comme il en a l'air, un cardinal égal à 2^r, ce qui terminera la preuve. Or l'application

$$\phi \ : \ \begin{array}{ccc} (\mathbf{Z}/2\mathbf{Z})^r & \longrightarrow & G \\ (\epsilon_1, \dots, \epsilon_r) & \longmapsto & g_1^{\epsilon_1} \dots g_r^{\epsilon_r} \end{array}$$

en effet, on vérifie que c'est un morphisme de groupe, et si $(\epsilon_1, \dots, \epsilon_r)$ est un élément du noyau de ϕ tel que $\epsilon_j = 1$, alors g_j s'écrit comme produit de puissances des autres g_k, $k \neq j$, ce qui contredit la minimalité de A, car $A \setminus \{g_j\}$ serait génératrice.

Il y a d'autres manières de résoudre cet exercice…

994.11

oit $(G, .)$ un groupe abélien d'ordre pq, où p et q sont deux nombres premiers distincts. Montrer que G est cyclique. Est-ce encore vrai si l'on ne suppose plus a priori G abélien ?

Le cas de Σ_3, d'ordre 2×3, montre qu'un groupe d'ordre pq n'est pas nécessairement commutatif, donc non nécessairement cyclique.
Commençons par une remarque : un élément de G autre que l'élément neutre a pour ordre p, q ou pq. Autre remarque un peu moins évidente : si g est d'ordre p et h d'ordre q, alors $g.h$ est d'ordre pq (voir le premier exercice pour des détails). On va donc essayer de montrer qu'il est impossible que tous les éléments soient d'ordre p. Ainsi, il sera de même impossible que tous les éléments soient d'ordre q, et on aura terminé. Supposons donc que tout élément (autre que l'élément neutre bien sûr) soit d'ordre p. Tout élément g ∤é engendre donc un sous-groupe $\langle g \rangle$ d'ordre p. Remarquons que, pour deux éléments h et g autres que e, on a $\langle g \rangle = \langle h \rangle$ ou $\langle g \rangle \cap \langle h \rangle = \{e\}$. En effet, si $k \in (\langle g \rangle \cap \langle h \rangle) \setminus \{e\}$, alors k engendre $\langle g \rangle$ et k engendre aussi $\langle h \rangle$ (voir : générateurs d'un groupe cyclique). Il y a en tout N sous-groupes distincts de la forme $\langle g \rangle$, l'intersection de deux quelconques de ces sous-groupes est $\{e\}$. On a donc, par dénombrement,

$$N(p-1) + 1 = pq$$

Donc N est congru à 1 modulo p : $N = mp + 1$. Et alors

$$(mp+1)(p-1) + 1 = pq$$

donne $mp + (1 - m) = q$. Bon, ce n'est pas très concluant, on n'a pas assez utilisé la structure de groupe ! Considérons, si $\langle g \rangle \cap \langle h \rangle = \{e\}$ (il existe de tels g et h, sinon le cardinal de G est p),

$$K = \langle g \rangle . \langle h \rangle = \{g^a h^b \ ; \ 0 \leq a \leq p-1, \ 0 \leq b \leq p-1\}$$

C'est un sous-groupe de G (vérification aisée, ne pas oublier que $(G, .)$ est commutatif). De cardinal p^2 : en effet,

$$\begin{aligned} g^a h^b = g^{a'} h^{b'} &\Leftrightarrow g^{a-a'} = h^{b'-b} \\ &\Leftrightarrow a \equiv a'[p] \text{ et } b \equiv b'[p] \end{aligned}$$

Là, petit problème : on va avoir du mal à prétendre ne jamais avoir entendu parler du théorème de Lagrange, qui dit que l'ordre d'un sous-groupe divise l'ordre du groupe. Ce qui permet ici de conclure, car p^2 ne peut pas diviser pq. Mais il faudra redémontrer le théorème de Lagrange (à revoir, de toute façon). Et sinon ? comme $p^2 \neq pq$, on peut prendre un élément g_1 qui n'est pas dans K, considérer

$$K' = \langle g \rangle . \langle h \rangle = \{g^a h^b \ ; \ 0 \leq a \leq p-1, \ 0 \leq b \leq p-1\}$$

qui va être un sous-groupe de $(G, .)$ de cardinal p^3…et ça ne s'arrête jamais, contradiction bien sûr…

994.12

oit $(G, *)$ un groupe. On suppose que le cardinal de G s'écrit mq, q premier, $m < q$. Montrer que G contient au plus un sous-groupe de cardinal q.

Soit H un sous-groupe de cardinal q. Tout élément de H est d'ordre divisant q, donc d'ordre 1 ou q. Donc tout élément de H qui n'est pas d'ordre 1 (donc qui n'est pas l'élément neutre) est d'ordre q, donc engendre H, qui donc est nécessairement cyclique. Supposons qu'il y ait deux sous-groupes H et H' d'ordre q, distincts. Alors $H \cap H' = \{e\}$ (car si $h \in H \cap H'$, si $h \neq e$, alors h engendre à la fois H et H', qui sont alors égaux). L'application

$$(h, h') \longmapsto h * h'$$

est alors injective. En effet, si $h_1 * h'_1 = h_2 * h'_2$, on a $h_2^{-1} * h_1 = h'_2 * (h'_1)^{-1}$, cet élément de G étant à la fois dans H et H' est donc égal à e, d'où $h_1 = h_2$ et $h'_1 = h'_2$. Il y aurait donc au moins q^2 éléments dans G, ce qui est contraire à l'hypothèse.

Solution de l'exercice **994.8** :
Si $KH = HK$, avec des notations évidentes, tout hk peut s'écrire $k'h'$, et réciproquement. Donc (toujours avec des notations évidentes) :

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = (h_1h'_1)(k'_2k_2)$$

et

$$(hk)^{-1} = k^{-1}h^{-1} = h'k'$$

D'où la première implication. Pour la seconde, il suffit de remarquer que si h et k sont dans H et K respectivement, et si HK est un groupe, $(h^{-1}k^{-1})^{-1}$ est dans HK. Donc $KH \subset HK$. Et $(hk)^{-1}$ est de la forme $h'k'$, donc $hk = k'^{-1}h'^{-1} \in KH$ d'où l'inclusion réciproque.

3 Polynômes

994.13

Montrer qu'un polynôme P de $\mathbf{R}[X]$ vérifie

$$\forall x \in \mathbf{R} \qquad P(x) \geq 0$$

si et seulement si il existe A et B dans $\mathbf{R}[X]$ tels que

$$P = A^2 + B^2$$

994.14

Montrer qu'un polynôme P de $\mathbf{R}[X]$ vérifie

$$\forall x \in \mathbf{R}^+ \qquad P(x) \geq 0$$

si et seulement si il existe A et B dans $\mathbf{R}[X]$ tels que

$$P = A^2 + XB^2$$

Des exercices d'oral indémodables. Ce ne sont pas de bons exercices : ils ne récompensent pas l'effort fait pendant l'année pour apprendre et comprendre le cours. Mais il faut comprendre les examinateurs, qui ont besoin d'un stock important d'énoncés…
On est excusable d'errer un peu. Donc il peut être intéressant de retenir deux idées :

- **Décomposition en facteurs irréductibles.**
- **Stabilité par produit.**

Dans un anneau commutatif quelconque (c'est d'ailleurs probablement le plus intéressant dans ces énoncés), l'ensemble des sommes de deux carrés est stable par produit. Autrement dit,

$$(a^2 + b^2)(c^2 + d^2) = (\dots\dots)^2 + (\dots\dots)^2$$

La manière la plus simple de retrouver cette formule est d'écrire, pour deux nombres complexes $z = a + ib$ et $t = c + id$,

$$|z|^2 \ |t|^2 = |zt|^2$$

Cette belle formule est une identité de Lagrange, et se généralise à des cadres plus compliqués.
On remarque alors que, dans la décomposition de P en facteurs irréductibles sur $\mathbf{R}$, on trouve, si $P \geq 0$ sur $\mathbf{R}$, des

$$(X - \alpha)^{2m} \qquad (m \geq 1)$$

et/ou des

$$(X^2 + \alpha X + \beta)^m \qquad (m \geq 1, \alpha^2 - 4\beta < 0)$$

(ceci s'obtient en passant par $\mathbf{C}$, mais il n'est pas utile d'y revenir, le cours nous donne directement la décomposition sur $\mathbf{R}$). En effet, il n'y a pas de racine réelle de multiplicité impaire, au voisinage de laquelle le polynôme changerait de signe.
On peut même regrouper ces deux types de termes en autorisant, dans le second cas, le discriminant à être nul. Reste à utiliser la mise sous forme canonique :

$$X^2 + \alpha X + \beta = (X + \frac{\alpha}{2})^2 + \left(\sqrt{\beta - \frac{\alpha^2}{4}}\right)^2$$

et voilà...on ne multiplie que des sommes de carrés. Remarquons qu'un carré est évidemment considéré comme somme de carrés, l'un des deux étant nul. On a oublié le coefficient dominant, mais il est positif (envisager la limite en $+\infty$), c'est donc un carré...L'autre énoncé se traite de manière analogue, un petit peu plus technique quand même ?

994.15

Déterminer les polynômes $P \in \mathbf{R}[X]$ tels que $P(X^2) = P(X-1)P(X)$

En fait, cet exercice admet au moins 3 ou 4 déclinaisons différentes, mais qui se traitent de même. Une idée : **considérer les racines de P, sur $\mathbf{C}$**. En effet, on a ici des résultats simples, comme
Si z est zéro de P, z^2 aussi. Or un polynôme n'a qu'un nombre fini de racines (bon, c'est vrai que le polynôme nul est solution, on écarte ce cas pas très intéressant). On voit donc assez facilement que $z = 0$ ou $|z| = 1$ (la deuxième condition est un peu faible : on pourrait dire que z est une racine de l'unité, ce qui est plus précis).
Ensuite, si z est zéro de P, $(z+1)^2$ l'est aussi. Donc, d'après ce qui précède, $z+1 = 0$ ou $|z+1| = 1$.
A l'oral, on dessinera un cercle trigonométrique pour montrer qu'on a déjà bien restreint l'ensemble des racines possibles : 0, -1, j, j^2. Pour que le polynôme soit réel, il faut que j et j^2 soient racines de même multiplicité. Bref, sont candidats les polynômes

$$aX^r(X+1)^s(X^2+X+1)^t$$

où r, s, t sont des entiers naturels. Un tel polynôme conviendra, réciproquement, si et seulement si

$$aX^{2r}(X+1)^{2s}(X^2+X+1)^{2t} = a^2(X-1)^rX^{s+r}(X^2+X+1)^t(X+1)^r(X^2-X+1)^t$$

Par unicité de la décomposition en facteurs irréductibles, il n'y a que le polynôme 1...

Ce qu'il faut surtout retenir de ce qui précède, c'est qu'un polynôme P n'est pas avant tout quelque chose que l'on doit écrire $\sum_{k=0}^{n} a_k X^k$. Ce qui est bien facile à comprendre : quand bien même il serait judicieux de décomposer P dans une base, pourquoi spécialement la base canonique ? Mais il arrive qu'on le fasse quand même. Par exemple dans cet exercice désagréable posé quelques fois ces dernières années :

994.16

Trouver les $P \in \mathbf{C}[X]$ stabilisant le cercle unité $\mathbf{U}$ de $\mathbf{C}$.

La résolution se résume à une astuce : si P est de degré d, il suffit pour rendre la relation

$$P(e^{i\theta})\overline{P}(e^{-i\theta}) = 1$$

polynomiale en $e^{i\theta}$ de la multiplier par $e^{id\theta}$. Et ensuite, on a deux polynômes qui coïncident sur un ensemble infini (l'ensemble des nombres complexes de module 1), ils sont donc égaux, on conclut que les seuls polynômes solutions sont les polynômes « évidents » $e^{i\alpha}X^n$.

4 Réduction

994.17

Diagonaliser la matrice carrée réelle dont tous les coefficients valent 1.

Pour la diagonalisabilité, deux méthodes concluent immédiatement : dire que J est symétrique **réelle** ou remarquer que $J^2 = nJ$, donc $X(X-n)$, scindé simple, annule J.
Pour la diagonalisation effective, remarquons que $\mathrm{rg}(J) = 1$, donc le noyau de J est un sous-espace propre de dimension $n-1$. Donc $P_J = X^{n-1}(X - \mathrm{Tr}(J)) = x^{n-1}(X-n)$. Or le vecteur $U = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ est propre associé à n.
On a donc utilisé deux remarques essentielles à l'oral : constater que U est vecteur propre (90% des matrices qu'on demande de diagonaliser à l'oral…), voir que le rang est petit et donc qu'il y a un « gros » noyau.
Reste à compléter U avec les vecteurs d'une base de $\mathrm{Ker}(J)$, là aussi le plus rapide est de dire que comme J est symétrique réelle,

$$\mathrm{Ker}(J) = (\mathrm{Vect}(U))^{\perp}$$

et donc ce noyau est le sous-espace d'équation $x_1 + \cdots + x_n = 0$.
Encore une compétence évaluée par cet exercice : savoir qu'une matrice P inversible telle que $J = PDP^{-1}$, avec D diagonale, est une matrice dont les colonnes sont une base de vecteurs propres de J. Deux exemples : avec

$$P_1 = \begin{pmatrix} 1 & 1 & 1 & \dots & \dots & 1 & 1 \\ -1 & 0 & 0 & \dots & \dots & 0 & 1 \\ 0 & -1 & 0 & & & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & \dots & \dots & 0 & -1 & 1 \end{pmatrix}$$

et $D_1 = \mathrm{diag}(0, 0, \dots, 0, n)$, on a

$$J = P_1 D_1 P_1^{-1}$$

ou alors (et il y a bien d'autre choix possibles) avec

$$P_2 = \begin{pmatrix} 1 & 1 & 0 & \dots & \dots & \dots & 0 \\ 1 & -1 & 1 & 0 & \dots & \dots & 0 \\ \vdots & 0 & -1 & \ddots & & & \vdots \\ \vdots & \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \ddots & 0 \\ \vdots & \vdots & & & \ddots & \ddots & 1 \\ 1 & 0 & \dots & \dots & \dots & 0 & -1 \end{pmatrix}$$

et $D_2 = \mathrm{diag}(n, 0, \dots, 0, 0)$, on a

$$J = P_2 D_2 P_2^{-1}$$

994.18

Habillage du précédent

Diagonaliser la matrice suivante :

$$\begin{pmatrix} \alpha & \beta & \dots & \beta \\ \beta & \alpha & \ddots & \vdots \\ \vdots & \ddots & \ddots & \beta \\ \beta & \dots & \beta & \alpha \end{pmatrix}$$

On a

$$A = \beta J + (\alpha - \beta) I_n$$

avec J une matrice pleine de 1. On est ramené à diagonaliser J, ce qui est fait dans l'exercice précédent. On obtient, si $J = PDP^{-1}$,

$$A = P(\beta D + (\alpha - \beta) I_n) P^{-1}$$

994.19

Matrice Compagnon

Soit

$$A = \begin{pmatrix} a_1 & a_2 & \dots & \dots & a_n \\ 1 & 0 & \dots & \dots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

1. Calculer le polynôme caractéristique de A.

2. Montrer que, pour tout scalaire λ, $\mathrm{rg}(A - \lambda I_n) \geq n-1$. En déduire que A est diagonalisable si et seulement si P est scindé simple.

3. Retrouver le résultat des questions précédentes en résolvant le système

   $$AX = \lambda X$$

   et en cherchant les λ pour lesquels il admet une solution X non nulle.

On peut donc dire que tout polynôme unitaire est-il le polynôme caractéristique d'une certaine matrice..

1. Pour calculer le polynôme caractéristique, un développement par rapport à la première ligne est un peu épineux (efficace, mais il faut écrire les mineurs avec beaucoup de soin). Les autres développements (par rapport à la dernière ligne, ou par rapport à la première ou dernière colonne) marchent, il faut simplement faire une récurrence, mais ce n'est pas gênant car les cas $n = 1$, $n = 2$, $n = 3$ permettent d'être sûr de la formule (il est d'ailleurs vivement conseillé à l'oral de commencer par $n = 2$, voire $n = 3$). L'astuce consiste en l'opération

   $$C_n \longleftarrow C_n + XC_{n-1} + X^2 C_{n-2} + \cdots + X^{n-1} C_1$$

   puis développement par rapport à le dernière colonne. On trouve dans tous les cas

   $$P_A = X^n - a_1 X^{n-1} - \ldots - a_n$$

   (on vérifie que la trace et le déterminant sont là où il faut !).

2. Les $n-1$ premières colonnes de $A - \lambda I_n$ sont linéairement indépendantes. Par théorème du rang, tout sous-espace propre est de dimension ≤ 1, donc de dimension 1. Et donc la somme des dimensions des sous-espaces propres vaut n si et seulement s'il y en a n, i.e. si et seulement si P_A est scindé simple. La condition suffisante se transforme ici en condition nécessaire et suffisante.

3. La résolution du système mène au fait qu'il n'a pas de solution non nulle lorsque $\lambda^n - a_1\lambda^{n-1} - \ldots - a_n \neq 0$. Et lorsque $\lambda^n - a_1\lambda^{n-1} - \ldots - a_n = 0$, il y a une droite vectorielle de solutions, engendrée par le vecteur

$$\begin{pmatrix} \lambda^{n-1} \\ \vdots \\ \lambda \\ 1 \end{pmatrix}$$

On retrouve ainsi les résultats précédents.

994.20

Etude des matrices de rang 1

Les questions sont indépendantes.

1. Démontrer qu'une matrice A de $\mathcal{M}_{p,q}(\mathbf{K})$ est de rang 1 si et seulement si elle peut s'écrire sous la forme $X\,Y^T$ où $X \in \mathcal{M}_{p,1}(\mathbf{K})$ et $Y \in \mathcal{M}_{q,1}(\mathbf{K})$, X et Y non nuls. Si $p = q$, comment s'exprime alors sa trace en fonction de X et Y ?

Dans les questions suivantes, les matrices considérées sont carrées.

2. Donner une matrice de rang 1 diagonalisable et une matrice de rang 1 non diagonalisable.

3. On suppose ici $p = q$, A une matrice de rang 1, carrée d'ordre p. Déterminer, suivant les valeurs de la trace de A, les valeurs propres de A. Donner une condition nécessaire et suffisante portant sur la trace de A pour que A soit diagonalisable. Que peut-on dire qi A n'est pas diagonalisable ?

4. Montrer que si une matrice carrée A vérifie $\mathrm{tr}(A) = \mathrm{rg}(A) = 1$, A est un projecteur (i.e. $A^2 = A$).

Posé à l'oral des Mines

5. Soit u un endomorphisme de rang 1. Montrer que u est non diagonalisable si et seulement si $\mathrm{Im}(u) \subset \mathrm{Ker}(u)$.

Posé à l'oral des Mines

---

1. Si $A = X\,Y^T$ où $X \in \mathcal{M}_{p,1}(\mathbf{K})$ et $Y \in \mathcal{M}_{q,1}(\mathbf{K})$, X et Y non nuls, on voit que les colonnes de A sont les y_jX. Elles sont toutes dans $\mathrm{Vect}(X)$, et donc le rang de A, qui est celui de la famille de ses vecteurs colonnes, est ≤ 1. Mais $A \neq 0$ (car il y a au moins un produit x_iy_j non nul), donc $\mathrm{rg}(A) = 1$. Si réciproquement $\mathrm{rg}(A) = 1$, soit $C \in \mathcal{M}_{n,1}(\mathbf{K})$ une colonne qui engendre l'espace vectoriel engendré par les colonnes de A. Alors ces colonnes peuvent s'écrire y_1C, ...,y_qC. Et donc, en notant $X = C$ et Y comme on pense, on a $A = X\,Y^T$. Dans le cas où $p = q$, la trace vaut $\sum x_iy_i$, c'est-à-dire $X^T\,Y$, c'est-à-dire $Y^T\,X$.

2. La matrice $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ est de rang 1 et diagonalisable car diagonale. La matrice $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ est de rang 1, triangulaire donc ses valeurs propres se voient sur la diagonale : il y a 0, c'est tout. Si elle était diagonalisable, elle serait semblable à la matrice nulle, donc nulle. Ce n'est pas le cas. Bien sûr on peut construire des matrices $n \times n$ de la même manière. Plus généralement, on voit que les matrices de la base canonique sont diagonalisable si et seulement si elles sont diagonales.

