Les astuces de Mançois Froulin

Son CDT 2024-2025

21 février 2025

Nouveau : pas mal d'exercices d'espaces vectoriels

Table des matières

Chapitre 1

Algèbre générale

1.1 Points méthode

1.2 Astuces

Recettes du sous-... Pour montrer qu'un ensemble est un sous-groupe, sous-anneau, sous-corps, sous-espace vectoriel, toujours s'assurer qu'il est non vide en justifiant qu'il contient 0 (neutre pour la loi principale !) voire 1 (pour un anneau ou un corps).

Recette du sous-... : remarque Pour montrer qu'un ensemble est un sous-groupe, un rapport de jury (XENS-A-2020) décrète que la méthode "montrer que $x - y \in H$" est convenable si la vérification est triviale ou découle des théorèmes généraux. Si c'est plus délicat, il vaut mieux distinguer la stabilité de la loi interne de l'existence d'un inverse.

Condition nécessaire pour que le groupe quotient soit un groupe Quand on a un groupe G et un sous-groupe H, pour que G/H soit un groupe, il faut que H soit distingué. En quotientant ainsi, on réduit le cardinal du groupe à étudier.

Sous-groupe fini de $\mathcal{GL}_n(\mathbb{K})$ et projecteur Si G est un sou-groupe fini de $\mathcal{GL}_n(\mathbb{K})$, alors

$$M = \frac{1}{|G|} \sum_{A \in G} A$$

est un projecteur. En effet, en élevant au carré et en utilisant que pour $A \in G$ fixé l'application de G dans G qui à B associe AB est une bijection (injective et égalité de cardinaux), on obtient le résultat par changement variables.

Étude d'éléments particuliers via une fonction En algèbre générale, quand on cherche un élément particulier, poser une application f telle que ce que l'on cherche soit un antécédent par f et montrer qu'il existe (par exemple montrer que f est surjective, potentiellement en commençant par l'injectivité pour établir la bijectivité !).

Application. Si on cherche les carrés de $\mathbb{Z}/p\mathbb{Z}$, on s'intéresse à $x \mapsto x^2$.

Application. Si on cherche un inverse pour tout élément non nul a dans un anneau commutatif, on montre que $x \mapsto ax$ est surjective. Il en résulte que tout anneau commutatif fini et intègre est un corps.

Un lemme Si G est un groupe et si a et b sont deux éléments qui commutent d'ordres respectifs p et q avec $p \wedge q = 1$, alors ab est d'ordre pq. Démonstration : notons $w(ab)$ l'ordre de ab. $(ab)^{pq} = a^{pq}b^{pq} = e$ car a et b commutent donc $w(ab) \mid pq$. De plus puisque $(ab)^{w(ab)} = e$, il vient $a^{w(ab)} = b^{-w(ab)}$ et $a^{w(ab)q} = b^{-w(ab)q} = e$ d'où $p \mid w(ab)q$ (p est l'ordre de a). Puisque $p \wedge q = 1$, il vient $p \mid w(ab)$. De même, on montre que $q \mid w(ab)$. Ainsi $pq \mid w(ab)$ puisque p et q sont premiers entre eux. pq et $w(ab)$ étant associés et positifs, il sont égaux.

Théorème de Cauchy Si G est un groupe fini d'ordre n et si p est un diviseur premier de n, alors G possède un élément d'ordre p. Il y a deux démonstrations possibles : l'une, plus simple, dans le cas d'un groupe abélien, et l'autre dans le cas général, mais plus difficile.

Lemme des bergers généralisé Si E et F sont des ensembles finis, et $f : E \to F$, alors on a la formule :

$$\mathrm{Card}(E) = \sum_{y \in F} \mathrm{Card}\left(\in (\{y\})\right)$$

En effet, l'unicité de l'image nous fournit l'union disjointe

$$E = \bigsqcup_{y \in f(E)} f^{-1}(\{y\})$$

et on peut prendre F tout entier car si y n'est pas dans $f(E)$, son image réciproque est vide. On obtient la relation en passant aux cardinaux.

Application. On retrouve le lemme de bergers. : si tout élément de F possède p antécédents, alors $\mathrm{Card}(E) = p\mathrm{Card}(F)$.

Application. En particulier, si f est un morphisme de groupes, on a l'égalité

$$\mathrm{Card}(E) = \mathrm{Card}(\mathrm{Im}(f)) \times \mathrm{Card}(\mathrm{Ker}(f))$$

Équation aux classes (HP) Penser à utiliser l'équation aux classes :

$$ACOMPLETER$$

Pour la démontrer, A COMPLETER

Utilisation des idéaux de $\mathbb{K}[X]$ Pour faire un usage intéressant du théorème de structure des idéaux de $\mathbb{K}[X]$, ne pas oublier de vérifier que l'idéal n'est pas réduit à $\{0\}$.

Un sous-groupe fini strict est au moins deux fois moins gros Si H est un sous-groupe strict du groupe G fini, alors $2|H| \leqslant G$. En effet, cela est une conséquence immédiate du théorème de Lagrange.

Application. Dans $\mathcal{S}_n$, il n'y a pas de sous-groupe strict contenant strictement $\mathcal{A}_n$, puisque celui-ci a déjà pour cardinal la moitié de celui-ci de $\mathcal{S}_n$.

Autour des corps finis contenant $\mathbb{F}_p$ On considère $\mathbb{K}$ un corps fini de cardinal q contenant $\mathbb{F}_p$. Alors, il existe $n \in \mathbb{N}^*$ tel que

$$q = p^n$$

En effet, on peut munir naturellement $\mathbb{K}$ d'une structure de $\mathbb{F}_p$-espace vectoriel. De plus, $\mathbb{K}$ est fini, donc admet une famille $\mathbb{F}_p$-génératrice finie, donc $\mathbb{K}$ est un espace vectoriel de dimension finie sur $\mathbb{F}_p$. Ainsi, $\mathbb{K}$ est isomorphe à un certain $\mathbb{F}_p^n$ et le résultat suit par égalité de cardinaux (bijectivité). Ensuite, on a :

$$\forall x \in \mathbb{K},\ x^q = x$$

En effet, si $x = 0$, c'est immédiat. Sinon, $x \in \mathbb{K}^*$, qui est un groupe de cardinal $q-1$. Donc $x^{q-1} = 1$ et $x^p = x$. Ensuite, l'application :

$$\begin{array}{rccc} \varphi : & \mathbb{K} & \longrightarrow & \mathbb{K} \\ & x & \longmapsto & x^p \end{array}$$

est un automorphisme de $\mathbb{K}$. En effet, c'est un morphisme additif en utilisant le fait que p divise toujours $\binom{p}{k}$ lorsque $1 \leqslant k \leqslant p-1$. Puis $\mathbb{K}$ est commutatif (on peut prendre cela comme définition d'un corps, mais de toute façon, le théorème de Wedderburn affirme que tout corps fini est commutatif), donc φ est un morphisme multiplicatif. Enfin, c'est un morphisme de corps, donc il est injectif puis bijectif par égalité de cardinaux. Enfin, on peut montrer que $\mathbb{K}^*$ est cyclique.

Caractéristique d'un corps Pour $\mathbb{K}$ un corps, on note

$$\begin{array}{rccc} j : & \mathbb{Z} & \longrightarrow & \mathbb{K} \\ & n & \longmapsto & n.1_{\mathbb{K}} \end{array}$$

C'est un morphisme donc son noyau est un idéal de $\mathbb{Z}$ et donc il existe $n \in \mathbb{N}$ tel que $\mathrm{Ker}(j) = n\mathbb{Z}$.

- Si $n = 0$, alors $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Q}$. On prolonge j de manière naturelle à $\mathbb{Q}$. Cette définition est bien consistante (le prouver à la main). Il est clair que ce prolongement de $\mathbb{Q}$ dans $\mathbb{K}$ est injectif, ce qui fournit le résultat annoncé.
- Si $n \geqslant 1$, alors n est un nombre premier et $\mathbb{K}$ contient un sous-corps isomorphe à $\mathbb{Z}/n\mathbb{Z}$. En effet, en raisonnant par l'absurde, l'intégrité de $\mathbb{K}$ couplée à la minimalité de n impose le fait que n soit premier. Si $\overline{k} = \overline{l}$ dans $\mathbb{Z}/n\mathbb{Z}$, alors $n \mid k - l$ si bien que $j(k-l) = 0$ car $j(n) = 0$. On "prolonge" ainsi sur $\mathbb{Z}/n\mathbb{Z}$, et le prolongement est injectif, ce qui fournit le résultat.

L'entier n est appelé **caractéristique du corps** $\mathbb{K}$.

Remarque. Un corps infini peut très bien être de caractéristique finie. Par exemple, $\mathbb{Z}/p\mathbb{Z}(X)$ avec p premier est infini (clairement, puisqu'il contient les monômes) et pourtant, il est de caractéristique p (cela s'hérite du fait que $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p).

1.3 Exercices classiques

Sous-groupes additifs de $\mathbb{R}$: HP à connaître

Les sous-groupes additifs de $\mathbb{R}$ sont soit de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}_+$, soit denses dans $\mathbb{R}$.

Démonstration. Soit H un sous-groupe additif de $\mathbb{R}$. Si $H = \{0\}$, alors il est bien de la forme $a\mathbb{Z}$ avec $a = 0$. Sinon, il contient un réel non nul, et quitte à passer à l'opposé, il contient un réel strictement positif. Donc $H \cap \mathbb{R}_+^*$ est non vide, et il admet une borne inférieure a.

- Supposons que $a \in H$, et montrons alors que $H = a\mathbb{Z}$.
  D'une part, on a $< a >= a\mathbb{Z} \subset H$ par définition du sous-groupe engendré. Réciproquement, soit $x \in H$. Comme $a \in \mathbb{R}_+^*$, on peut considérer $q = \left\lfloor \frac{x}{a} \right\rfloor \in \mathbb{Z}$ et $r = x - aq$. Alors, d'après la première inclusion, $r \in H$, et comme $r \in [0, a[$, on a $r = 0$ par minimalité de a. Donc $x = aq \in a\mathbb{Z}$.
- Supposons que $a \notin H \cap \mathbb{R}_+^*$., et montrons alors que H est dense dans $\mathbb{R}$.
  Donnons-nous un intervalle $]x, y[$ de largeur $\varepsilon = y - x > 0$.
  - Montrons qu'on peut trouver un $h \in]0, \varepsilon[$ dans H. Prenons dans $H \cap \mathbb{R}_+^*$ un h_1 tel que $h_1 \in [a, a+\varepsilon[$. Comme $a \notin H \cap \mathbb{R}_+^*$, on a même $h_1 \in]a, a+\varepsilon[$. Par le même raisonnement, prenons dans H un $h_2 \in]a, h_1[$. il suffit alors de poser $h = h_1 - h_2$.
  - Ensuite, posons $q = \left\lfloor \frac{x}{h} \right\rfloor + 1 \in \mathbb{Z}$. Alors qh appartient à H et il vérifie $x < qh < y$.
- Enfin, aucun $H = a\mathbb{Z}$ ne peut être dense dans $\mathbb{R}$ (il s'agit bien d'un "soit/soit"). En effet :
  - Si $a = 0$, alors l'intervalle $]0, 1[$ ne contient aucun élément de H.
  - Si $a > 0$, alors l'intervalle $]0, a[$ ne contient aucun élément de H.

Ainsi, la preuve est achevée. □

Nombre de permutations avec k cycles distincts

On note $u_{n,k}$ le nombre de permutations de $\mathcal{S}_n$ avec k cycles distincts (un point fixe compte pour un cycle). On a la formule de récurrence :

$$u_{n+1,k+1} = u_{n,k} + n \times u_{n,k+1}$$

Démonstration. Le premier terme correspond au cas où $n+1$ est seul dans son cycle, et le deuxième aux cas où $n+1$ n'est pas seul dans son cycle. □

Un groupe dont tous les éléments sont d'ordre 2 est commutatif

Montrer qu'un groupe dont tous les éléments sont d'ordre 2 est commutatif.

Démonstration. Supposons

$$\forall x \in G,\ x^2 = e$$

Alors : $\forall x \in G,\ x = x^{-1}$. En appliquant ceci à xy, on obtient :

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

donc G est commutatif. □

Petit théorème de Fermat sur les groupes : cas commutatif

Soit G un groupe commutatif fini de cardinal $|G|$ et d'élément neutre e. Soit $x \in G$. En calculant $\prod_{g \in G} (xg)$ de deux façons différentes, montrer que $x^{|G|} = e$.

Démonstration. Déjà, remarquons que c'est la commutativité de G qui nous autorise à définir ce produit correctement. Notons-le P dans la suite.

- D'une part, par commutativité, on a $P = x^{|G|} \prod_{g \in G} g$.
- D'autre part, l'application

$$f_x : \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & xg \end{array}$$

  est une bijection. En effet, elle est injective par régularité de x dans G, et elle est surjective car pour atteindre un élément g de G, il suffit de prendre comme antécédent $x^{-1}g$. On peut donc effectuer un changement de variable qui prouve que $P = \prod_{g \in G} g$.
- Enfin, en égalisant ces deux expressions de P et par régularité de $\prod_{g \in G} g$, on obtient bien que $x^{|G|} = e$.

$\square$

Petit théorème de Fermat pour les groupes : cas général

Soit G un groupe fini (non nécessairement commutatif) de cardinal $|G|$ et d'élément neutre e. Soit $x \in G$. On souhaite montrer que $x^{|G|} = e$.

1. Justifier l'existence de $p = \min\left\{n \in \mathbb{N}^* \mid x^n = e\right\}$.
2. Montrer que $\langle x \rangle = \left\{x^0, \ ..., x^{p-1}\right\}$ et en déduire que $\mathrm{Card}(\langle x \rangle) = p$.
3. Conclure.

Démonstration. Pour la 1, utiliser le principe des tiroirs.Pour la 2, utiliser la caractérisation du sous-groupe engendré par un élément et une division euclidienne. Montrer que les x^k sont deux à deux distincts pour k variant entre 0 et $p-1$. Pour la 3, utiliser le théorème de Lagrange (à savoir redémontrer car HP) ou utiliser sa variante au programme

1. Considérons $f_x : \begin{array}{ccc} [\![1, \ |G|+1]\!] & \longrightarrow & G \\ t & \longmapsto & x^t \end{array}$. D'après le principe des tiroirs, f_x n'est pas injective. On peut donc fixer $1 \leqslant a, b \leqslant |G|+1$ tels que $a \neq b$ et $f_x(a) = f_x(b)$. On a alors $x^a = x^b$. Sans perte de généralité, quitte à échanger a et b, on peut supposer que $a < b$. On a alors $x^{b-a} = e$ et $b - a \in \mathbb{N}^*$. L'ensemble que l'on considère est alors une partie de $\mathbb{N}$ non vide, donc son minimum existe.