3. Le rang de A vaut 1, donc

$$\dim(\mathrm{Ker}A) = \dim(E_0(A)) = n - 1$$

(théorème du rang). Donc (cours) 0 est valeur propre de multiplicité au moins $n-1$, donc le polynôme caractéristique P_A est divisible par X^{n-1}. Donc

$$P_A = X^n - \mathrm{Tr}(A)X^{n-1} = X^{n-1}\,(X - \mathrm{Tr}(A))$$

Et donc $\mathrm{Sp}(A) = \{0, \mathrm{Tr}(A)\}$. Si $\mathrm{Tr}(A) = 0$, il n'y a qu'une valeur propre, et le sous-espace propre n'est pas $\mathbf{K}^n$ tout entier, donc A n'est pas diagonalisable. Son polynôme caractéristique étant X^n, elle est nilpotente. Si $\mathrm{Tr}(A) \neq 0$, il y a deux sous-espaces propres, la somme de leurs dimensions vaut n, donc A est diagonalisable.

4. On reprend à peu près les arguments de la question précédente, pour montrer que A est diagonalisable, semblable à D telle que $d_{1,1} = 1$, $d_{i,j} = 0$ sinon. Or $D^2 = D$, donc $A^2 = A$.

5. Une remarque cruciale : tous les sous-epaces propres d'un endomorphisme sont soit égaux à son noyau, soit inclus dans son image. Cela résulte simplement du fait que, si $\lambda \neq 0$, si $u(x) = \lambda x$, alors $x = u\left(\frac{1}{\lambda}x\right)$.
   Donc, rang 1 ou pas rang 1, un endomorphisme non nul u tel que $\mathrm{Im}(u) \subset \mathrm{Ker}(u)$ est tel que

$$\bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u) \subset \mathrm{Ker}(u)$$

   et ne peut pas être diagonalisable.

   Autre remarque cruciale : $\mathrm{Im}(u)$ est toujours stable par u, c'est assez évident. Mais dans le cas où cette image est de rang 1, elle est alors nécessairement engendrée par un vecteur propre. Ce qui fait ici que si $\mathrm{Im}(u)$ n'est pas inclus dans $\mathrm{Ker}(u)$, on a

$$\mathrm{Ker}(u) \oplus \mathrm{Im}(u) = E$$

   et E est ainsi écrit comme somme de deux sous-espaces propres, il y a diagonalisabilité. Attention ! quand le rang est > 1, l'image n'a aucune raison d'être un sous-espace propre. Simplement, elle contient tous les sous-espaces propres autres que le noyau.

994.21

Réduction simultanée

1. Soit u, v deux endomorphismes d'un espace vectoriel de dimension finie, diagonalisables. Démontrer que u et v commutent si et seulement si ils sont diagonalisables dans une même base, c'est-à-dire si et seulement s'il existe une base formée de vecteurs propres à la fois pour u et pour v (on pourra utiliser la stabilité des sous-espaces propres de u par v ou réciproquement). Enoncer ce résultat en termes de matrices.

2. Soit $(u_i)_{i\in I}$ une famille d'endomorphismes diagonalisables qui commutent deux à deux. Démontrer qu'il existe une base dans laquelle les matrices de tous ces endomorphismes sont diagonales (on pourra commencer par une famille finie).

3. Dans cette question, le corps de base est $\mathbf{C}$. On suppose que u et v commutent, mais on ne les suppose plus diagonalisables. Démontrer qu'ils ont au moins un vecteur propre commun (on pourra utiliser la stabilité des sous-espaces propres de u par v ou réciproquement). Utiliser ce résultat pour démontrer que u et v sont simultanément trigonalisables.

---

1. Si u et v sont diagonalisables dans une même base, soit $\mathcal{B}$ une telle base. Deux matrices diagonales commutent, donc

$$\mathcal{M}_\mathcal{B}(v \circ u) = \mathcal{M}_\mathcal{B}(v)\mathcal{M}_\mathcal{B}(u) = \mathcal{M}_\mathcal{B}(u)\mathcal{M}_\mathcal{B}(v) = \mathcal{M}_\mathcal{B}(u \circ v)$$

   ce qui permet bien de conclure $u \circ v = v \circ u$.

   Supposons, réciproquement, $u \circ v = v \circ u$. Notons $\mathrm{Sp}(u) = \{\lambda_1, \ldots, \lambda_p\}$ (les λ_i étant deux à deux distincts), et, pour tout i entre 1 et p,
   $E_i(u) = \ker(u - \lambda_i Id)$. Comme u est diagonalisable,

$$E = \bigoplus_{i=1}^{p} E_i$$

   (on note E l'espace vectoriel sur lequel sont définis u et v). Les E_i sont stables par v (car v commute avec les $u - \lambda_i Id$). Donc v induit sur chaque E_i un endomorphisme v_i qui est, d'après le cours, diagonalisable. Soit $\mathcal{B}_i$ une base de E_i formée de vecteurs propres de v_i, donc de vecteurs propres de v. En « réunissant »

les bases $\mathcal{B}_1$,..., $\mathcal{B}_p$, on obtient une base de E (adaptée à $E = \bigoplus_{i=1}^{p} E_i$) formée de vecteurs propres pour u et pour v. Donc u et v sont simultanément diagonalisables.

En termes de matrices : soit A, B deux matrices diagonalisables ; $AB = BA$ si et seulement s'il existe $P \in \mathcal{GL}_n(\mathbf{K})$ et D, Δ diagonales telles que $A = PDP^{-1}$ et $B = P\Delta P^{-1}$

2. Montrons par récurrence $\mathcal{P}_n$: « si $u_1, \dots, u_n$ sont n endomorphismes diagonalisables qui commutent deux à deux, il existe une base dans laquelle les matrices de tous ces endomorphismes sont diagonales ».

   $\mathcal{P}_2$ a été démontrée.

   Montrons $\mathcal{P}_n \Rightarrow \mathcal{P}_{n+1}$. Soit donc $u_1, \dots, u_{n+1}$ $n+1$ endomorphismes diagonalisables qui commutent deux à deux. Soit E_λ un sous-espace propre de u_{n+1} ; E_λ est stable par $u_1, \dots, u_n$, qui induisent sur E_λ des endomorphismes $u_{\lambda,1}, \dots, u_{\lambda,n}$. Ces endomorphismes commutent car ils sont induits par des endomorphismes qui commutent. Par $\mathcal{P}_n$, il existe une base de E_λ formée de vecteur propres communs à $u_{\lambda,1}, \dots, u_{\lambda,n}$, donc de vecteurs propres communs à $u_1, \dots, u_n$. Ces vecteurs sont aussi vecteurs propres de u_{n+1}, puisqu'ils sont dans E_λ. Or $E = \bigoplus_{\lambda \in \mathrm{Sp}(u_{n+1})} E_\lambda$; en « réunissant » des bases des E_λ comme celle qu'on vient de construire, on obtient une base de E formée de vecteur propres commmuns à $u_1, \dots, u_{n+1}$. D'où $\mathcal{P}_{n+1}$. Et voilà donc pour les familles finies, par récurrence.

   Pour une famille $(u_i)_{i \in I}$ quelconque d'endomorphismes diagonalisables qui commutent, on commence par remarquer que si on considère une sous-famille finie $(u_j)_{j \in J}$, où J est une partie finie de I, ses éléments sont simultanément diagonalisables (d'après ce qui vient d'être fait). Donc toute combinaison linéaire des u_i est diagonalisable. Donc tous les éléments de $\mathrm{Vect}(u_i)_{i \in I}$ sont diagonalisables. Or ils commutent entre eux (facile). Mais cet espace est de dimension finie (comme sev de $\mathcal{L}(E)$), on peut en prendre une base et lui appliquer le cas « fini », ce qui conclut : tous les éléments de $\mathrm{Vect}(u_i)_{i \in I}$ sont simultanément diagonalisables.

3. Rédigé dans le document sur les « classiques ».

994.22

Utilisation des polynômes de matrices

Soit A et B dans $\mathcal{M}_n(\mathbf{C})$. On suppose qu'il existe $C \in \mathcal{M}_n(\mathbf{C})$ tel que $AC = CB$, C non nulle.

1. Montrer que $\forall k \in \mathbf{N} \quad A^k C = CB^k$.

2. Montrer que pour tout $P \in \mathbf{C}[X]$, $P(A)C = CP(B)$. *En général à l'oral, cette question serait posée directement, sans l'intermédiaire de la question précédente.*

3. Montrer que A et B ont au moins une valeur propre commune.

Récurrence pour la première question, combinaison linéaire pour la deuxième. On en déduit que si P est par exemple le polynôme minimal de A,

$$CP(B) = (0)$$

Ceci n'implique surtout pas que $P(B) = 0$, mais que $P(B) \notin GL_n(\mathbf{C})$. Or on scinde P (on est sur $\mathbf{C}$, c'est important) :

$$P = \prod_{i=1}^{d} (X - \alpha_i)$$

(les α_i ne sont donc pas supposés distincts : rien n'oblige A à être diagonalisable). Les α_i sont les valeurs propres de A. Alors

$$\prod_{i=1}^{d} (B - \alpha_i I_n) \notin GL_n(\mathbf{C})$$

Mais alors au moins un des $B - \alpha_i I_n$ n'est pas inversible, ce qui conclut.

994.23

Utilisation des…non, si je le dis, c'est trop facile

Soit u diagonalisable, λ une valeur propre de u, p_λ la projection sur le sous-espace propre de u associé à λ parallèlement à la somme des autres sous-espaces propres. Montrer que p_λ est un polynôme de u (on pourra raisonner matriciellement).

Dans une base adaptée à la décomposition de l'espace en somme directe des sous-espaces propres, on aura

$$A = \mathcal{M}_{\mathcal{B}}(u) = \begin{pmatrix} \lambda_1 I_{m1} & & & & \\ & \lambda_2 I_{m2} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \lambda_p I_{mp} \end{pmatrix}$$

et

$$B = \mathcal{M}_{\mathcal{B}}(p) = \begin{pmatrix} I_{m1} & & & & \\ & (0) & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & (0) \end{pmatrix}$$

où p est la projection sur le sep $E_{\lambda_1}(u)$ parallèlement à la somme des autres. Soit L_1 le polynôme qui vaut 1 en λ_1, 0 en λ_k pour $k = 1, 2, \ldots, p$ (Interpolation de Lagrange, on aura compris que c'est là l'idée essentielle de l'exercice…). On a $B = L_1(A)$ et donc $p = L_1(u)$.

994.24

Droites et plans stables

1. Soit u un endomorphisme d'un espace vectoriel complexe de dimension finie. Démontrer qu'il existe au moins une droite stable par u.

2. Soit u un endomorphisme d'un espace vectoriel réel de dimension finie. On veut démontrer qu'il existe au moins une droite ou un plan stable par u. Pour cela, on considère Q un diviseur irréductible de μ, polynôme minimal de u.

   (a) Montrer que $\mathrm{Ker}\big(Q(u)\big)$ est différent de $\{0_E\}$.

   (b) Soit x non nul dans $\mathrm{Ker}\big(Q(u)\big)$; vérifier que $\mathrm{Vect}\big(x, u(x)\big)$ est stable par u (on pourra distinguer deux cas, suivant le degré de Q). Conclure.

3. Soit A une matrice de $\mathcal{M}_n(\mathbf{R})$. On suppose que $\alpha + i\beta$ est une valeur propre complexe non réelle de A, et que $X_1 + iX_2$ est un vecteur propre associé (α et β sont des réels, X_1 et X_2 des matrices colonnes réelles, que l'on identifiera à des éléments de $\mathbf{R}^n$). Montrer que $\mathrm{Vect}(X_1, X_2)$ est stable par A, et retrouver le résultat de la question précédente.

---

1. u a au moins une valeur propre, donc au moins un vecteur propre. Or x est un vecteur propre pour u si et seulement si $\mathrm{Vect}(x)$ est stable par u.

2. (a) On écrit $\mu = QQ_1$; on a $Q(u) \circ Q_1(u) = \Theta$. Si $Q(u) \in \mathrm{GL}(E)$, alors $Q_1(u) = \Theta$, donc Q_1 annule u. Ce qui contredit la minimalité de μ. Donc $Q(u) \notin \mathrm{GL}(E)$, donc $\mathrm{Ker}\big(Q(u)\big) \neq \{0_E\}$.

(b) Si $Q = X - \alpha$, dire que $x \in \mathrm{Ker}\big(Q(u)\big)$ équivaut à dire

$$u(x) = \alpha x$$

Dans ce cas, $\mathrm{Vect}\big(x, u(x)\big) = \mathrm{Vect}(x)$ est stable par u, et c'est une droite.
Si $Q = X^2 + \alpha X + \beta$ (avec $\alpha^2 - 4\beta < 0$), dire que $x \in \mathrm{Ker}\big(Q(u)\big)$ équivaut à dire

$$u^2(x) = -\alpha u(x) - \beta x$$

et alors $\mathrm{Vect}\big(x, u(x)\big)$ est un plan stable par u.
Comme un polynôme réel irréductible est de degré 1 ou 2, qu'il n'est pas restrictif de supposer unitaire, on conclut.

3. On a $A(X_1 + iX_2) = (\alpha + i\beta)(X_1 + iX_2)$, donc $AX_1 - \alpha X_1 + \beta X_2 = i(-AX_2 + \beta X_1 + \alpha X_2)$. Une colonne dont les coefficients sont à la fois réels et imaginaires purs est nulle. Donc

$$AX_1 = \alpha X_1 - \beta X_2 \quad , \quad AX_2 = \beta X_1 + \alpha X_2$$

ce qui montre bien que $\mathrm{Vect}(X_1, X_2)$, qui est une droite ou un plan, est stable par A.

994.25

Réduction par blocs

Soit A, B deux matrices carrées d'ordre p et q respectivement. On définit par blocs la matrice

$$M = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

1. Démontrer que M est diagonalisable si et seulement si A et B le sont.
2. Démontrer que M est trigonalisable si et seulement si A et B le sont.
3. Soit C une matrice à p lignes et q colonnes. On définit

$$N = \begin{pmatrix} A & C \\ 0 & B \end{pmatrix}$$

On suppose que A et B sont diagonalisables et n'ont aucune valeur propre commune. Démontrer que N est diagonalisable, et est semblable à M

---

1. **Méthode polynomiale :** On démontre par récurrence, en utilisant le produit par blocs, que

$$\forall k \in \mathbf{N} \qquad M^k = \begin{pmatrix} A^k & 0 \\ 0 & B^k \end{pmatrix}$$

et, par combinaison linéaire de ces égalités, pour tout polynôme P :

$$P(M) = \begin{pmatrix} P(A) & 0 \\ 0 & P(B) \end{pmatrix}$$

Si M est diagonalisable, il existe P scindé à racines simples tel que $P(M) = 0$. Alors $P(A) = P(B) = 0$, donc A et B sont diagonalisables.

Réciproquement, si A et B sont diagonalisables, il existe Q_1 et Q_2 scindés à racines simples tels que $Q_1(A) = 0$ et $Q_2(B) = 0$ (remarque : on note toujours 0 la matrice nulle, quel que soit son format, ce qui est un peu abusif !). Soit $P = \mathrm{ppcm}(Q_1, Q_2)$. P est scindé simple (on peut écrire $Q_1 = \prod_{i=1}^{d}(X - a_i)^{m_i}$ et $Q_2 = \prod_{i=1}^{d}(X - a_i)^{m'_i}$ avec m_i et m'_i dans $\{0, 1\}$, et alors $P = \prod_{i=1}^{d}(X - a_i)^{\max(m_i, m'_i)}$), et $P(M) = 0$, donc M est diagonalisable.

On peut aussi raisonner par équivalences, en utilisant le polynôme minimal : on sait que

$$P(M) = 0 \Leftrightarrow P(A) = P(B) = 0$$

et donc, si $\mathcal{I}_M$ (resp. $\mathcal{I}_A$, $\mathcal{I}_B$) désigne l'idéal des polynômes annulateurs de M (resp. de A, de B), $\mathcal{I}_M = \mathcal{I}_A \cap \mathcal{I}_B$, donc, notant μ_M le polynôme annulateur de M (resp.…), $\mu_M = \text{ppcm}(\mu_A, \mu_B)$. Et donc

$$\begin{aligned} M \text{ diagonalisable} &\Leftrightarrow \mu_M \text{ scindé simple} \\ &\Leftrightarrow \mu_A \text{ et } \mu_B \text{ scindés simples} \\ &\Leftrightarrow A \text{ et } B \text{ diagonalisables} \end{aligned}$$

Méthode « vectorielle » Notons u l'endomorphisme de $\mathbf{K}^{p+q}$ canoniquement associé à M. Si $(\epsilon_1, \dots, \epsilon_{p+q})$ est la base canonique de $\mathbf{K}^{p+q}$, alors $F = \text{Vect}(\epsilon_1, \dots, \epsilon_p)$ et $G = \text{Vect}(\epsilon_{p+1}, \dots, \epsilon_{p+q})$ sont stables par u, et si on note u_F et u_G les endomorphismes induits par u sur ces sous-espaces, alors $A = \mathcal{M}_{(\epsilon_1,\dots,\epsilon_p)}(u_F)$ et $B = \mathcal{M}_{(\epsilon_{p+1},\dots,\epsilon_{p+q})}(u_G)$. D'après le cours, si u est diagonalisable, u_F et u_G le sont, donc A et B le sont. Réciproquement, si A et B sont diagonalisables, u_F et u_G le sont, il existe donc une base de F formée de vecteurs propres de u_F (donc de u) et une base de G formée de vecteurs propres de u_G (donc de u) ; en « recollant » ces deux bases, on obtient une base de $\mathbf{K}^{p+q}$ formée de vecteurs propres de u, donc u est diagonalisable, donc M l'est.

Autre méthode On peut calculer le polynôme caratéristique χ_M de M : $\chi_M = \chi_A \chi_B$, donc $\text{Sp}(M) = \text{Sp}(A) \cup \text{Sp}(B)$. Puis, pour tout $\lambda \in \text{Sp}(M)$, on essaye de trouver le sous-espace propre associé en résolvant $MX = \lambda X$. La structure par blocs de M suggère d'écrire, pour tout $X \in \mathcal{M}_{p+q,1}(\mathbf{K})$, $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$ où $X_1 \in \mathcal{M}_{p,1}(\mathbf{K})$ et $X_2 \in \mathcal{M}_{q,1}(\mathbf{K})$, et alors

$$MX = \lambda X \Leftrightarrow \begin{cases} AX_1 = \lambda X_1 \\ BX_2 = \lambda X_2 \end{cases}$$

Pour résoudre, on distingue trois cas, $\lambda \in \text{Sp}(A)$ et $\lambda \notin \text{Sp}(B)$, $\lambda \in \text{Sp}(B)$ et $\lambda \notin \text{Sp}(A)$, $\lambda \in \text{Sp}(A) \cap \text{Sp}(B)$. On y arrive (en appliquant la caractérisation de la diagonalisabilité qui utilise la somme des dimensions des sous-espaces propres), mais c'est plus long que les méthodes précédentes.

Autre idée Si A et B sont diagonalisables, on a $A = PDP^{-1}$ et $B = Q\Delta Q^{-1}$ (notations habituelles : P et Q inversibles, Δ et D diagonales). La matrice $R = \begin{pmatrix} P & (0) \\ (0) & Q \end{pmatrix}$ est inversible, d'inverse $R^{-1} = \begin{pmatrix} P^{-1} & (0) \\ (0) & Q^{-1} \end{pmatrix}$, et, en effectuant un produit par blocs, on trouve que $R^{-1}MR$ est diagonale. Donc M est diagonalisable. Cette idée ne marche pas très bien pour la réciproque.

2. Ici, les méthodes polynomiale et vectorielle fonctionnent, mais il est beaucoup plus rapide de dire que χ_M est scindé si et seulement si χ_A et χ_B le sont (car $\chi_M = \chi_A \chi_B$).