2. L'inclusion réciproque est immédiate car $\langle x\rangle = \left\{x^k \mid k \in \mathbb{Z}\right\}$. Dans l'autre sens, soit $y \in \langle x\rangle$. Fixons $k \in \mathbb{Z}$ tel que $y = x^k$. Effectuons la division euclidienne de k par p : $k = ap + b$ avec $a \in \mathbb{Z}$ et $b \in [\![0,\ p-1]\!]$. On a alors
$$y = x^{ap+b} = (x^p)^a x^b = e^a x^b = x^b$$
et obtient bien le résultat.

   Pour montrer que le cardinal de cet ensemble vaut p, il suffit de montrer que ses éléments sont deux à deux distincts. Soit $0 \leqslant m \leqslant n \leqslant p-1$ tels que $x^m = x^n$. Raisonnons par l'absurde : supposons que $n-m \geqslant p$. Alors $n \geqslant p+m \leqslant p > p-1$ ce qui est absurde. Donc $0 \leqslant n-m < p$. Or, $x^{n-m} = e$ donc par minimalité de p, $n-m = 0$ puis $n = m$. Les éléments sont bien deux à deux distincts, donc on a bien $\mathrm{Card}(\langle x\rangle) = p$.
3. $\langle x\rangle$ est un sous-groupe de G, donc, d'après le théorème de Lagrange, son cardinal divise $|G|$. On peut donc fixer $k \in \mathbb{Z}$ tel que $|G| = kp$. On a alors
$$x^{|G|} = x^{kp} = (x^p)^k = e^k = e$$

   Pour mémoire, si on considère un sous-groupe H quelconque de G fini, il faut considérer la relation d'équivalence $\forall (x,y) \in G^2,\ x \sim y \iff xy^{-1} \in H$. Toutes les classes ont même cardinal car ce sont les xH. Puisque les classes d'équivalences forment une partition, on obtient le théorème de Lagrange.

$\square$

Une propriété sur les cardinaux de parties d'un groupe

Soit A et B deux parties d'un groupe fini G telles que $\mathrm{Card}(A) + \mathrm{Card}(B) > \mathrm{Card}(G)$. Montrer que $G = AB$ avec
$$AB = \{ab \mid (a,b) \in A \times B\}$$

Indication. *Pour l'inclusion directe, se donner $x \in G$ puis on pourra montrer que $A^{-1}x \cap B \neq \emptyset$.*

Indication. *Relativement à l'indication qui précède, on pourra observer que $A \cap B \neq \emptyset$ puis remarquer que $Card(A^{-1}x) = Card(A)$.*

Démonstration. L'inclusion réciproque est immédiate par stabilité de G en tant que groupe. Passons à l'inclusion directe. Déjà, on peut remarquer que $A \cap B \neq \emptyset$: en effet, on a $A \cup B \subset G$ donc
$$\mathrm{Card}(A \cup B) = \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(A \cap B) \leqslant \mathrm{Card}(G)$$
Par hypothèse, il s'ensuit que
$$\mathrm{Card}(A \cap B) \geqslant \mathrm{Card}(A) + \mathrm{Card}(B) - \mathrm{Card}(G) > 0$$
donc on a bien $A \cap B \neq \emptyset$. Soit désormais $x \in G$. L'application
$$\begin{array}{rccl} f: & A & \longrightarrow & A^{-1}x \\ & a & \longmapsto & a^{-1}x \end{array}$$

est bijective. En effet, elle est injective par régularité de x et surjective par définition. Ainsi, on a $\mathrm{Card}(A^{-1}x) = \mathrm{Card}(A)$. Ensuite, on a donc l'inégalité stricte $\mathrm{Card}(A^{-1}x) + \mathrm{Card}(B) > \mathrm{Card}(G)$. Exactement de la même façon que dans notre remarque introductive, on montre que $A^{-1}x \cap B \neq \emptyset$. Ainsi, on peut fixer $b \in A^{-1}x \cap B$. On peut alors fixer $a \in A$ tel que $b = a^{-1}x$. On obtient donc $x = ab \in AB$, ce qui achève l'exercice. $\square$

Injectivité des morphismes de corps (peut-être du cours en spé ? ?)

Montrer que tout morphisme de corps est injectif.

Démonstration. Soit φ un morphisme du corps $\mathbb{K}$ vers le corps $\mathbb{L}$. Raisonnons par l'absurde : supposons que φ n'est pas injectif. On peut alors fixer $x \in \mathrm{Ker}(\varphi) \setminus \{0_{\mathbb{K}}\}$. Or, x est non nul, donc on a :

$$1_{\mathbb{L}} = \varphi(1_{\mathbb{K}}) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1}) = 0_{\mathbb{L}}$$

par propriétés des morphismes de corps ainsi que par absorbance. Or, nos corps sont toujours supposés non triviaux, donc ceci est **absurde**. Ainsi, φ est bien injectif, ce qui conclut. $\square$

Structure de corps des anneaux intègres finis

Montrer que tout anneau intègre fini est un corps.

Démonstration. Donnons-nous un anneau intègre fini A et a un élément non nul de A. Considérons l'application

$$\varphi_a : \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array}$$

Déjà, cette application est bien définie par stabilité de l'anneau par la deuxième loi. Ensuite, elle injective par intégrité de A. Enfin, elle est alors surjective par égalité de cardinaux. Donc on peut fixer un antécédent de 1_A par φ_a, ce qui montre que a est inversible. Ainsi, A est bien un corps car seule l'inversibilité des éléments non nuls manquait. $\square$

Idéaux d'un corps

Déterminer l'ensemble des idéaux d'un corps $\mathbb{K}$

Indication. *Que se passe-t-il si un élément non nul de $\mathbb{K}$ appartient à un idéal ?*

Démonstration. On raisonne classiquement par analyse-synthèse.

- **Analyse** : Soit I un idéal de $\mathbb{K}$. L'idéal nul est évidemment solution, donc on peut désormais supposer que I n'est pas réduit au groupe trivial. Fixons $x \in I \setminus \{0_{\mathbb{K}}\}$. Puisque I est un idéal, $xx^{-1} = 1_{\mathbb{K}} \in I$. Par suite, pour tout $y \in \mathbb{K}$, $y \times 1_{\mathbb{K}} = y \in I$, donc $I = \mathbb{K}$.
- **Synthèse** : Réciproquement, $\{0_{\mathbb{K}}\}$ et $\mathbb{K}$ sont bien des idéaux de $\mathbb{K}$, la vérification est immédiate.

$\square$

Anneau noethérien

Soit A un anneau. Montrer l'équivalence entre les assertions suivantes.

1. Tout idéal de A est engendré par un nombre fini d'éléments.
2. Toute suite croissante d'idéaux de A est stationnaire.
3. Toute famille non vide d'idéaux de A possède un élément maximal.

Lorsqu'un anneau vérifie l'une de ces trois conditions équivalentes, on dit que l'anneau est **noethérien**.

Remarque. On peut montrer qu'un anneau noethérien intègre est toujours un anneau factoriel, c'est-à-dire un anneau dans lequel a existence et unicité (à association près et à l'ordre des facteurs près) d'une décomposition en éléments irréductibles. Par exemple, tout anneau principal est noethérien puis factoriel, ce qui prouve par exemple de façon immédiate l'existence et l'unicité de la DFP dans $\mathbb{Z}$ et de la DFI dans $\mathbb{K}[X]$.

Chapitre 2

Arithmétique

2.1 Points méthode

2.2 Astuces

Travail sur des carrés Quand on travaille sur des carrés, penser à regarde ce qu'il se passe modulo 4 et 8 : cela fait très bon ménage avec les carrés. Modulo 4, les carrés valent 0 ou 1, et modulo 9, ils valent 0, 1 ou 4.

Travail sur des cubes Quand on travaille sur des cubes, penser à regarde ce qu'il se passe modulo 7 et 9 : cela fait très bon ménage avec les cubes. Modulo 7, les cubes valent 0, 1 ou 6, et modulo 9, ils valent 0, 1 ou 8.

Nombres premiers entre $n+1$ et $2n$ Soit p un nombre premier entre $n+1$ et $2n$. Il est facile de montrer que $p \mid \binom{2n}{n}$ et on en déduit :

$$\prod_{\substack{n+1<p\leqslant 2n \\ p \text{ premier}}} p \,\Bigg|\, \binom{2n}{n}$$

Application. On en déduit notamment l'inégalité :

$$\prod_{\substack{n+1<p\leqslant 2n \\ p \text{ premier}}} p \leqslant \binom{2n}{n} \leqslant \sum_{k=0}^{2n} \leqslant 4^n$$

Cela peut servir (en partie) à démontrer le théorème de Tchebychev / postulat de Bertrand : il existe toujours un nombre premier entre $n+1$ et $2n$ dès que $n \geqslant 2$. Et sinon, *cf* Maths A 2024...

Pseudo-réciproque d'une divisibilité Soit p premier. Si $(p^1-1) \mid (p^m-1)$, alors $n \mid m$. Il faut appliquer simultanément l'algorithme de division euclidienne à p^m-1 par p^n-1 et à m par n.

Décomposition d'un entier par les indicatrices d'Euler de ses diviseurs On a la formule :

$$\forall n \in \mathbb{N}^*,\ n = \sum_{d|n} \varphi(d)$$

Pour le démontrer, montrer l'égalité ensembliste suivante, et la passer aux cardinaux :

$$\left\{\frac{k}{n} | 1 \leqslant k \leqslant n\right\} = \bigsqcup_{d|n} \left\{\frac{k}{d} | k \wedge d = 1\right\}$$

Application. Calcul du déterminant de Smith.

Congruences de suites Quand on doit prouver des congruences sur les termes de suites, où le modulo varie, du type

$$a_n \equiv b_n n\ [m_n n]$$

où $n \in \mathbb{N}$, il faut revenir aux entiers et faire une récurrence. De façon générale, si on travaille avec des congruences qui n'ont pas le même modulo, il faut revenir aux entiers !

"PGCD" d'une infinité d'entiers Pour adapter le concept de PGCD pour une infinité d'entiers a_n, on observe l'idéal engendré par les a_n, ce qui permet en général de s'en sortir.

Équations de Pell-Fermat Ce sont des équations de la forme $a^2 - 2b^2 = \pm 1$. Penser au conjugué algébrique et par conséquent se placer dans

$$\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid (a, b) \in \mathbb{Z}^2\right\}$$

On y définit le morphisme de conjugaison

$$a + b\sqrt{2} \mapsto a - b\sqrt{2}$$

ainsi que le "module"

$$N : a + b\sqrt{2} \mapsto (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$$

Ce "module" est multiplicatif : $N(zz') = N(z)N(z')$. On se ramène donc à l'étude des inversibles.

Application. On peut faire cela de façon plus générale avec $a^2 - Kb^2$ si K n'est pas un carré (cela ajoute une dimension algébrique).

Une bijection Avoir en tête la bijection suivante :

$$\sigma : \begin{array}{ccc} \mathbb{N}^2 & \longrightarrow & \mathbb{N}^* \\ (m, n) & \longmapsto & (2m + 1)2^n \end{array}$$

En effet, on prouve qu'il s'agit d'une bijection en utilisant la valuations 2-adique.

Application. Montrer que

$$\forall z \in \mathbb{C},\ \sum_{k \in \mathbb{N}} \frac{z^{2^k}}{1 - z^{2^{k+1}}} = \frac{z}{1 - z}$$

On écrira le dénominateur comme la somme d'une famille, puis on appliquera le théorème sur les familles doubles. On conclura par changement d'indice avec la bijection sus-citée pour retrouver une série géométrique qui commence au rang 1.

2.3 Exercices classiques

Chapitre 3

Espaces vectoriels, dualité

3.1 Points méthode

Familles génératrices

Si $(x_i)_{i \in I}$ est une famille génératrice de E, une famille $(y_j)_{j \in J}$ de E est génératrice de E si, et seulement si, tous les x_i sont combinaison linéaire des y_j.

Décomposition d'un polynôme en u

Pour décomposer $v = P(u) \in \mathbb{K}[u]$, on détermine le reste de la division euclidienne de P pa le polynôme minimale de u. Par exemple, pour calculer les puissances successives de u, on peut déterminer le reste de la divison euclidienne de X^p, avec $p \in \mathbb{N}$, par le polynôme minimal de u.

Application. Calcul d'exponentielles d'endomorphismes.

3.2 Astuces

Astuce fondamentale de François Moulin, version endomorphismes Si on pense pouvoir faire un exercice en utilisant des endomorphismes, c'est qu'il faut utiliser des matrices carrées ! Du moins, il faut très rapidement passer du côté des matrices carrées et cela se déroule mieux en général. Évidemment, cela ne tient que pour quelque chose d'un peu abstrait.

Remarque. Attention, cette astuce et sa jumelle peuvent mener à des contradictions logiques majeures si on atteint le niveau de directement penser à changer de point de vue.

Application. Montrer que u est cyclique ssi $\forall \lambda,\ u - \lambda \mathrm{id}$ est cyclique. En effet, on a alors une matrice triangulaire supérieure avec uniquement des 1, ce qui est plutôt inversible donc on a bien une base. Remarquer qu'un sens se déduit de l'autre.

Base du sous-espace vectoriel engendré Si A est une partie de E, alors on peut extraire de A une base de $\mathrm{Vect}(A)$.

Dimension 1 et homothétie Une application linéaire dont l'espace de départ est de dimension un est nécessairement une homothétie.

Maximum de la dimension d'un SEV Quand on cherche la dimension maximale d'un sous-espace vectoriel V dont les vecteurs vérifient chacun une certaine propriété : on commence par majorer cette dimension, par exemple en exhibant un sous-espace A dont on connaît bien la dimension tel que $V \cap A = \{0\}$. On obtient donc

$$\dim(V) \leqslant \dim(E) - \dim(A)$$

Ensuite on exhibe un sous-espace V dont la dimension est précisément cette majoration, qui est donc atteinte !

Application. Dimension maximale d'un SEV de $\mathcal{M}_n(\mathbb{R})$ composé uniquement de matrices diagonalisables : penser au théorème spectral et s'intéresser à $A = \mathcal{A}_n(\mathbb{R})$.

Application. Dimension maximale d'un SEV de $\mathcal{M}_n(\mathbb{R})$ constitué de matrices nilpotentes ou quasi-nilpotentes : penser au fait qu'une matrice diagonalisable et nilpotente est nulle, et on peut prendre $A = \mathcal{S}_n(\mathbb{R})$.

Condition suffisante de non-somme directe Si on a deux sous-espaces vectoriels V_1 et V_2 de dimensions finies a et b, sous-espaces d'un même espace de dimension finie $n < a + b$, alors

$$V_1 \cap V_2 \neq 0$$

et l'intersection contient un élément non nul. On n'utilise pas la formule de Grassmann pour démontrer ceci, "la formule de Grassmann ne sert pas à ça" (François Moulin) : cette formule sert à calculer exactement la dimension d'une somme ou d'une intersection.

Utilisation de $\mathbb{Z}/2\mathbb{Z}$ Bien penser au fait que $(\mathbb{Z}/2\mathbb{Z})^n$ peut être vu comme un espace vectoriel de dimension n.