3. On a $\chi_N = \chi_A \chi_B$, donc $\text{Sp}(N) = \text{Sp}(A) \cup \text{Sp}(B)$. Soit $\lambda \in \text{Sp}(N)$, on cherche le sous-espace propre associé en résolvant $NX = \lambda X$. On écrit, si $X \in \mathcal{M}_{p+q,1}(\mathbf{K})$, $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$ où $X_1 \in \mathcal{M}_{p,1}(\mathbf{K})$ et $X_2 \in \mathcal{M}_{q,1}(\mathbf{K})$, et alors

$$NX = \lambda X \Leftrightarrow \begin{cases} AX_1 + CX_2 = \lambda X_1 \\ BX_2 = \lambda X_2 \end{cases}$$

Premier cas : $\lambda \in \text{Sp}(A)$ et, donc, $\lambda \notin \text{Sp}(B)$. Alors :

$$NX = \lambda X \Leftrightarrow \begin{cases} AX_1 = \lambda X_1 \\ X_2 = (0) \end{cases}$$

Donc, notant $E_\lambda(N)$ le sous-espace propre de N associé à λ,

$$E_\lambda(N) = \left\{ \begin{pmatrix} X_1 \\ (0) \end{pmatrix} \ ; \ X_1 \in E_\lambda(A) \right\}$$

L'application $X_1 \mapsto \begin{pmatrix} X_1 \\ (0) \end{pmatrix}$ est donc un isomorphisme de $E_\lambda(A)$ sur $E_\lambda(N)$, ces deux sous-espaces ont donc même dimension.

Deuxième cas : $\lambda \in \mathrm{Sp}(B)$ et, donc, $\lambda \notin \mathrm{Sp}(A)$

$$NX = \lambda X \;\Leftrightarrow\; \begin{cases} BX_2 = \lambda X_2 \\ X_1 = (A - \lambda I_n)^{-1} C X_2 \end{cases}$$

Donc,

$$E_\lambda(N) = \left\{ \begin{pmatrix} (A - \lambda I_n)^{-1} C X_2 \\ X_2 \end{pmatrix} \;;\; X_2 \in E_\lambda(B) \right\}$$

L'application $X_2 \mapsto \begin{pmatrix} (A - \lambda I_n)^{-1} C X_2 \\ X_2 \end{pmatrix}$ est donc un isomorphisme de $E_\lambda(B)$ sur $E_\lambda(N)$, ces deux sous-espaces ont donc même dimension.

Finalement,

$$\sum_{\lambda \in \mathrm{Sp}(N)} \dim\big(E_\lambda(N)\big) = \sum_{\lambda \in \mathrm{Sp}(A)} \dim\big(E_\lambda(A)\big) + \sum_{\lambda \in \mathrm{Sp}(B)} \dim\big(E_\lambda(B)\big) = p + q$$

d'où la diagonalisabilité de N. Elle a les mêmes valeurs propres que M, avec les même multiplicités. Comme M et N sont diagonalisables (M est « une N particulière » : avec $C = 0$), elles sont donc semblables à une même matrice diagonale (mêmes coefficients diagonaux, même nombre d'apparitions), elles sont semblables.

994.26

Ni une diagonalisation, ni une trigonalisation

Soit $A \in \mathcal{M}_2(\mathbf{R})$ n'ayant pas de valeur propre réelle. Montrer qu'il existe deux réels α et β tels que A soit semblable à la matrice

$$\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$$

On considère une valeur propre complexe $\alpha + i\beta$ (avec bien sûr α et β réels), $X_1 + iX_2$ un vecteur propre associé, X_1 et X_2 étant des colonnes réelles. Alors en identifiant (il n'est pas dur de voir qu'on a le droit) parties réelles et imaginaires, on obtient

$$AX_1 = \alpha X_1 - \beta X_2 \qquad , \qquad AX_2 = \beta X_1 + \alpha X_2$$

ce qui donne à peu près ce qu'on veut, à condition de voir que (X_1, X_2) est libre. Si X_2 est nulle, X_1 qui ne l'est pas est vecteur propre associé à la valeur propre α, à rejeter. Si $X_1 = tX_2$ avec t réel, on obtient que

$$AX_2 = (t\beta + \alpha)X_2$$

là encore contraire à l'hypothèse.

994.27

Commutant d'une matrice ou d'un endomorphisme diagonalisable

Soit E un espace vectoriel de dimension n, f un endomorphisme de E. Le commutant de f est $\mathcal{C}_f = \{g \in \mathcal{L}(E) \;;\; g \circ f = f \circ g\}$. C'est un sous-espace vectoriel de $\mathcal{L}(E)$.

1. Trouver les matrices qui commutent avec une matrice carrée diagonale à coefficients distincts.
2. Si f est diagonalisable, déterminer la dimension de $\mathcal{C}_f$ en fonction des dimensions des sous-espaces propres de f (on pourra remarquer qu'un endomorphisme qui commute avec f laisse stables les sous-espaces propres de f, et éventuellement poser le problème matriciellement).
3. Si f admet n valeurs propres distinctes, démontrer que $\mathcal{C}_f = \mathbf{K}[f]$.

La recherche d'un commutant est un sujet intéressant. Elle peut être préalable à la résolution d'une équation matricielle : par exemple, si on cherche une solution de $X^2 = M$, il est nécessaire que X commute avec M.

1. Soit D une matrice diagonale de $\mathcal{M}_n(\mathbf{K})$ à coefficients diagonaux distincts (on les notera d_i plutôt que $d_{i,i}$). Soit $A \in \mathcal{M}_n(\mathbf{K})$. Alors

$$\begin{aligned} AD = DA &\Leftrightarrow \forall (i,j) \in \{1,\dots,n\}^2 \quad (AD)_{i,j} = (DA)_{i,j} \\ &\Leftrightarrow \forall (i,j) \in \{1,\dots,n\}^2 \quad a_{i,j}d_j = d_i a_{i,j} \end{aligned}$$

   On obtient donc assez facilement (en distinguant ci-dessus les cas $i = j$ et $i \neq j$) :

$$AD = DA \qquad \Leftrightarrow (A \text{ diagonale})$$

2. Soit f diagonalisable, $\lambda_1, \dots, \lambda_p$ ses valeurs propres (distinctes) ; pour chaque i, on note E_i le sous-espace propre $E_i = \mathrm{Ker}(f - \lambda_i Id)$, et n_i la dimension de E_i (qui est aussi la multiplicité de λ_i, f étant diagonalisable).

   Si $g \in \mathcal{C}_f$, g commute avec f, donc avec $f - \lambda_i Id$, donc g laisse stable E_i (cours).

   Mais la réciproque est vraie : supposons que g laisse stable chaque E_i ; si $x \in E_k$, $(f \circ g)(x) = f\big(g(x)\big) = \lambda_k g(x)$ (car $g(x) \in E_k$) ; et $(g \circ f)(x) = g(\lambda_k x) = \lambda_k g(x)$. $g \circ f$ et $f \circ g$ coïncident sur chaque E_k, or $\bigoplus_{k=1}^{p} E_k = E$ (car f est diagonalisable), donc $f \circ g = g \circ f$.

   On a montré :

   Si f est diagonalisable, les endomorphismes qui commutent avec f sont les endomorphismes qui laissent stables les sous-espaces propres de f

   Maintenant, il reste à utiliser ceci pour calculer la dimension de $\mathcal{C}_f$.

   Une première méthode (matricielle) : Soit $\mathcal{B}$ une base adaptée à la décomposition $E = E_1 \oplus E_2 \oplus \dots \oplus E_p$ (les n_1 premiers vecteurs de $\mathcal{B}$ sont une base de E_1, les n_2 suivants une base de E_2, etc…). On vient de voir que g était dans $\mathcal{C}_f$ si et seulement si g laissait stables tous les E_k, donc si et seulement si la matrice de g dans la base $\mathcal{B}$ était diagonale par blocs de la forme :

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_p \end{pmatrix}$$

   où chaque A_k est carrée d'ordre n_k. Or l'espace F des matrices de cette forme est de dimension $n_1^2 + \dots + n_p^2$

   [on peut en donner une base, ou dire que l'application qui à $(A_1, \dots, A_p)$ associe la matrice construite ci-dessus est un isomorphisme de

   $\mathcal{M}_{n_1}(\mathbf{K}) \times \dots \times \mathcal{M}_{n_p}(\mathbf{K})$ dans F, or la dimension de

   $\mathcal{M}_{n_1}(\mathbf{K}) \times \dots \times \mathcal{M}_{n_p}(\mathbf{K})$ est $\sum_{k=1}^{p} n_k^2$].

   Comme l'application $g \mapsto \mathcal{M}_{\mathcal{B}}(g)$ est un isomorphisme de $\mathcal{L}(E)$ dans $\mathcal{M}_n(\mathbf{K})$ (et donc préserve la dimension), on conclut :

$$\boxed{\dim(\mathcal{C}_f) = \sum_{k=1}^{p} n_k^2}$$

   Une deuxième méthode : Soit G le sous-espace de $\mathcal{L}(E)$ constitué des endomorphismes qui laissent stables les E_k ; l'application de G dans $\mathcal{L}(E_1) \times \dots \times \mathcal{L}(E_p)$ qui à $g \in G$ associe $(g_1, \dots, g_p)$, où g_k désigne

l'endomorphisme induit par g sur E_k, est un isomorphisme (la linéarité est simple, il suffit de l'écrire. La bijectivité est un corollaire du résultat sur « la définition d'une application linéaire par ses restrictions aux facteurs d'une somme directe supplémentaire »). Or $\dim\big(\mathcal{L}(E_1)\times\ldots\times\mathcal{L}(E_p)\big) = \sum_{k=1}^{p}\dim(\mathcal{L}(E_k)) = \sum_{k=1}^{p} n_k^2$, ce qui donne la conclusion.

3. Un polynôme de f commute avec f. Donc $\mathbf{K}[f]\subset\mathcal{C}_f$. Mais le polynôme minimal de f a pour degré n (car il a n racines et ne peut être de degré $> n$). Donc $\dim(\mathbf{K}[f]) = n$. Or, par ce qui précède, si f est diagonalisable à valeurs propres distinctes, $\dim(\mathcal{C}_f) = n$. Ce qui conclut

---

994.28

Théorème des noyaux et cns polynomiale de diagonalisabilité

Soit A une matrice diagonalisable ; montrer que, pour tout p entier naturel, A^p est diagonalisable.
Réciproquement, soit $p\geq 2$ et $A\in\mathcal{GL}_n(\mathbf{C})$ tels que A^p soit diagonalisable. Démontrer que A est diagonalisable.
Donner un exemple montrant que ce résultat est en général faux si on ne suppose pas la matrice inversible.
Donner aussi un exemple montrant que le résultat est faux sur $\mathbf{R}$.
Si A^p est diagonale, A est-elle diagonale ?
Montrer enfin que A est diagonalisable si et seulement si A^p l'est et $\mathrm{Ker}(A^p) = \mathrm{Ker}(A)$.

De $A = PDP^{-1}$ on tire $A^p = PD^pP^{-1}$, ce qui résout la première question.
La seconde se résout en utilisant un argument polynomial : si A^p est diagonalisable, elle admet un polynôme annulateur scindé simple P. Mais $P(X^p)$ annule alors A. Est-il scindé simple ? pour le voir, on écrit

$$P(X) = \prod_{i=1}^{r}(X-a_i)$$

où les a_i sont deux à deux distincts. A quoi sert l'hypothèse d'inversibilité de A ? à pouvoir supposer les a_i non nuls (on peut par exemple choisir pour P le polynôme minimal de A^p, cette matrice n'ayant pas 0 pour valeur propre). Chaque a_i a exactement p racines p-ièmes distinctes : $\alpha_{i,1},\ldots,\alpha_{i,p}$. On a alors

$$P(X^p) = \prod_{i=1}^{r}(X^p-a_i) = \prod_{i=1}^{r}\left(\prod_{k=1}^{p}(X-\alpha_{i,k})\right)$$

qui est scindé simple (deux nombres complexes qui n'ont pas la même puissance p-ième ne peuvent pas être égaux). Et donc A est diagonalisable.
La considération de $A = \begin{pmatrix}0&1\\0&0\end{pmatrix}$ avec $p=2$ montre que la réciproque est fausse. Comme toujours sur $\mathbf{R}$, la matrice $R = \begin{pmatrix}0&-1\\1&0\end{pmatrix}$ est utile : R^2 est diagonalisable (diagonale, même) et pourtant R ne l'est pas. Et par la même occasion on voit que la réponse à la dernière question est négative.

Si A est diagonalisable, A^p l'est, elles sont semblables à des matrices diagonales (D et D^p) qui ont le même nombre de coefficients nuls sur la diagonale, donc leurs noyaux sont de même dimension, or $\mathrm{Ker}(A)\subset\mathrm{Ker}(A^p)$…Supposons réciproquement que A^p soit diagonalisable, et que $\mathrm{Ker}(A) = \mathrm{Ker}(A^p)$. On suppose ce noyau non nul, sinon le travail a déjà été fait. Et on écrit

$$P(X) = X\prod_{i=1}^{r}(X-a_i)$$

le polynôme minimal de A^p, avec les a_i deux à deux distincts, non nuls. Avec les notations ci-dessus, le polynôme

$$X^p\prod_{i=1}^{r}\left(\prod_{k=1}^{p}(X-\alpha_{i,k})\right)$$

annule A, donc, par théorème des noyaux,

$$\mathbf{K}^n = \mathrm{Ker}(A^p) \oplus \bigoplus_{i=1}^{r} \left(\bigoplus_{k=1}^{p} \mathrm{Ker}(A - \alpha_{i,k} I_n) \right)$$

Mais en remplaçant $\mathrm{Ker}(A^p)$ par $\mathrm{Ker}(A)$, on obtient que $\mathbf{K}^n$ est somme de sous-espaces propres de A (dans la somme directe, il y a peut-être des espaces réduits à $\{0_{\mathbf{K}^n}\}$, mais ce n'est pas grave, ils ne comptent pas). Donc A est diagonalisable.

994.29

Endomorphisme de $\mathcal{M}_n(\mathbf{K})$

Soit $A \in \mathcal{M}_n\mathbf{K}$, et soit $\Phi_A \in \mathcal{L}\big(\mathcal{M}_n(\mathbf{K})\big)$ définie par

$$\Phi_A(M) = AM$$

Montrer que Φ_A est diagonalisable si et seulement si A l'est.

Par récurrence on vérifie

$$\forall k \in \mathbf{N} \qquad \Phi_A^k \ : \ M \mapsto A^k M$$

Et, par combinaison linéaire de ces résultats :

$$\forall P \in \mathbf{K}[X] \qquad P(\Phi_A) \ : \ M \mapsto P(A)M$$

Donc $P(\Phi_A) = \Theta_{\mathcal{M}_n(\mathbf{K})} \ \Leftrightarrow \forall M \in \mathcal{M}_n(\mathbf{K}) \ P(A)M = (0) \ \Leftrightarrow P(A) = (0)$ Les polynômes annulateurs de Φ_A et ceux de A sont donc les mêmes. On en déduit que Φ_A est diagonalisable si et seulement si A l'est (car Φ_A admet un polynôme annulateur scindé simple si et seulement si A admet un polynôme scindé simple). Accessoirement, les valeurs propres de A et de Φ_A sont les mêmes.
Les exercices d'oral sur les endomorphismes de $\mathcal{M}_n(\mathbf{K})$ sont fréquemment traités avec des polynômes.

994.30

Pas difficile, mais à savoir !

Soit G un sous-groupe fini de $\mathcal{GL}_n(\mathbf{C})$. Démontrer que tous les éléments de G sont diagonalisables.

Tout élément est d'ordre fini, donc admet un polynôme annulateur de la forme $X^d - 1$. Or sur $\mathbf{C}$ un tel polynôme est scindé à racines simples.

994.31

Matrices « circulantes »

Soit $\mathcal{A}$ l'ensemble des matrices

$$\begin{pmatrix} a_0 & a_{n-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_2 \\ \vdots & \vdots & \dots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{pmatrix}$$

1. Montrer que $\mathcal{A}$ est une sous-algèbre commutative de $\mathcal{M}_n(\mathbf{C})$.
2. Montrer que les éléments de $\mathcal{A}$ sont simultanéments diagonalisables.

---

1. Notons

$$J = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 & 1 \\ 1 & \ddots & & & & 0 \\ 0 & \ddots & \ddots & & & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 1 & 0 \end{pmatrix}$$

Il peut être utile de voir J de la manière suivante : si j est l'endomorphisme de $\mathbf{C}^n$ canoniquement associé à J, si $(\epsilon_1, \dots, \epsilon_n)$ est la base canonique de $\mathbf{C}^n$, alors $j(\epsilon_i) = \epsilon_{i+1}$ si $1 \leq i \leq n-1$, et $j(\epsilon_n) = \epsilon_1$. Ou encore, $j(\epsilon_{\overline{a}}) = \epsilon_{\overline{a+1}}$ en définissant $\epsilon_{\overline{a}} = \epsilon_r$ où r est le reste de la division de a par n. Ces remarques permettent d'obtenir facilement J^2, J^3,...sans poser la multiplication matricielle. Et de voir que

$$\begin{pmatrix} a_0 & a_{n-1} & \dots & a_1 \\ a_1 & a_0 & \dots & a_2 \\ \vdots & \vdots & \dots & \vdots \\ a_{n-1} & a_{n-2} & \dots & a_0 \end{pmatrix} = a_0 I_n + a_1 J + \dots + a_{n-1} J^{n-1}$$

D'autre part, $J^n = I_n$. Le polynôme minimal de J est donc $X^n - 1$ (il divise $X^n - 1$, et ne peut être de degré strictement inférieur à n car le calcul précédent montre que la famille $(I_n, J, \dots, J^{n-1})$ est libre.

Finalement, $\mathcal{A} = \mathbf{C}[J]$, et donc est une sous-algèbre commutative de $\mathcal{M}_n(\mathbf{C})$.

2. J est annulée par $X^n - 1$, scindé à racines simples sur $\mathbf{C}$ (ses racines sont les n racines n-ièmes de l'unité dans $\mathbf{C}$). Donc J est diagonalisable ; il existe D diagonale et P inversible telles que

$$J = PDP^{-1}$$

Pour tous $(a_0, \dots, a_{n-1})$,

$$a_0 I_n + a_1 J + \dots + a_{n-1} J^{n-1} = P(a_0 I_n + a_1 D + \dots + a_{n-1} D^{n-1})P^{-1}$$

or $a_0 I_n + a_1 D + \dots + a_{n-1} D^{n-1}$ est diagonale. Ce qui répond à la question.

994.32

Diagonalisabilité et stabilité

Exercice instructif mais difficile.
Démontrer qu'un endomorphisme u d'un $\mathbf{C}$-espace vectoriel E est diagonalisable si et seulement si tout sous-espace stable par u admet un supplémentaire stable par u.

Supposons u diagonalisable. Soit F un sous-espace stable par u. On sait que u induit sur F un endomorphisme diagonalisable. Or les valeurs propres de u_F (induit par u sur F) sont des valeurs propres de u, et, si λ est une valeur propre de u_F, on a

$$\mathrm{Ker}(u_F - \lambda Id_F) = \mathrm{Ker}(u - \lambda Id_E) \cap F = E_\lambda(u) \cap F$$

La diagonalisabilité de u_F permet d'affirmer

$$F = \bigoplus_{\lambda \in \mathrm{Sp}(u)} (E_\lambda(u) \cap F)$$

(en autorisant dans cette somme directe des espaces réduits à $\{0\}$, pour les valeurs propres de u qui ne sont pas valeurs propres de u_F). Soit, pour tout $\lambda \in \mathrm{Sp}(u)$, G_λ un supplémentaire dans $E_\lambda(u)$ de $E_\lambda(u) \cap F$. Alors on vérifie assez facilement que $\bigoplus_{\lambda \in \mathrm{Sp}(u)} G_\lambda$ est un supplémentaire de F stable par u.
Supposons maintenant, réciproquement, que tout sous-espace stable par u admette un supplémentaire stable par u. Soit $E_\lambda(u)$ un sous-espace propre de u (il y en a car on est sur $\mathbf{C}$). Il admet un supplémentaire F stable par u. Soit u_F induit par u sur F. Si G est un sous-espace de F stable par u_F, il est stable par u, et admet donc un supplémentaire H (dans E) stable par u. On vérifie alors que $H \cap F$ est un supplémentaire de G dans F, stable par u_F. Comme u_F vérifie l'hypothèse « tout sous-espace stable par u_F admet un supplémentaire stable par u_F », on a l'idée de conclure par récurrence sur la dimension de l'espace, ce qui se fait sans problème (initialisation comme d'habitude évidente, en dimension 1, ou même en dimension 2 si on trouve la dimension 1 trop caricaturale).

994.33

X

Montrer qu'un endomorphisme u d'un espace vectoriel E de dimension n est diagonalisable si et seulement s'il

existe n hyperplans H_1,...,H_n de E stables par u et tels que

$$\bigcap_{i=1}^{n} H_i = \{0_E\}$$

Si $(e_1, \dots, e_n)$ est une base de vecteurs propres, il suffit de prendre

$$H_i = \text{Vect}(e_k)_{k \neq i}$$

Pour la réciproque, on pose

$$D_k = \bigcap_{i \neq k} H_i$$

Il est simple de montrer que D_k est stable par u. Que D_k soit une droite vient d'un résultat du programme : on sait (Grassmann) que si F est un sev et H un hyperplan, alors

$$\dim(F \cap H) \in \{\dim(F), \dim(F) - 1\}$$

et donc une intersection de p hyperplans en dimension n a une dimension $\geq n - p$ (récurrence sur p). Donc $\dim(D_k) \geq 1$, mais ≥ 2 est impossible car on aurait alors $\dim(\bigcap_{i=1}^{n} H_i) \geq 1$. Les D_k sont des droites stables. Prenons un vecteur non nul e_k dans chaque D_k. Aucun e_k ne peut être combinaison linéaire des autres, car une combinaison linéaire des e_i avec $i \neq k$ est dans H_k, et e_k n'y est pas. On tient donc bien une base de vecteurs propres.

994.34

Une trigonalisation « basique »

Soit f un endomorphisme d'un espace vectoriel de dimension 3, vérifiant $f^3 = f^2$ et $\dim(\ker(f - Id)) = 1$. Montrer qu'il existe une base dans laquelle la matrice de f est $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & \alpha \\ 0 & 0 & 0 \end{pmatrix}$ où $\alpha \in \{0, 1\}$.

$$X^3 - X^2 = X^2(X - 1)$$

n'est certes pas scindé à racines simples, mais ce polynôme annulateur donne déjà beaucoup d'indications. On peut utiliser le théorème des noyaux, tenant compte du fait que

$$X^2 \wedge (X - 1) = 1$$

et on obtient

$$E = \text{Ker}(f - Id) \bigoplus \text{Ker}(f^2)$$

Le premier sous-espace est de dimension 1 d'après l'énoncé, le second de dimension 2. Il peut être égal à $\text{Ker}(f)$, dans ce cas une base adaptée donne la forme voulue avec $\alpha = 0$. Si en revanche on a une inclusion stricte de $\text{Ker}(f)$ dans $\text{Ker}(f^2)$, on peut prendre e dans $\text{Ker}(f^2) \setminus \text{Ker}(f)$. Alors $f(e) \in \text{Ker}(f)$. Et $(f(e), e)$ est libre. On rajoute un élément de $\text{Ker}(f - Id)$ devant, on obtient ce qu'on veut avec $\alpha = 1$.

994.35

Diagonalisation d'une matrice « par blocs »

Soit A une matrice carrée d'ordre n. A quelle condition la matrice définie par blocs

$$M = \begin{pmatrix} A & A \\ 0 & A \end{pmatrix}$$

est-elle diagonalisable ?

Soit P un polynôme ; on montre (en commençant, par récurrence, par les X^k, puis pas combinaison linéaire) que

$$P(M) = \begin{pmatrix} P(A) & AP'(A) \\ 0 & P(A) \end{pmatrix}$$

Si M est diagonalisable, il existe P scindé simple tel que $P(M) = 0$, donc $P(A) = 0$ (A est donc diagonalisable) et $AP'(A) = 0$. Le polynôme minimal de A divise donc P et XP'. Il divise donc $P \wedge XP'$. Or, si P est scindé simple, $P \wedge P' = 1$. Donc $P \wedge XP' = P \wedge X$. Donc le polynôme minimal de A divise X, c'est donc X. Donc $A = 0$, la réciproque est claire.

994.36

Calculs sur les matrices nilpotentes

Soit N une matrice carrée d'ordre n nilpotente (c'est-à-dire ayant une puissance nulle).

1. Démontrer que N^n est nulle.
2. Démontrer que $I_n - N$ et $I_n + N$ sont inversibles, et calculer leurs inverses en fonction de N.
3. On écrit le développement limité de $\sqrt{1+x}$ au voisinage de 0 :

   $$\sqrt{1+x} = P_n(x) + \underset{x\to 0}{o}(x^n)$$

   où P_n est un polynôme de degré n qu'il n'est pas nécessaire d'expliciter

   En utilisant les opérations sur les développements limités, montrer que le polynôme $1 + x - P_n(x)^2$ est divisible par x^{n+1} ; déterminer alors, à l'aide de P_n et de n, une matrice M dont le carré soit égal à $I_n + N$.
4. Peut-on trouver par la même méthode une racine p-ième (matricielle, bien entendu) de $I_n + N$ ($p \geq 3$) ?

---

1. noyaux emboîtés ou Cayley-Hamilton.
2. une formule bien importante :

   $$I_n - N^n = (I_n - N)(I_n + \cdots + I_n^{n-1})$$

   et on peut remplacer N par $-N$, on obtient le résultat.
3. on a

   $$1 + x = P_n(x)^2 + \underset{x\to 0}{o}(x^n)$$

   Donc $1 + x - P_n(x)^2$ est $o_{x\to 0}(x^n)$. Mais c'est un polynôme, et un polynôme est négligeable devant x^n si et seulement si son terme de plus bas degré est de degré $\geq n + 1$. Donc

   $$1 + x - P_n(x)^2 = x^{n+1}Q(x)$$

   et en remplaçant par N :

   $$P_n(N)^2 = I_n + N$$
4. Même chose en considérant le développement limité de $(1 + x)^{1/p}$.

994.37

Une caractérisation de la nilpotence

qui ne passe pas de mode…et a d'assez nombreuses applications dans des exercices d'oral

Soit A une matrice carrée d'ordre n réelle ou complexe. Démontrer que A est nilpotente si et seulement si, pour tout k entre 1 et n, $\mathrm{tr}(A^k) = 0$.

Plusieurs méthodes possibles. On pourra par exemple utiliser une récurrence sur la dimension de la matrice et montrer que le polynôme minimal d'une matrice carrée d'ordre n vérifiant, pour tout k entre 1 et n, $\mathrm{tr}(A^k) = 0$, admet 0 pour racine.

Si A est nilpotente, elle annule un polynôme de la forme X^p, $p \geq 1$, qui est scindé. Elle est donc trigonalisable. Soit T triangulaire supérieure et P inversible telles que

$$A = PTP^{-1}$$

Les coefficients diagonaux de T sont ses valeurs propres, donc les valeurs propres de A. Or la seule valeur propres possible pour A est 0. Donc T est triangulaire supérieure « stricte », c'est aussi le cas de ses puissances ; on a donc, pour tout $k \neq 0$, $\mathrm{tr}(T^k) = 0$, donc $\mathrm{tr}(A^k) = 0$.
Pour la réciproque, supposons

$$\forall k \in \{1, \ldots, k\} \qquad \mathrm{tr}(A^k) = 0$$

Et soit $\mu = X^d + c_{d-1}X^{d-1} + \cdots + c_0$ le polynôme minimal de A ; alors

$$A^d + c_{d-1}A^{d-1} + \cdots + c_0 I_n = (0)$$

Prenons la trace ; comme $d \leq n$ (théorème de Cayley-Hamilton), on a $nc_0 = 0$, donc $c_0 = 0$ (on suppose ici que la caractéristique de $\mathbf{K}$ ne divise pas n, sinon le résultat n'est pas valable). On voit que $0 \in \mathrm{Sp}(A)$. Dans une base de $\mathbf{K}^n$ dont le premier vecteur est un élément de $\mathrm{Ker}\, A$, l'endomorphisme canoniquement associé à A a pour matrice

$$M = \begin{pmatrix} 0 & L \\ (0) & B \end{pmatrix}$$

où $B \in \mathcal{M}_{n-1}(\mathbf{K})$. Donc, par récurrence et produit par blocs,

$$M^k = \begin{pmatrix} 0 & L_k \\ (0) & B^k \end{pmatrix}$$

Et, pour tout k entre 1 et $n-1$, $\mathrm{tr}(A^k) = \mathrm{tr}(M^k) = \mathrm{tr}(B^k) = 0$. Admettant la propriété à l'ordre $n-1$, on conclut que B est nilpotente. Donc il existe p tel que $B^p = 0$, donc

$$M^p = \begin{pmatrix} 0 & L_p \\ (0) & (O) \end{pmatrix}$$

et donc $M^{p+1} = 0$, ce qui permet de dire $A^{p+1} = 0$. On conclut donc par récurrence, comme souvent très facile à initialiser (pour $n = 1$).
On peut aussi trigonaliser A, on arrive à un système de Vandermonde, mais cette méthode est un peu plus malcommode à rédiger, car il faut mettre de côté la valeur propre 0, ne garder qu'un certain nombre d'équations, etc…

994.38

Réduction « fine » d'une matrice nilpotente (vers la réduction de Jordan)

Réduire les matrices $A \in \mathcal{M}_5(\mathbf{K})$ telles que $A^3 = 0$ et $\mathrm{rg}(A) = 3$.

On constate que, X^3 étant scindé, la matrice est trigonalisable, semblable à une matrice triangulaire supérieur stricte.
Le problème est de trouver une matrice semblable à A et la plus simple possible. Soit u l'endomorphisme canoniquement associé à A (*il n'est pas nécessaire d'introduire u : on peut tout faire avec A, cela demande seulement un peu plus de précautions dans la rédaction*). Classiquement (noyaux emboîtés, à refaire si on a ce genre d'exercice à l'oral car ce n'est pas « du cours »), on a

$$\mathrm{Ker}(u^0) = \{0_E\} \subsetneq \mathrm{Ker}(u) \subsetneq \mathrm{Ker}(u^2) \subsetneq \mathrm{Ker}(u^3) = \mathbf{K}^5$$

Ceci bien sûr, à condition de vérifier que $A^2 \neq 0$. Ce qui n'est pas le plus difficile : si $A^2 = 0$, alors $\mathrm{Im}A \subset \mathrm{Ker}A$, ce qui est incompatible, pour des raisons de dimension, avec l'hypothèse $\mathrm{rg}(A) = 3$.

Comme $\dim(\mathrm{Ker}\, u) = 2$, la dimension de $\mathrm{Ker}(u^2)$ peut donc a priori être égale à 3 ou 4. On va examiner ces deux éventualités.

- Supposons $\dim\big(\mathrm{Ker}(u^2)\big) = 3$. Soit F un supplémentaire de $\mathrm{Ker}(u^2)$ dans $\mathbf{K}^5$; il est de dimension 2. Si (e, f) est une base de F, $u(e)$ et $u(f)$ sont dans $\mathrm{Ker}(u^2)$ (comme tout vecteur d'ailleurs) mais pas dans $\mathrm{Ker}(u)$ (car e et f ne sont pas dans $\mathrm{Ker}(u^2)$). Et ils forment une famille libre : si $au(e) + bu(f) = 0_{\mathbf{K}^n}$, on a $u(ae + bf) = 0_{\mathbf{K}^5}$, donc $ae + bf \in \mathrm{Ker}(u)$. Mais $F \cap \mathrm{Ker}(u) \subset F \cap \mathrm{Ker}(u^2) = \{0_{\mathbf{K}^5}\}$. Donc $ae + bf = 0_{\mathbf{K}^5}$. Et donc $a = b = 0$. On a donc une famille libre à deux éléments, qui engendre un sev de $\mathrm{Ker}(u^2)$ en somme directe avec $\mathrm{Ker}(u)$. On aurait donc $2 + 2 \leq 3$. **Ce cas ne peut pas se produire**. *On a montré plus généralement, dans l'exercice sur les noyaux emboîtés, que l'écart entre les dimensions de deux noyaux successifs était décroissant.*

- Supposons $\dim\big(\mathrm{Ker}(u^2)\big) = 4$. Si $e \notin \mathrm{Ker}(u^2)$, $u(e) \in \mathrm{Ker}(u^2) \setminus \mathrm{Ker}\, u$, soit f dans $\mathbf{K}^5$ tel que $(f, u(e))$ soit une base d'un supplémentaire de $\mathrm{Ker}\, u$ dans $\mathrm{Ker}(u^2)$ (possible pour des raisons de dimension). Alors on vérifie que $\big(u(f), u^2(e)\big)$ est une base de $\mathrm{Ker}\, u$. On vérifie aussi que $\big(u(f), f, u^2(e), u(e), e\big)$ est une base de $\mathbf{K}^5$ (former une combinaison linéaire nulle, prendre l'image par u^2, puis par u). Dans cette base, la matrice de u est

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

Il y a d'autres matrices aussi « valables » ; ici, le choix de l'ordre des vecteurs de la base est du type réduction de Jordan.

994.39

Densité de $\mathcal{GL}_n(\mathbf{K})$

1. Démontrer que $\mathcal{GL}_n(\mathbf{K})$ est dense dans $\mathcal{M}_n(\mathbf{K})$ ($\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$).

2. Démontrer que, si A et B sont deux matrices à coefficients réels ou complexes, alors

$$\mathrm{com}(AB) = \mathrm{com}(A)\,\mathrm{com}(B)$$

3. Soit A et B deux éléments de $\mathcal{M}_n(\mathbf{K})$, $\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$. Démontrer que AB et BA ont même polynôme caractéristique.

---

1. $A - \dfrac{1}{p} I_n \xrightarrow[p\to+\infty]{} A$ or au moins à partir d'un certain rang, $A - \dfrac{1}{p} I_n \in GL_n(\mathbf{K})$, car il suffit pour cela que $1/p$ ne fasse pas partie de l'ensemble, fini, des valeurs propres de A.

2. La formule $\mathrm{com}(A) = \det(A)\ \big(A^{-1}\big)^T$ donne $\mathrm{com}(AB) = \mathrm{com}(A)\,\mathrm{com}(B)$ pour A et B inversibles. Ensuite, on peut utiliser la densité précédente en deux coups (d'abord A inversible, B quelconque, puis A et B quelconques). Ou en un : soit A, B quelconques, (A_p) une suite de matrices inversibles qui converge vers A, (B_p) une suite de matrices inversibles qui converge vers B, alors (A_pB_p) converge vers AB par continuité du produit matriciel (bilinéaire sur un espace de dimension finie). Les coefficients de la comatrice de M sont polynomiaux en eux de M, donc

$$\mathrm{com}(A_pB_p) \xrightarrow[p\to+\infty]{} \mathrm{com}(AB)$$

Les mêmes arguments montrent que

$$\mathrm{com}(A_p)\,\mathrm{com}(B_p) \xrightarrow[p\to+\infty]{} \mathrm{com}(A)\,\mathrm{com}(B)$$

et on peut donc conclure.

3. Si A ou B est inversible, AB et BA sont semblables (par exemple, si A est inversible, $AB = A(BA)A^{-1}$). Donc $P_{AB} = P_{BA}$. Si A est quelconque, fixons $\lambda \in \mathbf{K}$. Alors

$$\det(\lambda I_n - A_p B) \xrightarrow[p\to+\infty]{} \det(\lambda I_n - AB)$$

(l'application $M \longmapsto \det(\lambda I_n - M)$ est polynomiale en les coefficients de M, donc continue). De même

$$\det(\lambda I_n - B A_p) \xrightarrow[p\to+\infty]{} \det(\lambda I_n - BA)$$

Or pour tout p, on a vu que $\det(\lambda I_n - BA_p) = \det(\lambda I_n - A_p B)$, ce qui conclut.

994.40

Continuité du polynôme caractéristique, pas du minimal

Soit $\mathbf{K} = \mathbf{R}$ ou $\mathbf{C}$. On fixe $n \geq 1$. Montrer que l'application

$$A \longmapsto P_A$$

(à valeurs dans $\mathbf{K}_n[X]$) est continue sur $\mathcal{M}_n(\mathbf{K})$. Montrer que l'application $A \mapsto \pi_A$ (où π_A est le polynôme minimal) n'est, elle, pas continue.

Si l'on écrit

$$P_A = Xn + a_1(A)X^{n-1} + \cdots + a_{n-1}(A)X + a_0(A)$$

alors $a_k(A)$ est polynomiale en les coefficients de A, donc chaque a_k est continue. Les applications composantes de P_A dans la base canonique étant continues, P_A l'est. En revanche, le polynôme minimal de la matrice $\begin{pmatrix} 0 & 1/p \\ 0 & 0 \end{pmatrix}$ est X^2, il ne tend pas quand $p \to +\infty$ vers le polynôme minimal de la matrice nulle.

994.41

Une densité sur $\mathbf{C}$

Montrer que l'ensemble des matrices diagonalisables est dense dans $\mathcal{M}_n(\mathbf{C})$.

Soit T une matrice trinagulaire supérieure. Notons (ce n'est qu'un exemple)

$$T_p = T + \mathrm{Diag}(1/p, 2/p, \ldots, n/p)$$

(avec des notations évidentes : la matrice diagonale dont les coefficients diagonaux sont…). Alors $T_p \xrightarrow[p\to+\infty]{} T$, et au moins à partir d'un certain rang, T_p est diagonalisable. En effet, par condition suffisante, pour qu'elle ne le soit pas, il est nécessaire d'avoir un couple (i, j) d'indices distincts tels que $\dfrac{i}{p} + T_{i,i} = \dfrac{j}{p} + T_{j,j}$, ce qui signifie $\dfrac{1}{p} = \dfrac{Tj, j - T_{i,i}}{i - j}$, et cela ne peut se produire qu'un nombre fini de fois.
Maintenant, si $M \in \mathcal{M}_n(\mathbf{C})$ est quelconque, alors il existe Q inversible et T triangulaire supérieure telles que

$$M = QTQ^{-1}$$

On considère une suite (T_p) de matrices diagonalisables qui converge vers T, alors, par continuité de $A \mapsto QAQ^{-1}$ (linéaire en dimension finie) on a

$$QT_pQ^{-1} \xrightarrow[p\to+\infty]{} QTQ^{-1}$$

ce qui achève la preuve.

994.42

Topologie et rang

Montrer que l'ensemble des matrices de rang $\geq r$ est ouvert dans $\mathcal{M}_p(\mathbf{K})$ ($\mathbf{K} = \mathbf{R}$ ou $\mathbf{K} = \mathbf{C}$). Que peut-on dire (topologiquement) de l'ensemble des matrices de rang $\leq r$? de l'ensemble des matrices de rang r ?

Pour $r = 0$, c'est évident, pour $r = p$, c'est connu (l'ensemble des matrices de rang $\geq p$ est $GL_p(\mathbf{K})$, c'est donc $\det^{-1}(\mathbf{K} \setminus \{0\})$. Notons dorénavant $\mathcal{R}$ l'ensemble des matrices de rang supérieur ou égal à r.
On doit montrer que $\mathcal{R}$ est voisinage de chacun de ses points.
a. Cas de la matrice canonique de rang r :
On commence par une matrice très simple de $\mathcal{R}$:

$$J_r = \begin{pmatrix} I_r & (0) \\ (0) & (0) \end{pmatrix}$$

notons que l'application $A \mapsto A_r$, où $A_r = (a_{i,j})_{1 \leq i,j \leq r}$ (A_r est le coin supérieur gauche $r \times r$ de A) est continue (c'est presque évident, et elle est linéaire en dimension finie). Par composition, l'application $\phi : A \mapsto \det(A_r)$ est continue. L'image réciproque $\mathcal{O}$ par ϕ de $\mathbf{K} \setminus \{0\}$ est un ouvert contenant J_r, car $\phi(J_r) = 1$. Mais $\mathcal{O} \subset \mathcal{R}$ (si on peut extraire d'une matrice une matrice carrée inversible $r \times r$, alors cette matrice est de rang $\geq r$). Finalement, $\mathcal{R}$ est voisinage de J_r.
b. « Transport » des résultats du a. vers une matrice quelconque de rang r :
Soit maintenant une matrice A de rang r. Il existe P, Q inversibles telles que $A = PJ_rQ$. L'isomorphisme $\psi : M \mapsto P^{-1}MQ^{-1}$ est continu car linéaire en dimension finie, et conserve le rang. L'image réciproque de $\mathcal{O}$ par ψ est un ouvert (car $\mathcal{O}$ est ouvert) contenant A ($\psi(A) = J_r \in \mathcal{O}$) et inclus dans $\mathcal{R}$ ($\psi^{-1} : M \mapsto PMQ$ conserve le rang). Donc $\mathcal{R}$ est un voisinage de A.
c. Cas des matrices de rang $> r$
Le même raisonnement que ci-dessus montre que, si A est de rang $p > r$, l'ensemble des matrices de rang supérieur ou égal à p est un voisinage de A, donc $\mathcal{R}$ aussi car il le contient.
En revanche, les matrices de rang r forment une partie fermée si $r = 0$, ouverte si $r = p$, ni l'un ni l'autre en général. Il est en effet facile de trouver une suite de matrices de rang r qui tend vers la matrice nulle (d'où l'aspect non fermé) et une suite de matrices de rang $> r$ qui tend vers une matrice de rang r donné (d'où l'aspect non ouvert).
On a raisonné sur des matrices carrées, mais si elles sont rectangulaires ça marche aussi bien.