Application. Un sous-groupe d'ordre pair ($\forall x,\ x^2 = e$) est de cardinal 2^n pour un certain n. En effet, on peut le munir d'une structure de $\mathbb{Z}/2\mathbb{Z}$-ev, et il est alors de dimension finie car admet une famille génératrice finie. G est donc isomorphe à un $(\mathbb{Z}/2\mathbb{Z})^n$, ce qui conclut.

Image et noyau du carré Soit E un EV et u un endomorphisme de E. alors :

$$\begin{cases} \mathrm{Ker}(u) = \mathrm{Ker}(u^2) \iff \mathrm{Im}(u) \cap \mathrm{Ker}(u) = \{0\} \\ \mathrm{Im}(u) = \mathrm{Im}(u^2) \iff \mathrm{Im}(u) + \mathrm{Ker}(u) = E \end{cases}$$

En dimension finie, ces deux conditions sont équivalentes à $\mathrm{Im}(u) \oplus \mathrm{Ker}(u) = E$. Pour le prouver, utiliser des doubles inclusions à l'ancienne...

Application. Ce résultat est notamment utile pour les exercices sur les matrices du type $A^2B = BA$ ou autres...

Bidual Soit E un espace vectoriel. Pour $x \in E$, on définit la forme linéaire $\hat{x}$ sur E^* par $\hat{x}(\varphi) = \varphi(x)$. Alors, l'application :

$$\begin{array}{rccc} j: & E & \longrightarrow & (E^*)^* \\ & x & \longmapsto & \hat{x} \end{array}$$

est une application linéaire injective (l'injectivité utilise l'existence d'une base, et donc l'axiome du choix si on n'est pas en dimension finie). Par conséquent, si E est de dimension finie, j est un isomorphisme. Il y a donc un isomorphisme canonique entre E et son bidual en dimension finie.

Application (Base antéduale). Supposons E de dimension finie. Soit $\mathcal{L}$ une base de E^*. Posons $\mathcal{B}$ l'antécédent par j de sa base duale $\mathcal{L}^*$. Alors, $\mathcal{B}^* = \mathcal{L}$, on dit que $\mathcal{B}$ est la base antéduale de $\mathcal{L}$.

Orthogonalité On considère E un espace vectoriel de dimension finie n.

- Soit A une partie de E. On appelle orthogonal de A la partie de E^* constituée des formes linéaires nulles sur A :
$$A^T = \{\varphi \in E^* \ : \ \forall x \in A,\ \varphi(x) = 0\}$$
- Soit B une partie de E^*. On appelle orthogonal de B l'intersection des noyaux des éléments de B :
$$B_T = \{x \in E \ : \ \forall \varphi \in B,\ \varphi(x) = 0\}$$

Il pourrait donc y avoir une ambiguïté sur l'orthogonal d'une partie de E^*, car on pourrait prendre la première ou la deuxième définition. Mais ces deux se correspondent par le biais de l'isomorphisme j entre E et son bidual $(E^*)^*$. On a des propriétés (décroissance, SEV, égal à celui de son Vect) entièrement identiques à celles des orthogonaux pour les espaces euclidiens. On a aussi les complémentarités des dimensions, et, en dimension finie, si on on applique successivement les deux orthogonaux pour un SEV, on retombe sur l'ensemble de départ.

Utilisation de la trace avec les projecteurs Avec des projecteurs en dimension finie, penser à utiliser la trace : elle est égale au rang (donc est un entier), elle est linéaire, etc.

Trace dans $\mathbb{Z}$ En dimension finie, si on parle trace dans $\mathbb{Z}$, c'est qu'il y a une affaire de projecteurs et de symétries cachée.

Projecteurs et lemme des noyaux Les projecteurs associés à la décomposition du lemme des noyaux sont des polynômes en u.

3.3 Exercices classiques

Intégrité affaiblie sur les formes linéaires

Soit E un $\mathbb{K}$-espace vectoriel et $(f, g) \in (E^*)^2$ telles que

$$\forall x \in E,\ f(x)g(x) = 0$$

Montrer que $f = 0$ ou $g = 0$

Démonstration. Raisonner par l'absurde en considérant deux éléments x et y qui n'annulent pas respectivement f et g puis considérer leur somme. Raisonnons par l'absurde et fixons $x \in E$ tel que $f(x) \neq 0$ et $y \in E$ tel que $g(y) \neq 0$. Alors, par hypothèse, on a $g(x) = 0$ et $f(y) = 0$ par intégrité de $\mathbb{K}$. Puis par hypothèse et en vertu de ce qui précède :

$$\begin{aligned} f(x+y)g(x+y) &= f(x)g(x) + f(x)g(y) + f(y)g(x) + f(y)g(y) \\ &= f(x)g(y) \\ &= 0 \end{aligned}$$

Or $f(x) \neq 0$ et $g(y) \neq 0$ donc $f(x)g(y) \neq 0$ par intégrité de $\mathbb{K}$, ce qui est **absurde**. Ainsi, $f = 0$ ou $g = 0$. □

Noyaux et images itérés

On considère E un EV de dimension finie n et $u \in \mathcal{L}(E)$. pour $k \in \mathbb{N}$, on pose $N_k = \mathrm{Ker}(u^k)$ et $I_k = \mathrm{Im}(u^k)$ On dispose de pleins de résultats intéressants (décomposition de Fitting, suites stationnaires, etc.) mais le résultat qui sert le plus souvent est la concavité de la suite des dimensions des noyaux itérés, *ie* la décroissance de la suite d'entiers :

$$(\dim(N_{k+1}) - \dim(N_k))_{k \in \mathbb{N}}$$

Démonstration. On applique le théorème du rang aux restrictions de u à I_k et I_{k+1}. Cela donne :

$$\begin{cases} \dim(I_k) = \dim(I_{k+1}) + \dim(\mathrm{Ker}(u) \cap I_k) \\ \dim(I_{k+1}) = \dim(I_{k+2}) + \dim(\mathrm{Ker}(u) \cap I_{k+1}) \end{cases}$$

Et puisque $\mathrm{Ker}(u) \cap I_{k+1} \subset \mathrm{Ker}(u) \cap I_k$, on en déduit :

$$\dim(I_{k+1}) - \dim(I_{k+2}) \leqslant \dim(I_{k+1}) - \dim(I_k)$$

En appliquant le théorème du rang à u^k, u^{k+1} et u^{k+2}, on obtient finalement :

$$\dim(N_{k+2}) - \dim(N_{k+1}) \leqslant \dim(N_{k+1}) - \dim(N_k)$$

□

Application. Sert à démontrer des résultats sur les images itérées d'un endomorphisme nilpotent d'indice maximal.

Un lemme pour la dualité en dimension quelconque

Soit E un espace vectoriel de dimension quelconque. Une famille $(\varphi_1, \ldots, \varphi_p)$ de formes linéaires sur E est libre si, et seulement si, l'application linéaire :

$$\begin{array}{rccl} v : & E & \longrightarrow & \mathbb{K}^p \\ & x & \longmapsto & (\varphi_1(x), \ldots, \varphi_p(x)) \end{array}$$

est surjective. Ce résultat est extrêmement utile pour l'étude de la dualité en dimension infinie.