994.43

Soit A une matrice carrée réelle ou complexe. Exprimer le déterminant de l'exponentielle de A à l'aide de la trace de A. *On pourra trigonaliser sur* $\mathbf{C}$.

On montre en passant par les sommes partielles, puis passage à la limite, que si T est triangulaire supérieure, les coefficients diagonaux de $\exp T$ sont les exponentielles des coefficients diagonaux de T. D'où le résultat pour une matrice triangulaire, puis pour une matrice trigonalisable. Or toute matrice réelle peut être trigonalisée sur $\mathbf{C}$, un rapport d'oral récent déplore que certains candidats n'y pensent pas.

994.44

Convergence d'une suite de puissances

Soit A une matrice carrée. On suppose que la suite (A^n) converge, soit B sa limite. Montrer que B est une matrice de projecteur.

La suite (A^{2n}) converge à la fois vers B et vers B^2.

994.45

Caractérisation topologique de la nilpotence

Si $A \in \mathcal{M}_n(\mathbf{C})$, on note

$$S(A) = \{PAP^{-1} \ ; \ P \in \mathcal{GL}_n(\mathbf{C})\} \ .$$

Montrer que A est nilpotente si et seulement si la matrice nulle est dans l'adhérence de $S(A)$.
[**Indication** Si $A = \mathcal{M}_{(e_1,\ldots,e_n)}(u)$, comment s'écrit $\mathcal{M}_{(e_1,\lambda e_2,\ldots,\lambda^{n-1}e_n)}(u)$ où $\lambda \neq 0$?]

Dans cet exercice, c'est presque l'indication qui est la chose la plus importante. Si $A = \mathcal{M}_{(e_1,\dots,e_n)}(u)$, alors, pour tout j,

$$\begin{aligned} u(\lambda^{j-1}e_j) &= \lambda^{j-1}\sum_{i=1}^{n} a_{i,j}e_i \\ &= \sum_{i=1}^{n} \lambda^{j-i}a_{i,j}\lambda^{i-1}e_i \end{aligned}$$

Donc $\mathcal{M}_{(e_1,\lambda e_2,\dots,\lambda^{n-1}e_n)}(u) = \left(\lambda^{j-i}a_{i,j}\right)_{1\leq i,j\leq n}$. On utilise généralement ce résultat pour des matrices triangulaires : si A est triangulaire supérieure, alors

$$\mathcal{M}_{(e_1,\lambda e_2,\dots,\lambda^{n-1}e_n)}(u) = \begin{pmatrix} a_{1,1} & \lambda a_{1,2} & \lambda^2 a_{1,3} & \dots & \dots & \lambda^{n-1}a_{1,n} \\ 0 & a_{2,2} & \lambda a_{2,3} & \dots & & \lambda^{n-2}a_{2,n} \\ \vdots & \ddots & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & \ddots & \ddots & \lambda a_{n-1,n} \\ 0 & \dots & \dots & \dots & 0 & a_{n,n} \end{pmatrix}$$

(chaque diagonale est multipliée par une puissance de λ qui croît jusqu'en haut à droite de la matrice). Donc, si A est triangulaire supérieure stricte, en remplaçant λ par $1/p$, on construit ainsi une suite de matrices semblables à A qui convergent vers (0). Cela montrer que la matrice nulle est dans l'adhérence de A. Si A est nilpotente, il existe T triangulaire supérieure stricte telle que

$$A = PTP^{-1}$$

Et il existe une suite (A_p) de matrices semblables à T, donc à A, qui converge vers la matrice nulle.
Supposons réciproquement que l'on ait une suite (A_p) d'éléments de $S(A)$ qui converge vers 0. Montrons que A est nilpotente en utiisant une caractérisation valable pour les matrice complexes (non pas les matrices réelles) : si $\mathrm{Sp}(A) = \{0\}$ alors A est nilpotente (pour une matrice réelle, il faut penser à dire que si $\mathrm{Sp}_{\mathbf{C}}(A) = \{0\}$ alors A est nilpotente, $\mathrm{Sp}_{\mathbf{R}}(A) = \{0\}$ ne suffit pas. Soit donc $\lambda \in \mathrm{Sp}(A) \setminus \{0\}$. On a, pour tout p, $\lambda \in \mathrm{Sp}(A_p)$, donc

$$\det(\lambda I_n - A_p) = 0$$

par continuité du déterminant, on peut prendre les limites quand $p \to +\infty$:

$$\det(\lambda I_n) = 0$$

contradiction (en fait, raisonner par l'absurde est inutile, il suffit de prendre une valeur propre et de montrer qu'elle est nécessairement nulle).

994.46

Rayon spectral

On appelle rayon spectral d'une matrice le plus grand des modules des valeurs propres de cette matrice. On note $\rho(A)$ le rayon spectral de la matrice A.

1. Soit $\|.\|$ une norme sur $\mathbf{C}^n$; on définit N sur $\mathcal{M}_n(\mathbf{C})$ par

$$N(A) = \operatorname*{Sup}_{X\neq 0} \frac{\|AX\|}{\|X\|}$$

(on identifie $\mathbf{C}^n$ à $\mathcal{M}_{n,1}(\mathbf{C})$). On admet que N est une norme, dite « subordonnée » à la norme $\|.\|$. Démontrer que

$$\rho(A) \leq N(A)$$

2. Montrer que $N(I_n) = 1$ et que, pour toutes matrices A et B,

$$N(AB) \leq N(A)N(B)$$

Une norme possédant ces deux propriétés est une « norme d'algèbre » sur $\mathcal{M}_n(\mathbf{C})$.

3. Trouver une matrice A non nulle telle que $\rho(A) = 0$. En déduire que ρ n'est pas une norme sur $\mathcal{M}_n(\mathbf{C})$.

4. Soit A une matrice carrée complexe fixée. Le but de cette partie est de démontrer que, pour tout réel strictement positif ϵ, il existe une norme d'algèbre μ sur $\mathcal{M}_n(\mathbf{C})$ telle que

$$\mu(A) \leq \rho(A) + \epsilon \ .$$

Pour cela, on utilise la trigonalisabilité de A : il existe une matrice inversible et une matrice triangulaire T telles que $A = PTP^{-1}$.

(a) Soit N_1 définie sur $\mathcal{M}_n(\mathbf{C})$ par

$$N_1(M) = \operatorname*{Max}_{1\leq j\leq n} \sum_{i=1}^{n} |a_{i,j}| \ .$$

Démontrer que N_1 est une norme sur $\mathcal{M}_n(\mathbf{C})$, subordonnée à la norme $\|.\|_1$ usuelle sur $\mathbf{C}^n$.

(b) Si Q est une matrice inversible, démontrer que l'application $M \longmapsto N_1(QMQ^{-1})$ est une norme d'algèbre sur $\mathcal{M}_n(\mathbf{C})$.

(c) Soit T une matrice triangulaire, D_t la matrice $\mathrm{Diag}(1, t, t^2, \ldots, t^{n-1})$ (on pourra remarquer qu'il s'agit de la matrice associée au changement de base vu dans la caractérisation topologique de la nilpotence). Démontrer que la norme N_1 de la matrice $D_tTD_t^{-1}$ tend, lorsque t tend vers une limite à déterminer, vers le plus grand des modules des valeurs propres de T.

(d) En déduire le résultat annoncé.

5. En utilisant les résultats précédents, démontrer que la suite de terme général A^k converge vers la matrice nulle si et seulement si $\rho(A) < 1$.

---

1. Soit λ une valeur propre de module maximal : $|\lambda| = \rho(A)$. Si $X \in \mathcal{M}_{n,1}(\mathbf{C}) \setminus \{0\}$ est tel que $AX = \lambda X$, alors

$$\frac{\|AX\|}{\|X\|} = \rho(A)$$

et donc $\rho(A) \leq \|A\|$.

2. $N(I_n) = 1$ est simple. Notons que, si $X \neq (0)$, on a

$$\|AX\| \leq N(A)\|X\|$$

et que c'est encore, facilement, vrai si $X = (0)$. Donc, pour toutes matrices A et B de $\mathcal{M}_n(\mathbf{C})$, pour tout $X \in \mathcal{M}_{n,1}(\mathbf{C})$,

$$\|(AB)X\| \leq N(A)\|BX\| \leq N(A)N(B)\|X\|$$

qui donne, si $X \neq (0)$,

$$\frac{\|(AB)X\|}{\|X\|} \leq N(A)N(B)$$

et donc, la borne supérieure d'un ensemble étant son plus petit majorant,

$$N(AB) \leq N(A)N(B)$$

3. Il suffit de prendre une matrice nilpotente non nulle.

4. (a) Soit $X \in \mathcal{M}_{n,1}(\mathbf{C})$; on peut écrire

$$\begin{aligned}\|AX\|_1 &= \sum_{i=1}^{n} |(AX)_i| \\ &= \sum_{i=1}^{n} \left| \sum_{j=1}^{n} a_{i,j}x_j \right| \\ &\leq \sum_{i=1}^{n} \left(\sum_{j=1}^{n} |a_{i,j}||x_j| \right) \\ &= \sum_{j=1}^{n} |x_j| \left(\sum_{i=1}^{n} |a_{i,j}| \right) \qquad \leq N_1(M) \sum_{j=1}^{n} |x_j| \\ &= N_1(M)\|X\|_1\end{aligned}$$

   De plus, si j_0 est tel que

$$\sum_{i=1}^{n} |a_{i,j_0}| = \operatorname*{Max}_{1\leq j\leq n} \sum_{i=1}^{n} |a_{i,j}|$$

   alors, en prenant tous les x_j nuls sauf x_{j_0}, il y a égalité dans toutes les inégalités précédentes, ce qui permet de conclure

   (b) Pas difficile.

   (c) Quand $t \to +\infty$…il suffit en effet de calculer la matrice $D_t T D_t^{-1}$.

   (d) On trigonalise A : $A = PTP^{-1}$. La norme N_1 de $D_t P^{-1} A (D_t P^{-1})^{-1}$ est $N_1(D_t T D_t^{-1}$ qui tend, vers $+\infty$, vers $\rho(T)$, mais $\rho(T) = \rho(A)$, donc si t est assez grand,

$$\mu \ : \ M \longmapsto N_1\left(D_t P^{-1} A (D_t P^{-1})^{-1}\right)$$

   convient.

5. Le sens facile : soit λ tel que $|\lambda| = \rho(A)$, $X \neq (0)$ tel que $AX = \lambda X$, alors $A^k X = \lambda^k X$ pour tout $k \geq 0$, donc, si (A^k) converge vers (0), (λ^k) aussi, donc $|\lambda| < 1$.

   Réciproquement, si $\rho(A) < 1$, on peut choisir μ norme d'algèbre telle que $\mu(A) < 1$. On a facilement par récurrence, pour tout entier naturel k,

$$\mu(A^k) \leq (\mu(A))^k$$

   et le second membre converge vers 0, donc le premier membre aussi.

994.47

Montrer que $GL_n(\mathbf{C})$ est connexe par arcs. Dénombrer le nombre de composantes connexes par arcs de $GL_n(\mathbf{R})$.

Très à la mode ces dernières années, aux ens, mais maintenant aussi aux Mines…
Quand on doit montrer qu'un ensemble est connexe par arcs, on peut penser à l'idée suivante : essayer de voir si on peut relier deux éléments par un segment. Et sinon…faire un détour !
Ici, pour $GL_n(\mathbf{C})$, on peut essayer de relier une matrice $M \in GL_n(\mathbf{C})$ quelconque à I_n. Pourquoi I_n ? parce que c'est l'élément le plus simple de $GL_n(\mathbf{C})$, donc pourquoi pas I_n.
On voit assez facilement que, s'il existe $t_0 \in [0,1]$ tel que $t_0 I_n + (1-t_0)M \notin GL_n(\mathbf{C})$, alors M a une valeur propre réelle (une valeur propre réelle négative même, sauf erreur). Pour une matrice complexe, c'est assez exceptionnel. Et l'idée est alors de dire qu'il existe $\theta \in \mathbf{R}$ tel que $t_0 e^{i\theta} I_n + (1-t_0)M \notin GL_n(\mathbf{C})$. Sinon, pour tout ϕ, M aurait au moins une valeur propre ayant pour argument ϕ, ce qui fait une infinité non dénombrable de valeurs propres…Donc M est joignable par un segment à au moins une matrice $e^{i\theta} I_n$. Or l'arc $t \mapsto e^{it\theta} I_n$ relie I_n et $e^{i\theta} I_n$, et est bien tracé sur $GL_n(\mathbf{C})$.

En revanche, $GL_n(\mathbf{R})$ ne peut être connexe par arcs, l'application det, continue, vérifierait le théorème des valeurs intermédiaires. Or $\det(GL_n(\mathbf{R})) = \mathbf{R} \setminus \{0\}$ n'est pas un intervalle, donc non : $GL_n(\mathbf{R})$ n'est pas connexe

par arcs.
Il y a mille manières de montrer que $GL_n^+(\mathbf{R}) = \{M\ ;\ \det(M) > 0\}$ est connexe par arcs. En voici une qui n'est pas très usuelle, mais qui utilise à fond le programme, donc peut plaire à un examinateur :
Première étape : Toute matrice $M \in GL_n(\mathbf{R})$ peut s'écrire sous la forme $M = QR$ avec $Q \in O(n)$ et $R \in T_n^+(\mathbf{R})$, R étant une matrice triangulaire supérieure à coefficients strictement positifs.
Démonstration : on interprète M comme matrice de passage de la base canonique à une base B, on orthonormalise B par la méthode de Schmidt. Un grand classique !
Deuxième étape $SO(n)$ est connexe par arcs.
Démonstration : on utilise le théorème de réduction des automorphismes orthogonaux, dans la matrice réduite on regroupe les éventuels -1 par paire (il y en a un nombre pair) pour en faire des blocs diagonaux

$$R_\pi = \begin{pmatrix} \cos\pi & -\sin\pi \\ \sin\pi & \cos\pi \end{pmatrix}$$

et on considère l'arc construits en remplaçant chaque bloc diagonal R_θ (rotation 2×2) par un bloc diagonal $R_{t\theta}$, ce qui conduit de I_n à n'importe quelle matrice de rotation donnée à l'avance.
Troisième étape L'ensemble des matrices triangulaires supérieures à coefficients diagonaux strictement positifs est connexe par arcs.
Démonstration : il est convexe.
Quatrième étape Si X et Y sont deux parties connexes par arcs de deux evn (pas forcément le même), alors $X \times Y$ est connexe par arcs.
Démonstration : si γ est un arc qui joint a à b dans X, si δ est un arc qui joint a' à b' dans Y, (γ, δ) est un arc qui joint (a, a') à (b, b') dans $X \times Y$. Conclusion Image d'un connexe par arcs par $(A, B) \longmapsto AB$ qui est continue car restriction d'une application bilinéaire en dimension finie, $GL_n^+(\mathbf{R})$ est connexe par arcs. Si $M \in GL_n^-(\mathbf{R})$, $\psi_M\ :\ A \mapsto AM$ est continue et vérifie $\psi_M\left(GL_n^+(\mathbf{R})\right) = GL_n^-(\mathbf{R})$ et on tient donc la deuxième composante connexe par arcs.

---

5 Algèbre bilinéaire

994.48

Un peu de géométrie euclidienne

Soit p un projecteur d'un espace euclidien E (on suppose $p \neq \Theta$). Démontrer que p est un projecteur orthogonal si et seulement si

$$\forall x \in E \qquad \|p(x)\| \leq \|x\|$$

Si p est un projecteur orthogonal, le théorème de Pythagore donne

$$\|x\|^2 = \|p(x)\|^2 + \|x - p(x)\|^2$$

qui donne bien ce qu'on veut. La réciproque est moins évidente, mais se fait si on sait bien poser le problème. On veut montrer que, si $y \in \mathrm{Ker}p$ et si $z \in \mathrm{Im}p$, alors $y \perp z$. Tout le raisonnement se place dans le plan $\mathrm{Vect}(y, z)$, il est donc conseillé de faire un dessin, sur lequel on peut voir ce qui se passe. Mais contentons-nous d'écrire

$$\forall t \in \mathbf{R} \qquad \|p(y + tz)\|^2 \leq \|y + tz\|^2$$

(prendre le carré de la norme est un réflexe quasi systématique lorsqu'on travaille avec la norme euclidienne), ou encore

$$\forall t \in \mathbf{R} \qquad t^2\|z\|^2 \leq \|y\|^2 + 2t(y|z) + t^2\|z\|^2$$

On aboutit à

$$\forall t \in \mathbf{R} \qquad \|y\|^2 + 2t(y|z) \geq 0$$

qui donne facilement $(y|z) = 0$.

994.49

Un peu de géoémtrie euclidienne

Soit, dans E préhilbertien réel, $(u_i)_{i \in I}$ une famille de vecteurs unitaires de E tels que, si $i \neq j$, $\|u_i - u_j\| = 1$. Montrer qu'une telle famille est libre. Si E est de dimension finie n, peut-on trouver une famille de n vecteurs ayant ces propriétés ?

La condition proposée équivaut à $\forall i \qquad \|u_i\| = 1$ et $\forall i \neq j \qquad (u_i|u_j) = 1/2$. Si on écrit une combinaison linéaire nulle des u_i, remarquons d'abord que pour l'indépendance il suffit de considérer une combinaison linéaire d'un nombre fini de u_i, et ça ne change rien si on suppose ce nombre fini de u_i indexé par $\{1, \ldots, p\}$. Supposons alors

$$\lambda_1 u_1 + \cdots + \lambda_p u_p = 0_E$$

et faisons le produit scalaire avec u_j ; on obtient, en multipliant par 2,

$$\sum_{i \neq j} \lambda_i + 2\lambda_j = 0$$

pour tout j. En ajoutant toutes ces égalités, on obtient $\sum_{i=1}^{p} \lambda_j = 0$. Et en retranchant cette dernière identité à toutes les équations, on tombe sur $\lambda_i = 0$ pour tout i.
Pour l'existence, c'est bien de faire une figure et de voir que ce qu'on nous demande, c'est de montrer l'existence d'un triangle équilatéral dans le plan, d'un tétraèdre régulier dans l'espace de dimension 3, etc…Or pour construire un tétraèdre régulier, a priori on construit un triangle équilatéral qui sert de base, puis on construit le vecteur suivant…donc faisons une récurrence sur n. Comme toujours on peut trouver le cas $n = 1$ un peu famélique, alors considérons $n = 2$. On part d'un vecteur unitaire u_1. Pour construire u_2, on considère e_2 unitaire orthogonal à u_1. On cherche $u_2 = \alpha u_1 + \beta e_2$. On veut $(u_1|u_2) = 1/2$, i.e. $\alpha = 1/2$. Et $\|u_2\| = 1$. C'est-à-dire $\beta = \pm\sqrt{3}/2$. On n'est pas étonné de retrouver le cosinus et le sinus de $\pi/3$.
Soit E un espace de dimension $n + 1$, euclidien bien sûr, et H un hyperplan. Par hypothèse de récurrence il existe un n-uplet $(u_1, \ldots, u_n)$ de vecteurs convenables dans E. Soit e unitaire directeur de $H^\perp$. On cherche

$$u_{n+1} = \alpha(u_1 + \ldots + u_n) + \beta e$$

(en effet, il n'y a pas de raison que la composante sur un des u_k soit différente des autres). La condition $(u_k|u_{n+1}) = 1/2$ (pour $1 \leq k \leq n$) donne

$$\alpha(1 + \frac{n-1}{2}) = \frac{1}{2}$$

c'est-à-dire $\alpha = 1/(n+1)$. Et alors on détermine β par la condition $\|u_{n+1}\| = 1$. Le peut-on ? on commence par calculer

$$\|u_1 + \cdots + u_n\|^2 = n + \frac{n(n-1)}{2}$$

(en développant le carré scalaire). La condition devient donc (e est orthogonal à $u_1 + \cdots + u_n$) :

$$\frac{1}{(n+1)^2}\left(n + \frac{n(n-1)}{2}\right) + \beta^2 = 1$$

et on arrive bien à trouver β (car la valeur trouvée pour β^2 est ≥ 0).

994.50

Reconnaissance d'une projection orthogonale

Calculer

$$\inf\left\{\int_0^{+\infty} (x^3 + ax^2 + bx)^2 e^{-2x} \ ; \ (a,b) \in \mathbf{R}^2\right\}$$

(le calcul effectif est un peu pénible, on se contentera de donner une méthode efficace !)

Qu'est-ce qui doit ici nous faire penser à un problème de projection orthogonale sur un sev de dimension finie ? déjà, le fait que l'« inf » est sur un espace vectoriel de dimension finie : notant F l'espace vectoriel des fonctions polynômes de degré ≤ 2 sur $[0, +\infty[$, la question équivaut à calculer

$$\inf\left\{\int_0^{+\infty} (x^3 - P(x))^2 e^{-2x}\ dx;\ P \in F\right\}$$

Pourrquoi ce signe $-$? parce que ça facilite la compréhension de la suite…Le carré doit ensuite faire penser à une norme euclidienne, ou plus exactement à son carré ; existe-t-il une norme euclidienne telle que, en notant

$$f\ :\ x \mapsto x^3$$

on ait

$$\|f - P\|^2 = \int_0^{+\infty} (f(x) - P(x))^2 e^{-2x}\ dx \qquad ?$$

à ce stade, les choses deviennent plus simples : on définit le produit scalaire, d'un genre classique

$$(g|h) = \int_0^{+\infty} e^{-2t} g(t)h(t)dt$$

sur l'espace des fonctions polynômes (on peut d'ailleurs se contenter des fonctions polynômes de degré ≤ 3). Le théorème de projection sur un espace de dimension finie dit que l'inf est un min, atteint en un point unique qui est P_0, projeté orthogonal de f sur F (faire un dessin). Le problème du calcul de P_0 est plus pénible techniquement. Si on note

$$P_0\ :\ x \mapsto \alpha x^2 + \beta x + \gamma$$

(on a $P_0 \in F$) alors on a $f - P_0 \in F^\perp$, ce qui se traduit par les trois équations

$$\int_0^{+\infty} e^{-2x}\left(x^3 - \alpha x^2 - \beta x - \gamma\right) dx = 0$$

$$\int_0^{+\infty} e^{-2x} x\left(x^3 - \alpha x^2 - \beta x - \gamma\right) dx = 0$$

$$\int_0^{+\infty} e^{-2x} x^2\left(x^3 - \alpha x^2 - \beta x - \gamma\right) dx = 0$$

(on écrit que $f - P_0$ est orthogonal à tous les vecteurs d'une base de F, ici la base naturelle $(1, X, X^2)$. Ce système n'est pas si difficile à écrire si on se souvient de la fonction Γ (faire un changement de variable $x = u/2$). Il est de Cramer, on en déduit (α, β, γ) et donc P_0, puis on calcule $\|f - P_0\|^2$, ou encore $\|f\|^2$ et $\|P_0\|^2$ car, en vertu du théorème de Pythagore (faire un dessin) :

$$\|f\|^2 = \|P_0\|^2 \ + \ \|f - P_0\|^2$$

994.51

Reconnaissance d'une projection orthogonale

Soit A une matrice de $\mathcal{M}_n(\mathbf{R})$, $\mathcal{S}_n$ le sous-espace de $\mathcal{M}_n(\mathbf{R})$ formé des matrices symétriques. Déterminer

$$\inf_{M \in \mathcal{S}_n} \left[\sum_{i,j} (A_{i,j} - M_{i,j})^2 \right].$$

Dans ce genre d'exercice qui se pose à l'oral, l'important est d'identifier un problème de projection orthogonale. Comme dans l'exercice précédent. Ensuite, il faut trouver la réponse aux questions suivante : dans quel espace ? ici, assez clairement, dans $\mathcal{M}_n(\mathbf{R})$. Pour quel produit scalaire ? ici, le produit scalaire canonique, qui est donné par

$$(U|V) = \sum_{i,j} U_{i,j} V_{i,j} = \mathrm{Tr}\left(U^T \ V\right)$$

Sur quel sous-espace ? sur $\mathcal{S}_n(\mathbf{R})$. Une bonne idée est de déterminer une base orthonormale de $\mathcal{S}_n(\mathbf{R})$ pour ce produit scalaire canonique. Une meilleure est de montrer que, pour ce produit scalaire canonique,

$$\mathcal{S}_n(\mathbf{R})^\perp = \mathcal{A}_n(\mathbf{R})$$

Alors le théorème de projection orthogonale dit que la borne inférieure recherchée est un minimum, atteint en un point unique :

$$M = P_{\mathcal{S}_n(\mathbf{R})}(A) = \frac{1}{2}(A + A^T)$$

et valant

$$\|\frac{1}{2}(A - A^T)\|^2 = \frac{1}{4} \sum_{(i,j) \in [\![1,n]\!]^2} (A_{i,j} - A_{j,i})^2$$

994.52

Produit scalaire sur $\mathbf{R}[X]$

Vérifier que l'égalité suivante définit un produit scalaire sur l'espace des fonctions polynômes réelles :

$$\langle P, Q \rangle \ = \ \int_{-\infty}^{+\infty} e^{-t^2} P(t) Q(t) dt$$

Démontrer qu'il existe une unique suite orthogonale de polynômes $(P_n)_{n \in \mathbf{N}}$, tels que pour tout n, P_n soit unitaire (i.e. de coefficient dominant égal à 1) de degré n.
Montrer que les P_n sont scindés à racines simples.
Démontrer qu'il existe deux suites (λ_n) et (μ_n) de réels telles que, pour tout entier naturel $n \geq 2$,

$$P_n = (X - \lambda_n) P_{n-1} - \mu_n P_{n-2}$$

(indication : décomposer XP_{n_1} dans la base des P_k).

On commence par dire que, si P et Q sont des polynômes,

$$e^{-t^2} P(t) Q(t) = \underset{t \to \pm\infty}{\mathrm{o}} \left(\frac{1}{t^2} \right)$$

ce qui assure l'existence de l'intégrale. Les propriétés du produit scalaire sont faciles à vérifier, ne pas oublier la propriété « si une fonction est continue, positive, intégrable sur un intervalle, son intégrale sur cet intervalle est nulle si et seulement si elle est nulle »
Notons ϕ_n la projection orthogonale sur $\mathbf{R}_n[X]$ (pour $n=-1$, $\phi_{-1}=\widetilde{0}$), la seule solution au problème posé est

$$\forall n \geq 0 \qquad P_n = X^n - \phi_{n-1}(X^n)$$

Soit $n \geq 2$. Supposons que P_n ait exactement d racines réelles de multiplicité impaire (et éventuellement d'autres racines de multiplicité paire qui ne nous intéressent pas), avec $d < n$. Notons $\alpha_1, \dots, \alpha_d$ ces racines. Soit $Q = \prod_{i=1}^{d}(X-\alpha_i)$ (si $d=0$, $Q=1$). Comme $d<n$, $Q \in \mathrm{Vect}(P_0, \dots P_{n-1})$. Donc $(P_n|Q)=0$. Mais cela signifie que $\int_{-\infty}^{+\infty} e^{-t^2} P_n(t)Q(t)dt = 0$. Or le polynôme P_nQ ne peut pas changer de signe (il n'a que des racines de multiplicité paire), contradiction. Donc P_n a au moins n racines de multiplicité impaire. Mais il est de degré n, il est donc scindé à racines simples.
Enfin, pour des raisons de degré et de coefficient dominant,

$$XP_{n-1} = P_n + \sum_{k=0}^{n-1} \alpha_k P_k$$

mais par orthogonalité,

$$\alpha_k \|P_k\|^2 = (XP_{n-1}|P_k)$$

Or (et attention, ce n'est pas une propriété générale du produit scalaire, c'est une propriété de ce type particulier de produit scalaire)

$$(XP_{n-1}|P_k) = (P_{n-1}|XP_k)$$

si $k < n-2$, $XP_k \in \mathbf{R}_{n-2}[X]^\perp$ et $\alpha_k = 0$. Ce qui conclut.

994.53

Déterminants de Gram : régulièrement posés à l'oral

Si $u_1, \dots, u_n$ sont n vecteurs d'un espace préhilbertien réel $\big(E, \langle .,. \rangle\big)$, on définit leur matrice de Gram, $G(u_1, \dots, u_n)$, comme la matrice carrée d'ordre n dont le coefficient en ligne i et colonne j est $\langle u_i, u_j \rangle$.

1. Démontrer que si la famille $(u_1, \dots, u_n)$ est liée alors le déterminant de sa matrice de Gram est nul (on pourra commencer par supposer que u_n s'écrit comme combinaison linéaire des autres u_i).

2. On suppose maintenant $(u_1, \dots, u_n)$ libre, et on considère $(e_1, \dots, e_n)$ une base orthonormale de $\mathrm{Vect}(u_1, \dots, u_n)$. On note :
$$A = \mathcal{M}_{(e_1,\dots,e_n)}(u_1, \dots, u_n).$$
   (a) Exprimer $G = G(u_1, \dots, u_n)$ à l'aide d'un produit faisant intervenir A et sa transposée.
   (b) Montrer que le déterminant de G est strictement positif.

3. On suppose la famille $(u_1, \dots, u_n)$ libre ; on désigne par F le s.e.v. engendré par $(u_1, \dots, u_n)$, et par x un vecteur de E. Démontrer :
$$\big[d(x,F)\big]^2 = \frac{\det\big(G(u_1, \dots, u_n, x)\big)}{\det\big(G(u_1, \dots, u_n)\big)}$$
   On pourra par exemple, dans le calcul de $\det\big(G(u_1, \dots, u_n, x)\big)$ écrire $x = (x-z) + z$, z désignant le projeté orthogonal de x sur F.

---

1. Supposons $u_n = \alpha_{n-1}u_{n-1} + \dots + \alpha_1 u_1$. Alors, pour tout $i \in [\![1, n-1]\!]$,

$$\langle u_i, u_n \rangle = \alpha_{n-1}\langle u_i, u_{n-1}\rangle + \dots + \alpha_1 \langle u_i, u_1 \rangle$$

ou encore

$$\begin{pmatrix}\langle u_1,u_n\rangle\\ \vdots\\ \langle u_n,u_n\rangle\end{pmatrix}=\alpha_{n-1}\begin{pmatrix}\langle u_1,u_{n-1}\rangle\\ \vdots\\ \langle u_n,u_{n-1}\rangle\end{pmatrix}+\cdots+\alpha_1\begin{pmatrix}\langle u_1,u_1\rangle\\ \vdots\\ \langle u_n,u_1\rangle\end{pmatrix}$$

que l'on peut lire de la manière suivante :

$$c_n=\alpha_{n-1}c_{n-1}+\ldots+\alpha_1c_1$$

où les c_k sont les colonnes de la matrice de Gram $G(u_1,\ldots,u_n)$. Les colonnes étant liées, le déterminant est nul.

Dans le cas général, il n'est pas nécessaire que u_n soit combinaison linéaire des autres u_i. Mais si la famille $(u_1,\ldots,u_n)$ est liée, au moins un des u_i s'écrit comme combinaison linéaire des autres u_k. Et on conclut de la même manière, en montrant que la colonne c_i est alors combinaison linéaire des autres.

---

2. Rappelons que, pour tout couple (i,j) de $[\![1,n]\!]^2$,

$$G_{i,j}=\langle u_i,u_j\rangle$$

et, la base $(e_1,\ldots,e_n)$ étant orthonormale,

$$A_{i,j}=\langle e_i,u_j\rangle$$

Mais d'autre part (calcul du produit scalaire dans une base orthonormale) :

$$\begin{aligned}G_{i,j}&=\sum_{k=1}^{n}\langle e_k,u_i\rangle\langle e_k,u_j\rangle\\&=\sum_{k=1}^{n}A_{k,i}A_{k,j}\\&=\left({}^tA\ A\right)_{i,j}\end{aligned}$$

et donc

$$G={}^tA\ A$$

On en déduit

$$\det(G)=(\det A)^2>0$$

($A\in GL_n(\mathbf{R})$). En fait, on peut dire plus : G est symétrique définie positive.

---

3. La dernière colonne de $G(u_1,\ldots,u_n,x)$ est

$$\begin{pmatrix}\langle u_1,x\rangle\\ \langle u_2,x\rangle\\ \vdots\\ \vdots\\ \langle u_n,x\rangle\\ \langle x,x\rangle\end{pmatrix}=\begin{pmatrix}\langle u_1,z\rangle\\ \langle u_2,z\rangle\\ \vdots\\ \vdots\\ \langle u_n,z\rangle\\ \langle x,z\rangle\end{pmatrix}+\begin{pmatrix}\langle u_1,x-z\rangle\\ \langle u_2,x-z\rangle\\ \vdots\\ \vdots\\ \langle u_n,x-z\rangle\\ \langle x,x-z\rangle\end{pmatrix}$$

où z est le projeté orthogonal de x sur $F = \text{Vect}(u_1, \dots, u_n)$. Donc :

$$\begin{pmatrix} \langle u_1, x\rangle \\ \langle u_2, x\rangle \\ \vdots \\ \vdots \\ \langle u_n, x\rangle \\ \langle x, x\rangle \end{pmatrix} = \begin{pmatrix} \langle u_1, z\rangle \\ \langle u_2, z\rangle \\ \vdots \\ \vdots \\ \langle u_n, z\rangle \\ \langle z, z\rangle \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ \langle x-z, x-z\rangle \end{pmatrix}$$

Utilisons la linéarité du déterminant par rapport à sa dernière colonne. On obtient, notant $g(\dots) = \det(G(\dots))$:

$$g(u_1, \dots, u_n, x) = g(u_1, \dots, u_n, z) + \begin{vmatrix} \langle u_1, u_1\rangle & \dots & \dots & \langle u_1, u_n\rangle & 0 \\ \vdots & & & \vdots & \vdots \\ \vdots & & & \vdots & \vdots \\ \langle u_n, u_1\rangle & \dots & \dots & \langle u_n, u_n\rangle & 0 \\ \langle z, u_1\rangle & \dots & \dots & \langle z, u_n\rangle & \|x-z\|^2 \end{vmatrix}$$

(on réutilise le fait que $\langle u_k, x\rangle = \langle u_k, z\rangle + \langle u_k, x-z\rangle = \langle u_k, z\rangle$). On développe alors par rapport à la dernière colonne le dernier déterminant ; tenant compte de la nullité de $g(u_1, \dots, u_n, z)$ (famille liée), on conclut :

$$g(u_1, \dots, u_n, x) = \|x-z\|^2 \; g(u_1, \dots, u_n)$$

994.54

Décomposition QR

1. En utilisant le procédé d'orthonormalisation de Schmidt, démontrer que, si A est une matrice inversible carrée d'ordre n à coefficients réels, il existe une matrice Q orthogonale d'ordre n et une matrice R triangulaire supérieure à coefficients réels telle que

   $$A = QR$$

   (on interprétera A comme matrice de passage de la base canonique à la base des vecteurs colonnes, et on orthonormalisera cette dernière).

2. Expliquer l'intérêt de la décomposition $A = QR$ pour la résolution d'un système $AX = B$.

3. Y-a-t-il unicité de la décomposition ?

4. On veut montrer l'inégalité de Hadamard : si M est une matrice carrée réelle, $(c_1, \dots, c_n)$ la famille de ses vecteurs colonnes, $||.||$ la norme euclidienne canonique sur $\mathbf{R}^n$, alors

   $$|\det M| \leq ||c_1|| \dots ||c_n||$$

   (a) Montrer l'inégalité lorsque M n'est pas inversible.

   (b) On suppose M inversible, on l'écrit $M = QR$ où Q est une matrice orthogonale et R une matrice triangulaire supérieure. Si $(\gamma 1, \dots, \gamma_n)$ est la famille des vecteurs colonnes de R, si q est l'endomorphisme de $\mathbf{R}^n$ canoniquement associé à Q, exprimer γ_k à l'aide de q et de c_k

   (c) Conclure

   (d) Peut-il y avoir égalité dans l'inégalité de Hadamard ?

1. Si $(c_1, \dots, c_n)$ est la famille des vecteurs colonnes de A, A est la matrice de passage de la base canonique $\mathcal{BC}$ de $\mathbf{R}^n$ à la base $\mathcal{C} = (c_1, \dots, c_n)$. On munit $\mathbf{R}^n$ du produit scalaire canonique (pour lequel, donc, $\mathcal{BC}$ est orthonormale). Soit $\mathcal{B}$ une base orthonormale de $\mathbf{R}^n$ obtenue à partir de $\mathcal{C}$ par le procédé de Schmidt. On a alors, avec des notations habituelles :

$$\mathrm{P}_{\mathcal{BC}}^{\mathcal{C}} = \mathrm{P}_{\mathcal{BC}}^{\mathcal{B}}\ \mathrm{P}_{\mathcal{B}}^{\mathcal{C}}$$

Mais $\mathrm{P}_{\mathcal{BC}}^{\mathcal{B}}$, matrice de passage d'une base orthonormale à une bas orthonormale, est orthogonale. Et l'algorithme de Schmidt garantit que, pour tout k,

$$c_k \in \mathrm{Vect}(e_1, \dots, e_k)$$

où l'on note $\mathcal{B} = (e_1, \dots, e_n)$ (on a en effet, pour tout k,

$$\mathrm{Vect}(e_1, \dots, e_k) = \mathrm{Vect}(c_1, \dots, c_k) \quad)$$

et donc…ça marche.

2. On écrit le système équivalent $RX = Q^T B$, c'est un système triangulaire.

3. Visiblement non, vu le (petit) choix dans l'algorithme de Schmidt. Mais allons plus loin : à quelle condition a-t-on

$$QR = Q'R'$$

où Q et Q' sont orthogonales, R et R' triangulaires supérieures inversibles ?

On remarque que l'égalité étudiée équivaut à

$$Q'^{-1}Q = R'R^{-1}$$

où le premier membre est une matrice orthogonale, le second une matrice triangulaire supérieure. Le problème est donc : quelles sont les matrices à la fois orthogonales et triangulaires supérieures ? construisons une telle matrice : son premier vecteur colonne, unitaire et dont seule la première composante est possiblement non nulle, est donc $(\pm 1, 0, \dots, 0)$. Son deuxième vecteur colonne est orthogonal au premier, sa première composante est donc nulle. Donc seule sa deuxième composante est non nulle, et vaut nécessairement ± 1 car il est unitaire. Ainsi de suite…Bref,

$$\mathcal{O}_n(\mathbf{R}) \cap \mathcal{T}_n^+(\mathbf{R}) = \{D_\epsilon\ ;\ \epsilon \in \{-1, 1\}^n\}$$

où, si $\epsilon = (\epsilon_1, \dots, \epsilon_n)$, $D_\epsilon = \mathrm{diag}(\epsilon_1, \dots, \epsilon_n)$. On conclut que

$$QR = Q'R' \ \Leftrightarrow \exists \epsilon \in \{-1, 1\}^n \quad R' = D_\epsilon R \text{ et } Q' = QD_\epsilon$$

(on s'est servi du fait que D_ϵ était sa propre inverse). Grosso modo, cela signifie que dans deux décompositions QR, au signe près on retrouve les mêmes coefficients.

4. (a) Le premier membre est nul, le second membre est positif.
   (b) $c_k = q(\gamma_k)$
   (c) Donc, pour tout k, $\|c_k\| = \|\gamma_k\|$. Or, pour tout k,

$$\|\gamma_k\| = \sqrt{\sum_{i=1}^{k} R_{i,k}^2} \geq |R_{k,k}|$$

Il suffit alors de remarquer que

$$\prod_{k=1}^{n} |R_{k,k}| = |\det(R)| = |\det(M)|$$

   (d) Oui. Si et seulement si la matrice R est diagonale, d'après ce qui précède. Et donc si et seulement si les colonnes de M forment une famille orthogonale.

994.55

Matrices symétriques positives, définies positives

C'est « du cours », mais il faut être à l'aise avec la démonstration

1. On dit qu'une matrice symétrique $M \in \mathcal{S}_n(\mathbf{R})$ est positive lorsque

$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T\ M\ X\ \geq\ 0$$

On note $\mathcal{S}_n^+(\mathbf{R})$ l'ensemble des matrices symétriques positives.