Démonstration. Si v est surjective, on fixe des x_j tels que $\varphi_i(x_j) = \delta_{i,j}$ puis on utilise la caractérisation des familles libres. Pour l'autre sens, on raisonne par contraposée. Si v n'est pas surjective, son image est incluse dans un hyperplan H de $\mathbb{K}^p$. On fixe une équation $\sum a_i y_i = 0$ de cette hyperplan (avec $(a_1, \ldots, a_p) \neq (0, \ldots, 0)$). Alors, on a la relation de liaison $\sum a_i \varphi_i = 0$, si bien que la famille est liée. □

Indépendance des formes linéaires

Soit $(\varphi, \varphi_1, \ldots, \varphi_n)$ des formes linéaires sur E (de dimension quelconque). Alors, on a le théorème d'indépendance des formes linéaires :

$$\bigcap_{i=1}^{n} \operatorname{Ker}(\varphi_i) \subset \operatorname{Ker}(\varphi) \iff \varphi \in \operatorname{Vect}(\varphi_1, \ldots, \varphi_n)$$

Démonstration. Le sens réciproque est trivial. Pour le sens direct, se réduire au cas d'une famille libre de formes linéaires puis utiliser le lemme pour la dualité en dimension quelconque (exercice précédent). □

Existence d'un supplémentaire commun en dimension finie

Soit E un espace de dimension finie et F et G deux sous-espaces vectoriels de E de même dimension. Montrer que F et G possèdent un supplémentaire commun.

Démonstration. Voici une méthode qui est faisable en sup :il y en probablement des meilleures mais je n'ai que celle-là sous la main quand j'écris.
Considérer l'ensemble des dimensions des sous-espaces vectoriels de E qui sont à la fois en somme directe avec F et G. Cet ensemble est non vide puisqu'il contient 0 car l'espace nul est en somme directe avec tous les espaces. Cet ensemble est évidemment majoré par la dimension de E. Enfin, c'est une partie de $\mathbb{N}$, donc on peut lui fixer un plus grand élément et à cet élément on peut associer un sous-espaces vectoriel V qui le réalise. Il faut désormais montrer que V est un supplémentaire de F et de G. Pour cela, on raisonne par l'absurde en utilisant le fait que l'union de deux sous-espaces vectoriels est un sous-espace vectoriel si, et seulement si, l'un est inclus dans l'autre. Puis on utilise le lemme d'adjonction, et on montre que les sommes de F et G avec le nouvel ensemble obtenu sont directes. Ceci est alors absurde par maximalité de la dimension de V. □

Propriété analogue à la dimension

Soit E un espace de dimension finie $n \geqslant 2$. On note

$$\mathcal{A} = \{F \text{ sev de } E\}$$

Déterminer toutes les fonctions $f : \mathcal{A} \longrightarrow \mathbb{R}$ telles que

$$\forall (V, W) \in \mathcal{A}^2,\ f(V + W) = f(V) + f(W) - f(V \cap W)$$

Démonstration. On peut déjà remarquer que la fonction dimension fonctionne d'après la formule de Grassmann. On raisonne par analyse-synthèse.

- **Analyse** : Soit f qui convienne. Dans un premier temps, on montre que toutes les droites vectorielles (c'est-à-dire les espaces vectoriels de dimension 1) ont la même image par f. Soit D_1 et D_2 deux droites vectorielles. On peut leur fixer un supplémentaire commun H (cf. exercice qui précède). On obtient alors immédiatement en utilisant l'hypothèse sur f avec $H \oplus D_1 = H \oplus D_2 = E$ que $f(D_1) = f(D_2)$ Posons désormais a l'image d'une droite vectorielle quelconque par f et b l'image de l'espace nul par f. Montrons par récurrence finie sur la dimension des sous-espaces qu'on a $f = (a_b)\dim + b$.
  - Initialisations (rang 0 et 1) : Immédiat par définition de a et b.
  - Hérédité : Soit $n \geqslant m \geqslant 2$ tel que pour tout $k \leqslant m-1$, on ait l'égalité souhaitée pour les sous-espaces de dimension k. Soit F un sous-espace de E de dimension m. On peut fixer x un élément non nul de F et considérer D la droite vectoriel engendrée par x. On peut alors fixer H un hyperplan de F tel que $F = H \oplus D$. On a alors par hypothèse de récurrence :

$$\begin{aligned} f(F) &= f(H) + f(D) - f(\{0_E\}) \\ &= (a-b)(m-1) + b + a - b \\ &= (a-b)m + b \\ &= (a-b)\dim(F) + b \end{aligned}$$

  ce qui achève la récurrence. Ainsi, si f convient, alors il existe des constantes réelles λ et μ telles que $f = \lambda \dim + \mu$.
- **Synthèse** : Réciproquement, on vérifie immédiatement qu'une telle fonction convient.

□

Union finie de SEV stricts

Soit E un $\mathbb{K}$-espace vectoriel où $\mathbb{K}$ est un corps de caractéristique nulle.

1. Montrer que si F et G sont deux SEV stricts de E, alors il existe un vecteur de E n'appartenant ni à F ni à G.
2. Et pour $n \geqslant 2$ SEV ?

Démonstration. Le premier cas se fait facilement, mais le deuxième est plus complexe.

1. Si $F \subset G$ ou $G \subset F$, le résultat est immédiat. Sinon, on prend $x \in F \setminus G$ et $y \in G \setminus F$. Alors $x+y$ ne peut pas être dans F sans quoi, par différence, y appartiendrait à F. De même, $x+y$ ne peut appartenir à G sans quoi, par différence, x appartiendrait à G. Donc $x+y$ n'appartient ni à F ni à G.
2. On se donne $F_1, \ldots, F_n$ des SEV stricts de E. Sans perte de généralité, quitta à supprimer certains F_i, on peut supposer qu'aucun F_i n'est pas inclus dans la réunion des autres F_j pour $j \neq i$. On prend alors pour tout i un $x_i \in F_i$ qui n'est dans aucun F_j pour $j \neq i$. On note D la droite affine passant par x_1 et x_2. Comme $x_2 \notin F_1$ et $x_1 \in F_1$, D ne rencontre F_1 qu'en x_1. Soit $i \geqslant 2$. Alors D n'est pas incluse dans F_i car D contient x_1 qui n'appartient pas à F_i. Donc $D \cap F_i$ est vide ou réduite à un singleton. Par conséquent, $D \cap \left(\bigcup_{i=1}^{n} F_i \right)$ est finie. Or,

D est infinie car $\mathbb{K}$ est infini (car de caractéristique nulle). Donc $\bigcup_{i=1}^{n} F_i$ ne recouvre pas E.

$\square$

Liberté d'une famille de ln

Montrer que la famille des

$$f_a : \begin{array}{ccc} \mathbb{R}_+ & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \ln(x+a) \end{array}$$

pour $a >$ à est libre.

Démonstration. Prendre une combinaison linéaire nulle et dériver. Utiliser ensuite le fait que la famille des

$$\frac{1}{X+a}$$

pour $a > 0$ est libre comme sous-famille de la base canonique de $\mathbb{R}(X)$ (théorème de décomposition en éléments simples). $\square$

Famille libres des espaces de dimension dénombrable

1. Soit E un espace vectoriel muni d'une base dénombrable $(e_n)_{n\in\mathbb{N}}$. Montrer que toute famille libre de E est au plus dénombrable.
2. Les espaces vectoriels $\mathbb{C}[X]$ et $\mathbb{C}(X)$ sont-ils isomorphes ?

Démonstration.

1. On considère $(x_i)_{i\in I}$ une famille libre de E. On note :

$$\forall n \in \mathbb{N},\ E_n = \text{Vect}(e_0, \dots, e_n)$$

Ensuite, on pose :

$$\forall n \in \mathbb{N},\ I_n = \{i \in I \mid x_i \in E_n\}$$

La liberté de $(x_i)_{i\in I}$ impose que chaque I_n est fini. or, on vérifie aisément que

$$I = \bigcup_{n\in\mathbb{N}} I_n$$

Donc, en tant que réunion au plus dénombrable d'ensembles finis, I est au plus dénombrable.