Montrer qu'une matrice symétrique est positive si et seulement si toutes ses valeurs propres sont dans $\mathbf{R}^+$.

2. Montrer que tous les coefficients diagonaux d'une matrice symétrique positive sont positifs. Donner un exemple de matrice symétrique positive dont tous les coefficients sont strictement négatifs sauf les coefficients diagonaux.

3. On dit qu'une matrice symétrique $M \in \mathcal{S}_n(\mathbf{R})$ est définie positive lorsque

$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \setminus \{(0)\} \qquad X^{\mathrm{T}}\ M\ X\ >\ 0$$

On note $\mathcal{S}_n^{++}(\mathbf{R})$ l'ensemble des matrices symétriques positives.

Caractériser par leur spectre les éléments de $\mathcal{S}_n^{++}(\mathbf{R})$ parmi les éléments de $\mathcal{S}_n(\mathbf{R})$.

4. Soit $(E, (.|.))$ un espace euclidien, u un endomorphisme symétrique de E. On dit que u est symétrique positif lorsque

$$\forall x \in E \qquad (x|u(x)) \geq 0$$

Montrer qu'un endomorphisme symétrique u est positif si et seulement si

$\mathrm{Sp}(u) \subset \mathbf{R}^+$.

5. Définir et caractériser un endomorphisme symétrique « défini positif »

---

1. Soit $M \in \mathcal{S}_n(\mathbf{R})$. Par théorème spectral, il existe $P \in \mathcal{O}_n(\mathbf{R})$ et D diagonale dans $\mathcal{M}_n(\mathbf{R})$ telles que

$$M = PDP^{-1} = PDP^T$$

Alors

$$\begin{aligned}\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T\ M\ X\ \geq\ 0 &\Leftrightarrow \forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T\ PDP^T\ X\ \geq\ 0\\ &\Leftrightarrow \forall Y \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad Y^T DY\ \geq\ 0\end{aligned}$$

car l'application $X \mapsto P^T X$ est une bijection de $\mathcal{M}_{n,1}(\mathbf{R})$ dans lui-même (un automorphisme, même), de réciproque $Y \mapsto PY$. Or, avec des notations « évidentes »,

$$Y^T DY = \sum_{i=1}^{n} d_i y_i^2$$

et $\mathrm{Sp}(M) = \{d_i\ ;\ 1 \leq i \leq n\}$. Si tous les d_i sont positifs, alors $\forall Y \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad Y^T DY\ \geq\ 0$, et réciproquement, en prenant les Y dans la base canonique de $\mathcal{M}_{n,1}(\mathbf{R})$.

2. Soit $S \in \mathcal{S}_n(\mathbf{R})$ positive. Si les E_i sont les vecteurs de la base canonique de $\mathcal{M}_{n,1}(\mathbf{R})$, pour tout i on a

$$E_i^T S E_i = S_{i,i}$$

d'où la réponse à la première question. Rappelons d'autre part que, si J est une matrice $n \times n$ dont tous les coefficients sont égaux à 1, les valeurs propres de J (qui est symétrique réelle, c'est la manière la plus simple de dire qu'elle est daigonalisable) sont 0 et n. On en déduit donc, si $\alpha \in \mathbf{R}$, que les valeurs propres de $I_n - \alpha J$ sont 1 et $1 - n\alpha$. Il suffit de choisir $\alpha = 1/n$ pour répondre à la deuxième question.

3. Les calculs de la première question montrent que les éléments de $\mathcal{S}_n^{++}(\mathbf{R})$ sont les éléments de $\mathcal{S}_n(\mathbf{R})$ dont les valeurs propres sont toutes strictement positives.

4. Le théorème spectral donne l'existence d'une base orthonormale de vecteurs propres de u. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une telle base. Pour tout i, $u(e_i) = \lambda_i e_i$, et $\mathrm{Sp}(u) = \{\lambda_1, \dots, \lambda_n\}$. Soit $x \in E$. Décomposons x dans la base $\mathcal{B}$: $x = \sum_{i=1}^{n} x_i e_i$. Alors

$$(x|u(x)) = \left(\sum_{i=1}^{n} x_i e_i | \sum_{i=1}^{n} \lambda_i x_i e_i\right) = \sum_{i=1}^{n} \lambda_i x_i^2$$

5. Soit $(E, (.|.))$ un espace euclidien, u un endomorphisme symétrique de E. On dit que u est symétrique défini positif lorsque

$$\forall x \in E \setminus \{0_E\} \qquad (x|u(x)) > 0$$

Un endomorphisme symétrique u est défini positif si et seulement si $\mathrm{Sp}(u) \subset \mathbf{R}_*^+$.

994.56

Formule variationnelle

Là aussi, si on ne savait pas faire à l'oral, la note serait infinitésimale…
Soit u un endomorphisme symétrique d'un espace vectoriel euclidien E. Montrer que l'application

$$x \longmapsto \frac{(x|u(x))}{\|x\|^2}$$

atteint sur $E \setminus \{0_E\}$ un minimum et un maximum, les exprimer en fonction des valeurs propres de u.
Traduire ce résultat matriciellement.

Par théorème spectral, on fixe une base orthonormale $(e_1, \dots, e_n)$ de E composée de vecteurs propres de u : $u(e_i) = \lambda_i$. Il n'est pas restrictif de supposer $\lambda_1 \leq \ldots \leq \lambda_n$. Et alors, si $x = x_1 e_1 + \cdots + x_n e_n$, on a

$$(x|u(x)) = \sum_{i=1}^{n} \lambda_i x_i^2$$

donc

$$\lambda_1 \|x\|^2 \leq (x|u(x)) \leq \lambda_n \|x\|^2$$

l'inégalité de gauche est une égalité si et seulement si $x \in \mathrm{Ker}(u - \lambda_1 \mathrm{Id}_E$, l'inégalité de droite est une égalité si et seulement si $x \in \mathrm{Ker}(u - \lambda_n \mathrm{Id}_E$. Donc il y a un minimum et un maximum, qui sont $\mathrm{Min}\,(\mathrm{Sp}(A))$ et $\mathrm{Max}\,(\mathrm{Sp}(A))$.
Pour les matrices symétriques réelles, même chose en considérant le quotient

$$\frac{X^T\ A\ X}{X^T\ X}$$

X parcourant $\mathcal{M}_{n,1}(\mathbf{R}) \setminus \{0\}$. *Cet hyper-classique a une belle extension, le lemme de Courant-Fischer, donné dans les exercices de révision pour l'écrit.*

994.57

Matrices orthogonales

Soit A une matrice orthogonale carrée d'ordre n. Soit U la colonne $\begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$. Exprimer $\sum_{i,j} a_{i,j}$ à l'aide de U et de A. En déduire :

$$\left|\sum_{i,j} a_{i,j}\right| \leq n\ .$$

Y-a-t-il des cas d'égalité ?

Savoir que AU est une matrice colonne dont les coefficients sont les sommes des coefficients de chaque ligne de A aide à trouver

$$^tU\ A\ U = \sum_{i,j} a_{i,j}$$

Mais considérons le produit scalaire canonique sur $\mathcal{M}_{n,1}(\mathbf{R})$; on peut alors interpréter

$$^tU\ A\ U = \langle U, AU\rangle$$

Et l'inégalité de Cauchy-Schwarz donne

$$|\langle U, AU\rangle| \ \leq\ \|U\|\ \|AU\|$$

Mais A, orthogonale, conserve la norme euclidienne. Comme $\|U\| = \sqrt{n}$, l'inégalité est démontrée (assez facile avec l'indication, mais sans ladite indication ce le serait nettement moins). L'égalité dans Cauchy-Schwarz a lieu si et seulement si AU et U sont liés, soit si et seulement si $AU = \pm U$ (A conserve la norme). Soit si et seulement si la somme des coefficients de chaque ligne vaut 1 (respectivement -1).

994.58

Étude d'une suite d'endomorphismes

Soit E un espace euclidien, u une isométrie vectorielle de E, on définit $v = Id_E - u$.

1. Démontrer que $\ker v = (\operatorname{im} v)^\perp$.
2. On définit
$$P_n = \frac{1}{n}\sum_{k=0}^{n-1} u^k.$$
Démontrer que $\big(P_n(x)\big)_{n\in\mathbf{N}}$ converge, pour tout élément x de E, vers la projection orthogonale de x sur Ker$v$.

---

1. Considérons $x \in \ker v$, $y \in \operatorname{im} v$. Il existe z tel que $y = v(z)$. Et
$$(x|y) = (x|v(z)) = (x|z) - (x|u(z))$$
Mais $x = u(x)$, donc $(x|u(z)) = (u(x)|u(z))$ et u conserve le produit scalaire ; on conclut bien que
$$(x|y) = 0$$
Il en ressort que $\ker v \perp \operatorname{im} v$. Donc $\ker v \subset (\operatorname{im} v)^\perp$. L'égalité résulte alors de l'égalité des dimensions, elle-même conséquence du théorème du rang.
2. Soit $x \in E$, on peut écrire $x = y + z$ où $y \in$ Ker$v$, c'est-à-dire $y = u(y)$, et $z \in (\text{Ker}v)^\perp = \text{im}(v)$, ce qui signifie qu'il existe $t \in E$ tel que $z = v(t) = t - u(t)$. On a alors
$$P_n(x) = \frac{1}{n}\sum_{k=0}^{n-1} u^k(y)\ +\ \frac{1}{n}\sum_{k=0}^{n-1} u^k(z)$$
Mais pour tout k on a $u^k(y) = y$ (récurrence sur k), et $u^k(z) = u^k(t) - u^{k+1}(t)$ ce qui fait que la deuxième somme est télescopique. Donc
$$P_n(x) = y + \frac{1}{n}\big(t - u^n(t)\big)$$
Mais par orthogonalité de u, on a $\|u^n(t)\| = \|t\|$, donc
$$P_n(x) \xrightarrow[n\to+\infty]{} y$$
ce qui conclut.

994.59

Produit scalaire canonique sur $\mathcal{M}_n(\mathbf{R})$

Encore « presque du cours »

1. Démontrer que l'application $(A, B) \mapsto \mathrm{Tr}(A^{\mathrm{T}}\ B)$ est un produit scalaire sur $\mathcal{M}_n(\mathbf{R})$.
2. On note $||.||$ la norme associée. Calculer la norme d'une matrice en fonction de ses coefficients.
3. $||.||$ est-elle une norme subordonnée ?
4. Si A est une matrice symétrique, écrire $||A||$ en fonction des valeurs propres de A.
5. Quel est, pour ce produit scalaire, l'orthogonal de l'espace des matrices symétriques ?

---

1. Première méthode : Il n'est guère douteux que l'on définisse ainsi une forme bilinéaire symétrique (la symétrie vient du fait que la trace de ${}^tAB$ est aussi celle de sa transposée, ${}^tBA$). Est-elle définie positive ? il suffit pour le voir de calculer

$$tr({}^tAA) = \sum_{i=1}^{n}({}^tAA)_{i,i} = \sum_{i=1}^{n}(\sum_{k=1}^{n} a_{k,i}^2)$$

qui est bien positif et n'est nul que si et seulement si A l'est.

Deuxième méthode : Calculons, directement,

$$tr({}^tAB) = \sum_{j=1}^{n}({}^tAB)_{j,j} = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} a_{i,j}b_{i,j}\Big) = \sum_{1\leq i,j\leq n} a_{i,j}b_{i,j}$$

On voit que c'est bien un produit scalaire, et qu'il mérite le qualificatif de « canonique » car la base canonique est orthonormale pour ce produit scalaire.

2. $$\|A\| = \sqrt{\sum_{1\leq i,j\leq n} a_{i,j}^2}$$

3. Non, car $\|I_n\| = \sqrt{n} \neq 1$.

4. On peut écrire $A = PDP^{-1} = P\ D\ {}^tP$ où P est une matrice orthogonale et D une matrice diagonale.
On a $\|A\|^2 = \mathrm{tr}({}^tA\ A) = \mathrm{tr}(P\ {}^tD\ {}^tP\ P\ D\ {}^tP) \ = \ \mathrm{tr}(P\ D^2\ P^{-1}) = \ \mathrm{tr}(D^2)$
et donc
$$\|A\| = \sqrt{\sum_{i=1}^{n}\lambda_i^2}$$
si $\lambda_1, \ldots \lambda_n$ sont les valeurs propres de A, répétées autant de fois que leur multiplicité.

5. Si B est antisymétrique et A symétrique, on a
$$\mathrm{tr}({}^tAB) = \mathrm{tr}(AB) = \mathrm{tr}\big({}^t(AB)\big) = \mathrm{tr}\big({}^tB\ {}^tA\big) = \mathrm{tr}(-BA) = -\mathrm{tr}(AB)$$
et un nombre égal à son opposé est nul. Donc $\mathcal{S}_n(\mathbf{R})$ et $\mathcal{A}_n(\mathbf{R})$ sont orthogonaux. Donc $\mathcal{A}_n(\mathbf{R}) \subset \big(\mathcal{S}_n(\mathbf{R})\big)^{\perp}$. Et, ces deux sous-espaces ayant même dimension, ils sont égaux.
Autre argument : la somme $\mathcal{A}_n(\mathbf{R}) \oplus \mathcal{S}_n(\mathbf{R})$ est orthogonale donc directe, or toute matrice M de $\mathcal{M}_n(\mathbf{R})$ s'écrit $M = \dfrac{1}{2}(M + {}^tM) + \dfrac{1}{2}(M - {}^tM)$ somme d'une matrice symétrique et d'une matrice antisymétrique, donc $\mathcal{A}_n(\mathbf{R})$ et $\mathcal{S}_n(\mathbf{R})$ sont supplémentaires orthogonaux.

994.60

racine carrée d'une matrice symétrique positive, décomposition polaire

La décomposition polaire d'un endomorphisme est analogue à la décomposition trigonométrique d'un nombre complexe (forme module-argument). Classique, et utile dans un grand nombre d'exercices.

On dit qu'une matrice symétrique (respectivement un endomorphisme autoadjoint) est positive (respectivement positif) lorsque toutes ses valeurs propres sont positive.

Soit E un espace euclidien de dimension n.

1. Si A est une matrice symétrique positive, montrer qu'il existe B symétrique positive telle que
$$B^2 = A$$
Que dire de B si A est supposée définie positive, i.e. si toutes ses valeurs propres sont strictement positives ?

2. Soit u un endomorphisme symétrique positif.
   (a) Etablir l'existence d'un endomorphisme h symétrique positif telle que $h^2 = u$.
   (b) En utilisant le fait que, si $h^2 = u$, h et u commutent, démontrer l'unicité de h. Que peut-on dire de h si u est défini positif ?

3. Montrer qu'une matrice $M \in \mathcal{S}_n(\mathbf{R})$ est symétrique positive si et seulement si
$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T\ M\ X \geq 0$$
En déduire que l'ensemble des matrices symétriques positives est fermé dans $\mathcal{M}_n(\mathbf{R})$.
Montrer que $M \in \mathcal{S}_n(\mathbf{R})$ est définie positive si et seulement si
$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \setminus \{(0)\} \qquad X^T\ M\ X > 0$$

4. Soit $A \in GL_n(\mathbf{R})$.
   (a) Vérifier que $A^T\ A$ est une matrice symétrique définie positive.
   (b) Démontrer qu'il existe un couple (Q, S) de matrices, la première orthogonale et la seconde symétrique définie positive, telles que $A = QS$.

5. Montrer que $GL_n(\mathbf{R})$ est dense dans $\mathcal{M}_n(\mathbf{R})$.

6. Montrer que $O(n)$ est compact.

7. Soit $A \in M_n(\mathbf{R})$. Démontrer, en utilisant les questions précédentes, qu'il existe un couple (Q, S) de matrices, la première orthogonale et la seconde symétrique positive, telles que $A = QS$.

---

1. Par théorème spectral, il existe $P \in \mathcal{O}(n)$ et $D \in \mathcal{D}_n(\mathbf{R})$ (i.e. diagonale) telles que
$$A = PDP^T = PDP^{-1}$$
Et $D = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$ (notation non officielle...) où les λ_i sont les valeurs propres de$D$, donc de A. Donc les λ_i sont positifs, et, en posant $\Delta = \mathrm{diag}(\sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$ et $B = P\Delta P^{-1} = P\Delta P^T$ on obtient une matrice symétrique (deuxième forme) et à valeurs propres positives (première forme) telle que $B^2 = A$.
Si A est définie positive, elle est dans $GL_n(\mathbf{R})$ (elle n'a pas 0 pour valeur propre), donc B aussi (prendre le déterminant, ou encore dire que $A^{-1}BB = I_n$), donc B, étant déjà positive, est définie positive.

2. (a) On pourrait bien sûr passer par les matrices et utiliser la question précédente. Mais plutôt : soit, par le théorème spectral, $(e_1, \dots, e_n)$ une base orthonormale de vecteurs propres de u :

$$\forall i \in \{1, \dots, n\} \qquad u(e_i) = \lambda_i e_i$$

où les λ_i sont positifs. Soit v l'unique endomorphisme tel que

$$\forall i \in \{1, \dots, n\} \qquad v(e_i) = \sqrt{\lambda_i} e_i$$

alors $v^2 = u$ (car v^2 et u coïncident sur une base), et v est symétrique car sa matrice dans la base orthonormale $\mathcal{B}$ l'est (elle est en effet diagonale). Les valeurs propres de v sont les $\sqrt{\lambda_i}$ donc sont positives.

(b) $hu = uh = h^3$, d'où la commutation. Donc les sous-espaces propres de u sont stables par h. Soit $E_\lambda(u)$ l'un d'eux. Sur $E_\lambda(u)$, h induit un endomorphisme symétrique donc diagonalisable que l'on note h_λ. Si μ est une valeur propre de h_λ, alors $\mu \geq 0$, et d'autre part μ^2 est valeur propre de $h_\lambda^2 = \lambda Id_{E_\lambda(u)}$ (en effet $\lambda Id_{E_\lambda(u)}$ est l'endomorphisme induit par u sur $E_\lambda(u)$). Donc $\mu = \sqrt{\lambda}$. Et donc (un endomorphisme qui n'a qu'une valeur propre est une homothétie) $h_\lambda = \sqrt{\lambda} Id_{E_\lambda(u)}$. D'où l'unicité de h (car

$$E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda(u)$$

et un endomorphisme de E est donc défini de manière unique par ses restrictions aux $E_\lambda(u)$).

3. Tout a été fait dans un précédent exercice sauf la question topologique. Si $X \in \mathcal{M}_{n,1}(\mathbf{R})$, $\phi_X : M \mapsto X^T M X$ est continue car linéaire avec un espace de départ $(\mathcal{M}_n(\mathbf{R}))$ de dimension finie. De même $\psi : M \mapsto M - M^T$. Or l'ensemble des matrices positives est

$$\psi^{-1}(\{(0)\}) \cap \bigcap_{X \in \mathcal{M}_{n,1}(\mathbf{R})} \phi_X^{-1}(\{0\})$$

et une intersection de fermés est un fermé.

4. (a) C'est assez facilement une matrice symétrique. Et, si $X \in \mathcal{M}_{n,1}(\mathbf{R})$,

$$X^T(A^T A)X = Y^T Y \qquad \text{où } Y = AX$$

Or, si $X \neq (0)$, $AX \neq (0)$, or si $Y \neq (0)$, $Y^T Y > 0$.

(b) En utilisant les questions précédentes, il existe S symétrique définie positive telle que

$$S^2 = A^T A$$

Posons $Q = AS^{-1}$; on calcule

$$Q^T Q = (S^{-1})^T A^T A S^{-1} = S^{-1} S^2 S^{-1} = I_n$$

Donc Q est orthogonale.

5. Si $M \in \mathcal{M}_n(\mathbf{R})$,

$$M - \frac{1}{p} I_n \xrightarrow[p \to +\infty]{} M$$

Or, au moins à partir d'un certain rang, $1/p \notin \mathrm{Sp}(M)$.

6. Fermé et borné…n'oublions surtout pas : d'un espace vectoriel de dimension finie.

7. Soit (A_p) une suite d'éléments de $GL_n(\mathbf{R})$ qui converge vers A. Pour tout $p \in \mathbf{N}$, il existe Q_p orthogonale et S_p symétrique positive telles que

$$A_p = Q_p S_p$$

On extrait de (Q_p), par compacité, une suite $\left(Q_{\phi(p)}\right)$ qui converge vers Q orthogonale. Et en écrivant

$$S_{\phi(p)} = Q_{\phi(p)}^T A_{\phi(p)}$$

On voit que la suite $\left(S_{\phi(p)}\right)$ converge vers $Q^T A$. Par **3.**, $Q^T A = S$ est symétrique positive. Ce qui conclut.