2. Par indénombrabilité de $\mathbb{R}$, la famille

$$\left(\frac{1}{X+a}\right)_{a\in\mathbb{R}}$$

est une famille libre (théorème de décomposition en éléments simples) indénombrable. Donc $\mathbb{C}[X]$ n'est pas de dimension dénombrable d'après la question précédente. Or, $\mathbb{C}[X]$ n'est clairement pas de dimension finie donc $\mathbb{C}[X]$ est de dimension indénombrable. Comme $\mathbb{C}[X]$ est de dimension dénombrable, on en déduit que $\mathbb{C}[X]$ et $\mathbb{C}[X]$ ne sont pas isomorphes.

$\square$

Lemme de Dedekind

Soit G un groupe multiplicatif et Σ l'ensemble des morphismes de G dans $(\mathbb{C}^*, \times)$. Montrer que Σ est une famille libre de $\mathbb{C}^G$. Que peut-on en déduire sur $\mathrm{Card}(\Sigma)$ si G est fini ?

Démonstration. Procéder par récurrence sur le nombre de morphismes. Dans la récurrence, multiplier par le nouveau morphisme, mais utiliser aussi la nouvelle propriété de morphisme. On obtient :

$$\forall (g, g') \in G^2,\ \sum_{i=1}^{n} \lambda_i f_i(g) \left[f_i(g') - f_0(g') \right] = 0$$

d'où on tire

$$\forall g' \in G,\ \sum_{i=1}^{n} \lambda_i \left[f_i(g') - f_0(g') \right] f_i = 0$$

Or, on a pris les f_i distincts, donc on peut trouver g' tel que $f_i(g') - f_0(g') \neq 0$. On utilise alors l'hypothèse de récurrence et on se ramène à $\lambda_0 f_0 = 0$ ce qui est l'initialisation (immédiate en évaluant en e élément neutre de G). Lorsque G est fini, $\mathbb{C}^G$ est de dimension finie égale à $\mathrm{Card}(G)$ puisque $(x \mapsto \delta_{g,x})_{g \in G}$ en est une base par exemple. Donc on en déduit que

$$\mathrm{Card}(\Sigma) \leqslant \mathrm{Card}(G)$$

□

Famille de réels sur $\mathbb{R}$ en tant que $\mathbb{Q}$-ev

On considère $\mathbb{R}$ en tant que $\mathbb{Q}$-espace vectoriel.

1. La famille $(\ln(n))_{n \geqslant 2}$ est-elle libre ?
2. La famille $(\ln(p))_{p \text{ premier}}$ est-elle libre ?

Démonstration.

1. La réponse est non puisque par exemple $\ln(4) = 2\ln(2)$ et 2 est non nul.
2. La réponse est oui. Écrire tous les scalaires de la relation de liaison sous forme irréductible et tout multiplier par le PPCM des scalaires. Séparer en les entiers positifs et négatifs. Passer à l'exponentielle et utiliser l'unicité de la DFP.

□

Dimension et surcorps : multiplicativité des degrés

Soit $\mathbb{L}$ un surcorps de $\mathbb{K}$ de dimension p sur $\mathbb{K}$. Soit E un $\mathbb{L}$-espace vectoriel (qui est donc aussi un $\mathbb{K}$-espace vectoriel). Montrer que E est de dimension finie sur $\mathbb{K}$ si, et seulement si, E est de dimension finie sur $\mathbb{L}$. Donner alors une relation entre ces deux dimensions.

Démonstration. Un exemple non trivial de tels corps peut être donné par $\mathbb{R}$ et $\mathbb{C}$. Dans le sens direct, une base de E comme $\mathbb{K}$-ev est alors génératrice d E en tant que $\mathbb{L}$-ev car tout scalaire de $\mathbb{K}$ est un scalaire de $\mathbb{L}$. Donc OK. Réciproquement, il faut multiplier une base de E en tant que

$\mathbb{L}$-ev par une base de $\mathbb{L}$ en tant que $\mathbb{K}$-ev. On vérifie alors qu'on obtient une base de E en tant que $\mathbb{K}$-ev. On en déduit alors que :

$$\dim_{\mathbb{K}}(E) = \dim_{\mathbb{K}}(\mathbb{L}) \times \dim_{\mathbb{L}}(E)$$

$\square$

Tous les supplémentaires d'un même SEV sont isomorphes

Soit F un SEV de E. Montrer que tous les supplémentaires de F dans E sont isomorphes.

Démonstration. On fixe G un supplémentaire de F dans E et on se donne H un supplémentaire de F dans E quelconque. On note p le projecteur sur G parallèlement à F. Puisque H est un supplémentaire de $F = \mathrm{Ker}(p)$, alors H et $G = \mathrm{Im}(p)$ sont isomorphes en vertu du théorème du rang géométrique. $\square$

Supplémentaire commun à un nombre fini de SEV de même dimension

Montrer que m SEV $F_1, \ldots, F_m$ de même dimension k de E de dimension finie n admettent un supplémentaire commun.

Démonstration. Procéder par récurrence descendante sur k. Pour l'initialisation, prendre pour supplémentaire $\{0\}$. Pour l'hérédité, considérer un vecteur y qui n'appartient par à la réunion des F_i (possible d'après un exercice précédent), puis ajouter aux F_i la droite $\mathbb{K}y$. Appliquer l'hypothèse de récurrence aux $F_i \oplus \mathbb{K}y$ et conclure par associativité de la somme directe. $\square$

CNS pour avoir égalité entre Ker(u) et Im(u)

Soit E un espace vectoriel de dimension finie. CNS pour qu'il existe $u \in \mathcal{L}(E)$ tel que $\mathrm{Ker}(u) = \mathrm{Im}(u)$?

Démonstration. D'après le théorème du rang, il est nécessaire que $\dim(E)$ soit pair. Réciproquement, prendre une base de taille paire puis envoyer les impairs sur 0 et les pairs sur l'impair qui précède. $\square$

Inégalité de Frobenius

Soit $u \in \mathcal{L}(E, F)$, $v \in \mathcal{L}(F, G)$ et $w \in \mathcal{L}(G, H)$ où E, F, G et H sont de dimension finie. Montrer que

$$\mathrm{rg}(v \circ u) + \mathrm{rg}(w \circ v) \leqslant \mathrm{rg}(v) + \mathrm{rg}(w \circ v \circ u)$$

Démonstration. Appliquer le théorème du rang aux restrictions de w à $\mathrm{Im}(v)$ et $\mathrm{Im}(v \circ u)$ puis sommer les deux relations obtenues. Observer ensuite que

$$\mathrm{Ker}(w_{|\mathrm{Im}(v \circ u)}) \subset \mathrm{Ker}(w_{|\mathrm{Im}(v)})$$

$\square$

Application. Permet de retrouver la concavité de la suite des noyaux itérés en dimension finie.

Un classique sur la commutation et les polynômes

Soit E un espace vectoriel de dimension finie $n+1$ et $u \in \mathcal{L}(E)$. On suppose qu'il existe $a \in E$ tel que $\left(u^k(a)\right)_{0 \leqslant k \leqslant n}$ soit une base de E.

1. Donner un exemple d'un tel endomorphisme.
2. Soit $v \in \mathcal{L}(E)$ tel que $v \circ u = u \circ v$. Montrer que v est un polynôme en u.