994.61

Une inégalités sur les déterminants de matrices symétriques

Un exercice ne contenant que des méthodes classiques, là encore

1. Soit $\lambda_1, \dots, \lambda_n$ des réels positifs. Démontrer que
$$\Big[\prod_{i=1}^{n}(1+\lambda_i)\Big]^{1/n} \geq 1 + \Big[\prod_{i=1}^{n}(\lambda_i)\Big]^{1/n}$$

2. On dit qu'une matrice symétrique est positive lorsque toutes ses valeurs propres sont positives. Montrer qu'une matrice symétrique positive admet une « racine carrée » symétrique positive (on ne demande pas d'examiner l'unicité).

3. Utiliser les questions précédentes pour montrer que, si A est symétrique positive d'ordre n,
$$\big[\det(I_n + A)\big]^{1/n} \geq 1 + \big[\det(A)\big]^{1/n}$$
puis que, si A et B sont symétriques positives,
$$\big[\det(A+B)\big]^{1/n} \geq \big[\det(A)\big]^{1/n} + \big[\det(B)\big]^{1/n}$$
(on remarquera que seul le cas où au moins l'une des deux matrices est inversible est intéressant. Si A est symétrique positive inversible, on écrira, en notant $A^{1/2}$ la « racine carrée » de A et $A^{-1/2}$ son inverse $B = A^{1/2}\big(A^{-1/2}BA^{-1/2}\big)A^{1/2}$ et on se ramènera à l'inégalité précédente.

On a, si f est convexe sur un intervalle I, et si $x_1, \dots, x_n \in I$,
$$f\left(\frac{1}{n}(x_1 + \cdots + x_n)\right) \leq \frac{1}{n}\left(f(x_1) + \cdots + f(x_n)\right)$$
La fonction ln étant croissante, l'inégalité proposée équivaut à
$$\frac{1}{n}\sum_{i=1}^{n}\ln(1+\lambda_i) \geq \ln\left(1 + \exp\left(\frac{1}{n}\sum_{i=1}^{n}\ln\lambda_i\right)\right)$$
…du moins si les λ_i sont strictement positifs. Mais si l'un des λ_i est nul, l'inégalité que l'on cherche est simple, on peut donc les supposer tous strictement positifs. L'inégalité proposée est donc équivalente à :
$$\frac{1}{n}\sum_{i=1}^{n}\ln\left(1+\exp(\ln\lambda_i)\right) \geq \ln\left(1 + \exp\left(\frac{1}{n}\sum_{i=1}^{n}\ln\lambda_i\right)\right)$$
Et si on montre que l'application $x \mapsto \ln(1+e^x)$ est convexe, on conclut (en appliquant l'inégalité générale de convexité aux $\ln\lambda_i$). Or cette fonction est C^∞ sur $\mathbf{R}$, et sa dérivée est
$$x \mapsto \frac{e^x}{1+e^x} = 1 - \frac{1}{1+e^x}$$
qui croît manifestement (on peut aussi calculer la dérivée seconde).

Si $A \in \mathcal{S}_n^+(\mathbf{R})$, on écrit $A = P\ D\ P^{-1} = P\ D\ {}^tP$ où $P \in \mathcal{O}(n)$ et
$D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$, $\forall i \quad \lambda_i \geq 0$. Donc $\det(A) = \prod_{i=1}^{n}\lambda_i$ et
$\det(I_n + A) = \det(P(I_n + D)P^{-1}) = \det(I_n + D) = \prod_{i=1}^{n}(1+\lambda_i)$. On est donc ramené à l'inégalité du début.

Si A et B sont symétriques positives, $A+B$ l'est (classique, utiliser la définition et non la caractérisation par le spectre). Si les deux matrices sont positives non définies, leurs déterminants sont nuls, le membre de droite de l'inégalité souhaitée vaut 0, le membre de gauche est positif (une matrice symétrique positive a un spectre inclus dans $\mathbf{R}^+$, et est diagonalisable, donc a un déterminant positif). On peut donc supposer $A \in \mathcal{S}_n^{++}$. Il est classique, à partir de la diagonalisation de A avec matrice de passage orthogonale, de trouver $A^{1/2}$ symétrique définie positive telle que

$$\left(A^{1/2}\right)^2 = A$$

On notera $\left(A^{1/2}\right)^{-1} = A^{-1/2}$, on a donc

$$A+B = A^{1/2}(I_n + A^{-1/2}BA^{-1/2})A^{1/2}$$

Or, si $C = A^{-1/2}BA^{-1/2}$, on vérifie que C est symétrique (B et $A^{-1/2}$ le sont, et le produit est palindromatique). De plus, si X est une colonne non nulle,

$$^tXCX = {}^tYBY \qquad \text{avec} \qquad Y = A^{-1/2}X \neq (0)$$

donc ${}^tXCX > 0$. On conclut que C est symétrique définie positive (symétrique positive suffisait). Et donc on est ramené à ce qui précède :

$$\begin{aligned}
[\det(A+B)]^{1/n} &= \left[\det\left(A^{1/2}(I_n + A^{-1/2}BA^{-1/2})A^{1/2}\right)\right]^{1/n} \\
&= \left[\left(\det(A^{1/2})\right)^2\right]^{1/n}\left[\det\left(I_n + A^{-1/2}BA^{-1/2}\right)\right]^{1/n} \\
&\geq (\det A)^{1/n}\left(1 + \left[\det(A^{-1/2}BA^{-1/2})\right]^{1/n}\right)
\end{aligned}$$

Mais $\det(A^{-1/2}BA^{-1/2}) = \dfrac{\det B}{\det A}$, on conclut…

994.62

Une technique classique : la racine carrée

Si S et T sont deux matrices symétriques dont toutes les valeurs propres sont positives, montrer que $\mathrm{tr}(ST) \geq 0$.

On considère une racine carrée Σ de S avec $\Sigma \in \mathcal{S}_n^+(\mathbf{R})$. Alors

$$\mathrm{tr}(ST) = \mathrm{tr}(\Sigma^2 T) = \mathrm{tr}(\Sigma T \Sigma)$$

Mais $\Sigma T\Sigma$ est symétrique (facile, T et Σ le sont et le produit est un palindrome), positive car

$${}^tX\Sigma T\Sigma X = {}^tYTY$$

avec $Y = \Sigma X$.

994.63

Un peu plus difficile

Initialement posé aux ens, ce genre de chose se répand…

Soit $A \in \mathcal{S}_n(\mathbf{R})$, de valeurs propres $\lambda_1, \ldots, \lambda_n$, supposées strictrement positives, et f convexe sur $\mathbf{R}_*^+$. Montrer que, pour tout i, $a_{i,i} > 0$ puis que

$$\sum_{i=1}^n f(a_{i,i}) \leq \sum_{i=1}^n f(\lambda_i)$$

Qu'obtient-on si l'on prend $f = -\ln$?

Soit $f : \mathbf{R} \to \mathbf{R}$ convexe, $A \in \mathcal{S}_n(\mathbf{R})$, de valeurs propres $\lambda_1, \ldots, \lambda_n$. Montrer que

$$f(a_{1,1}) + \ldots + f(a_{n,n}) = f(\lambda_1) + \ldots + f(\lambda_n)$$

En déduire que si A est définie positive, alors

$$\det(A) \leq a_{1,1} \dots a_{n,n}$$

Par théorème spectral, il existe P orthogonale telle que

$$A = P\text{diag}(\lambda_1, \dots, \lambda_n)P^T$$

En particulier on a, pour tout $i \in [\![1, n]\!]$:

$$\begin{aligned} a_{i,i} &= \sum_{k=1}^{n} p_{i,k} \left(\text{diag}(\lambda_1, \dots, \lambda_n)P^T\right)_{k,i} \\ &= \sum_{k=1}^{n} p_{i,k}\lambda_k (P^T)_{k,i} \\ &= \sum_{k=1}^{n} p_{i,k}^2 \lambda_k \end{aligned}$$

Mais f est convexe, et P étant orthogonale vérifie, pour tout i,

$$\sum_{k=1}^{n} p_{i,k}^2 = 1$$

Donc

$$f(a_{i,i}) \leq \sum_{k=1}^{n} p_{i,k}^2 f(\lambda_k)$$

On somme pour i allant de 1 à n, on intervertit les sommes, on utilise une fois encore l'orthogonalité de P, et le résultat s'ensuit. Si A est définie positive, comme

$$\det(A) = \prod_{i=1}^{n} \lambda_i$$

on a envie de prendre le logarithme. Or $-\ln$ est convexe. Mais seulement sur $\mathbf{R}_*^+$. Le calcul ci-dessus est donc valable (la stricte positivité des $a_{i,i}$ peut se montrer a priori, en utilisant la caractérisation

$$\forall M \in \mathcal{S}_n(\mathbf{R}) \qquad \left(\text{Sp}(M) \subset \mathbf{R}_*^+\right) \Leftrightarrow \left(\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \setminus \{0\} \quad X^T M X > 0\right)$$

qui se montre avec le théorème spectral, et en l'appliquant aux $X = E_i$ de la base canonique ; mais cette stricte positivité des $a_{i,i}$ est aussi une conséquence du premier calcul fait plus haut qui montre que chaque $a_{i,i}$ est barycentre à coefficients positifs des λ_i. On a même le fait que tous les $a_{i,i}$ sont entre la plus petite et la plus grande valeur propre de A). Le résultat s'ensuit.

994.64

Ordre de Löwner

Très difficile : niveau X-ens

Sur $\mathcal{S}_n(\mathbf{R})$, on définit la relation $\leq$ par : $A \leq B \Leftrightarrow B - A \in \mathcal{S}_n^+(\mathbf{R})$ où $\mathcal{S}_n^+(\mathbf{R})$ est l'ensemble des matrices symétriques dont les valeurs propres sont positives.

1. Montrer que $\leq$ est une relation d'ordre sur $\mathcal{S}_n(\mathbf{R})$.
2. Montrer qu'une partie de $\mathcal{S}_n(\mathbf{R})$ est bornée si et seulement si elle est majorée et minorée pour $\preceq$.
3. Montrer que toute suite croissante majorée pour $\preceq$ converge.

4. Si $A \in \mathcal{S}_n^{++}(\mathbf{R})$ et $X \in \mathcal{M}_{n,1}(\mathbf{R})$, calculer

$$\sup\{2\langle X, Y\rangle - \langle AY, Y\rangle \ ; \ Y \in \mathcal{M}_{n,1}(\mathbf{R})\}$$

où $\mathcal{S}_n^{++}(\mathbf{R})$ désigne l'ensemble des matrices symétriques dont toutes les valeurs propres sont strictement positives.

5. En déduire que $A \leq B \ \Rightarrow \ A^{-1} \geq B^{-1}$ quels que soient A et B dans $\mathcal{S}_n^{++}(\mathbf{R})$

---

1. La seule difficulté est l'antisymétrie, qui se ramène à montrer la propriété suivante : si $M \in \mathcal{S}_n(\mathbf{R})$, si $\forall X \in \mathcal{M}_{n,1}(\mathbf{R})$ $X^T M X = 0$, alors $M = (0)$.

   Mais si X est un vecteur propre de M associé à la valeur propre λ, on a $X^T M X = \lambda X^T X$. Or $X^T X \in \mathbf{R}_*^+$ ($X^T X = \|X\|^2$, où $\|.\|$ est la norme euclidienne canonique). Donc, si $X^T M X = 0$, $\lambda = 0$. On en déduit que si $\forall X \in \mathcal{M}_{n,1}(\mathbf{R})$ $X^T M X = 0$, $\lambda = 0$, ce pour toute valeur propre λ de M. Et comme M est diagonalisable (théorème spectral), on a bien $M = 0$.

2. Une très bonne idée est de munir $\mathcal{M}_n(\mathbf{R})$ (et a fortiori $\mathcal{S}_n(\mathbf{R})$) de la norme

$$\|M\| = \sqrt{\mathrm{Tr}(M^T M)}$$

   On se souvient en effet de l'expression du produit scalaire canonique sur $\mathcal{M}_n(\mathbf{R})$:

$$(A|B) = \mathrm{Tr}(A^T B)$$

   qui se vérifie facilement analytiquement. Remarquons que, si M est symétrique, le théorème spectral donne l'existence de P orthogonale et de D diagonale telles que

$$M = PDP^T = PDP^{-1}$$

   et alors

$$\|M\|^2 = \mathrm{Tr}(M^2) = \mathrm{Tr}\left(\left(PDP^{-1}\right)^2\right) = \sum_{i=1}^{n} \lambda_i^2$$

   où $\lambda_1, \ldots, \lambda_n$ sont les valeurs propres de M, répétées autant de fois que leur multiplicité.

   Supposons que $\mathcal{E}$ soit une partie de $\mathcal{S}_n(\mathbf{R})$ majorée par $A \in \mathcal{S}_n(\mathbf{R})$ et minorée par $B \in \mathcal{S}_n(\mathbf{R})$; il est utile de se rappeler que, pour toute matrice $M \in \mathcal{S}_n(\mathbf{R})$,

$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad \lambda_{\min} X^T X \leq X^T M X \leq \lambda_{\max} X^T X \tag{1}$$

   où $\lambda_{\max}$ et $\lambda_{\min}$ sont respectivement la plus grande et la plus petite valeur propre de M. La démonstration la plus simple de ce fait se rédige en termes d'endomorphismes : si u est un endomorphisme symétrique, si $(e_1, \ldots, e_n)$ est une base orthonormale de vecteurs propres de u associés respectivement aux valeurs propres $\lambda_1 \leq \ldots \leq \lambda_n$, si $x = \sum_{i=1}^{n} x_i e_i$,

$$\lambda_{\min}\left(\sum_{i=1}^{n} x_i^2\right) \leq (x|u(x)) = \sum_{i=1}^{n} \lambda_i x_i^2 \leq \lambda_{\max}\left(\sum_{i=1}^{n} x_i^2\right)$$

   ce qui, matriciellement, s'interprète comme la relation (1). On remarquera que cet encadrement est optimal : les deux inégalités ci-dessus sont des égalités en prenant respectivement $x = e_n$ et $x = e_1$.

   Reprenons : si $\mathcal{E}$ est majorée par A et minorée par B, on a, pour tout $X \in \mathcal{M}_{n,1}(\mathbf{R}$, pour tout $M \in \mathcal{E}$,

$$\alpha X^T X \leq X^T M X \leq \beta X^T M X$$

   où $\beta = \mathrm{Max}\,(\mathrm{Sp}(A))$ et $\alpha = \mathrm{Min}\,(\mathrm{Sp}(B))$. On en déduit facilement que $\mathrm{Sp}(M) \subset [\alpha, \beta]$. (prendre une valeur propre de M, appliquer l'inégalité ci-dessus à un vecteur propre associé). Notant $\gamma = \mathrm{Max}(|\alpha|, |\beta|)$, on obtient

$$\forall \lambda \in \mathrm{Sp}(M) \qquad \lambda^2 \leq \gamma^2$$

Finalement

$$\forall M \in \mathcal{E} \qquad \|M\|^2 \leq n\gamma^2$$

et $\mathcal{E}$ est bien borné.

Supposons réciproquement $\mathcal{E}$ bornée. Soit R tel que

$$\forall M \in \mathcal{E} \qquad \|M\| \leq R$$

Alors (par l'expression de la norme à l'aide des valeurs propres) on a

$$\forall M \in \mathcal{E} \qquad \mathrm{Sp}(M) \subset [-R, R]$$

et donc

$$\forall M \in \mathcal{E} \qquad -RI_n \preceq M \preceq RI_n$$

ce qui conclut la réciproque.

Si on ne pensait pas à utiliser la norme euclidienne canonique et la formule avec la trace qui la donne, on pouvait quand même s'en sortir. L'essentiel est de voir que borner des matrices symétriques, c'est borner leurs valeurs propres : en effet, dans la formule

$$M = PDP^T = PDP^{-1}$$

la matrice P qui est orthogonale a tous ses coefficients entre -1 et 1 ; trouver une borne pour toutes les $M \in \mathcal{E}$, c'est donc trouver une borne « pour toutes les D », i.e. borner les valeurs propres.

3. Un peu de topologie : soit (S_n) une suite croissante majorée pour $\preceq$. Elle est aussi minorée pour $\preceq$ (par S_0). Donc bornée par la question précédente. On est ne dimension finie, on peut donc utiliser le théorème de Bolzano-Weierstrass. Extrayons une suite convergente $(S_{\phi(n)})$. Elle est croissante pour $\preceq$, et sa limite est $S \in \mathcal{S}_n(\mathbf{R})$. Soit $(S_{\psi(n)})$ une autre suite extraite convergente, S' sa limite. Fixons $n \in \mathbf{N}$; à partir d'un certain rang p_0, on a $\psi(p) \geq \phi(n)$, donc

$$S_{\phi(n)} \preceq S_{\psi(p)} \preceq S' \tag{1}$$

(cette dernière inégalité vient du fait que

$$\forall q \geq p \qquad S_{\psi(p)} \preceq S_{\psi(q)}$$

donc

$$\forall q \geq p \quad \forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \quad X^T S_{\psi(p)} X \leq X^T S_{\psi(q)} X$$

mais, par linéarité en dimension finie donc continuité de $M \mapsto X^T M X$, on a, pour toute X,

$$X^T S_{\psi(q)} X \xrightarrow[q \to +\infty]{} X^T S' X$$

et les inégalités larges (dans $\mathbf{R}$, bien sûr) passent à la limite quand $q \to +\infty$). En interprétant de nouveau l'inégalité (1) par

$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \quad X^T S_{\phi(n)} X \leq X^T S' X$$

qui est vraie sans restriction sur n et en utilisant la conservation des inégalités larges à la limite quand $n \to +\infty$, on obtient

$$S \preceq S'$$

mais symétriquement $S' \preceq S$ et donc par antisymétrie $S' = S$. Reste à se souvenir qu'une suite dans un compact qui a une unique valeur d'adhérence converge pour conclure.

4. Méthode très, très classique : on commence par examiner le cas où, par exemple, $B = I_n$ (on pourrait aussi envisager le cas où $A = I_n$). Ce cas n'est pas dur, car l'hypothèse $A \preceq I_n$ donne que toutes les valeurs propres de A sont dans $]0, 1]$ (on sait qu'elles sont strictement positives car $A \in \mathcal{S}_n^{++}(\mathbf{R})$). Donc toutes les valeurs propres de A^{-1} sont > 1, ce qui donne bien $I_n \preceq A^{-1}$.

   Dans le cas général, soit $C \in \mathcal{S}_n^{++}(\mathbf{R})$ telle que $C^2 = B$ (existence classique mais hors-programme, à redémontrer). Les lignes suivantes sont alors équivalentes :

$$A \preceq B$$

$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T A X \leq (CX)^T (CX)$$
$$\forall Y \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad (C^{-1}Y)^T A (C^{-1}Y) \leq Y^T Y$$
$$\forall Y \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad Y^T (C^{-1} A C^{-1}) Y \leq Y^T Y$$

On montre alors que $C^{-1}AC^{-1} \in \mathcal{S}_n^{++}$; qu'elle soit symétrique n'est pas difficile ; qu'elle soit définie positive vient d'une caractérisation qu'il faut savoir établir, via le théorème spectral :

$$\forall M \in \mathcal{S}_n(\mathbf{R}) \qquad \Big(\mathrm{Sp}(M) \subset \mathbf{R}_*^+\Big) \Leftrightarrow \Big(\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \setminus \{0\} \quad X^T M X > 0\Big)$$

On a donc $C^{-1}AC \preceq I_n$, on peut donc déduire du cas $B = I_n$ que $I_n \preceq CA^{-1}C$. Ce qui équivaut successivement à

$$\forall Y \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad Y^T (CA^{-1}C) Y \geq Y^T Y$$
$$\forall Y \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad (CY)^T A^{-1} (CY) \geq Y^T Y$$
$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T A^{-1} X \geq (C^{-1}X)^T (C^{-1}X)$$

$$\forall X \in \mathcal{M}_{n,1}(\mathbf{R}) \qquad X^T A^{-1} X \geq X^T C^{-1} C^{-1} X$$
$$B^{-1} \preceq A^{-1}$$