Démonstration. 1. Tout endomorphisme nilpotent d'indice de nilpotence maximal convient. On peut en expliciter un en envoyant tous les vecteurs d'une base sur le suivant, et en envoyant le dernier sur 0.

2. On peut écrire :

$$v(a) = \sum_{k=0}^{n} \lambda_k u^k(a)$$

On montre alors que

$$v = \sum_{k=0}^{n} \lambda_k u^k$$

en montrant que ces deux applications linéaires coïncident sur la base $\left(u^k(a)\right)_{0 \leqslant k \leqslant n}$ grâce à la commutation.

□

CNS pour que le rang de la somme soit la somme des rang

Soient u et v deux endomorphismes d'un espace vectoriel E de dimension finie. Montrer l'équivalence entre les deux conditions suivantes :

1. $\operatorname{rg}(u+v) = \operatorname{rg}(u) + \operatorname{rg}(v)$
2. $\operatorname{Im}(u) \cap \operatorname{Im}(v) = \{0\}$ et $\operatorname{Ker}(u) + \operatorname{Ker}(v) = E$

Démonstration. Utiliser l'inégalité

$$\operatorname{rg}(u+v) \leqslant \operatorname{rg}(u) + \operatorname{rg}(v) - \dim\left(\operatorname{Im}(u) \cap \operatorname{Im}(v)\right) \leqslant \operatorname{rg}(u) + \operatorname{rg}(v)$$

C'est moche comme tout, mais ça se fait. Dans le sens direct, on obtiendra

$$\dim(\operatorname{Ker}(u) + \operatorname{Ker}(v)) \geqslant \dim(E)$$

Dans le sens réciproque, on montrera que

$$\operatorname{Im}(u+v) = \operatorname{Im}(u) + \operatorname{Im}(v)$$

L'inclusion réciproque viendra du fait que $E = \operatorname{Ker}(u) + \operatorname{Ker}(v)$. On conclura en utilisant la formule de Grassmann. □

CNS de commutation avec un projecteur

Soit p un projecteur d'un espace vectoriel E. Montrer qu'un endomorphisme u de E commute avec p si, et seulement si, il laisse stable le noyau et l'image de p.

Démonstration. En réalité, il s'agit là de résultats de réduction. Le sens direct est immédiat (c'est même du cours en réduction). Réciproquement, décomposer $x \in E$ sur $\text{Ker}(p) \oplus \text{Im}(p)$ en $x = a + b$ et calculer $u(p(x))$ et $p(u(x))$. On obtient dans les deux cas $u(b)$. □

Nouveau projecteur

Soit p et q deux projecteurs d'un espace vectoriel E tels que $\text{Im}(p) \subset \text{Ker}(q)$. Montrer que

$$r = p + q - p \circ q$$

est un projecteur. Montrer que

$$\begin{cases} \text{Im}(r) = \text{Im}(p) \cap \text{Im}(q) \\ \text{Ker}(r) = \text{Ker}(p) + \text{Ker}(q) \end{cases}$$

Démonstration. Calculer r^2 et utiliser le fait que $q \circ p = 0$. On trouve bien $r^2 = r$. Montrer ensuite à la main toutes les inclusions qu'il faut (c'est long et embêtant). □

CNS pour qu'une somme de projecteurs soit un projecteur

Soit $p_1, \ldots, p_r$ des projecteurs d'un espace vectoriel E de dimension finie. Montrer que $p = p_1 + \ldots + p_r$ est un projecteur si, et seulement si,

$$\forall i \neq j,\ p_i \circ p_j = 0$$

On montrera que l'image de p est la somme directe des images des p_i.

Démonstration. Le sens réciproque est immédiat. pour le sens direct, utiliser la trace (qui est égale au rang pour des projecteurs), ce qui permet d'obtenir par linéarité de la trace :

$$\text{rg}(p) = \sum_{i=1}^{n} \text{rg}(p_i)$$

On en déduit que les images des p_i sont en somme directe et que

$$\text{Im}(p) = \bigoplus_{i=1}^{n} \text{Im}(p_i)$$

On remarque ensuite grâce à cette égalité que $p \circ p_i = p_i$ et on écrit pour tout $x \in E$, par définition de p :

$$p_i(x) = p_i(x) + \sum_{j \neq i} \underbrace{p_j \circ p_i(x)}_{\in \text{Im}(p_j)}$$

Puisque la somme est direct, on en déduit que $p_j \circ p_i(x) = 0$ et donc $p_j \circ p_i = 0$, ceci valant pour tout $x \in E$. □

Une somme irrationnelle de projecteurs

Soit p, q et r trois projecteurs d'un $\mathbb{R}$-espace vectoriel de dimension finie. On suppose que $p + \sqrt{2}q + \sqrt{3}r = 0$. Montrer que $q = r = 0$.

Démonstration. En dimension finie, la trac d'un projecteur est égale à son rang. On passe à la trace. Tout revient alors à prouver que la famille $(1, \sqrt{2}, \sqrt{3})$ est $\mathbb{Q}$-libre. Pour cela, élever une relation de liaison au carré et utiliser le fait que $\sqrt{2}$ est irrationnel (savoir redémontrer ce fait rapidement avec des valuations 2-adiques). □

Somme nulle de trois projecteurs

Soit p, q et r trois projecteurs d'un espace vectoriel E sur un corps de caractéristique différente de 2 et de 3. On suppose que $p + q + r = 0$. Montrer que $p = q = r = 0$.

Démonstration. Premièrement, on montre que

$$\mathrm{Im}(p) \cap \mathrm{Im}(q) \cap \mathrm{Im}(r) = \{0\}$$

en utilisant le fait que la caractéristique est différente de 3. Ensuite, on prouve que

$$\mathrm{Im}(p) \cap \mathrm{Im}(q) \subset \mathrm{Im}(r)$$

en utilisant le fait que la caractéristique est différente de 2. On a de même les inclusions symétriques. On en déduit que

$$\mathrm{Im}(p) \cap \mathrm{Im}(q) = \mathrm{Im}(p) \cap \mathrm{Im}(r) = \mathrm{Im}(q) \cap \mathrm{Im}(r) = \{0\}$$

Soit $x \in \mathrm{Ker}(r)$. Alors $p(x) = q(-x) \in \mathrm{Im}(p) \cap \mathrm{Im}(q)$ donc

$$\mathrm{Ker}(r) \subset \mathrm{Ker}(p) \quad \text{et} \quad \mathrm{Ker}(r) \subset \mathrm{Ker}(q)$$

On a de même les inclusions symétriques, dont on déduit :

$$\mathrm{Ker}(p) = \mathrm{Ker}(q) = \mathrm{Ker}(r)$$

Enfin, soit $x \in E$ qu'on décompose comme $a_1 + b_1$ selon p, $a_2 + b_2$ selon q et $a_3 + b_3$ selon r. On a alors $a_1 + a_2 + a_3 = 0$ par hypothèse donc $3.x = b_1 + b_2 + b_3$. L'égalité des noyaux fournit alors :

$$3.p(x) = 3.q(x) = 3.r(x) = 0$$

On conclut en utilisant le fait que E n'est pas de caractéristique 3. □

Chapitre 4

Polynômes, fractions rationnelles

4.1 Points méthode

4.2 Astuces

Structure de corps de $\mathbb{K}(X)$ Lorsque $\mathbb{K}$ est un corps, $\mathbb{K}(X)$ en est un aussi.

Une méthode pour montrer qu'un polynôme est scindé à racines simples Pour montrer qu'un polynôme est scindé à racines simples, on peut considérer ses racines de multiplicité impaire et montrer que la multiplicité vaut 1, puis montrer qu'il n'y a pas de racine de multiplicité paire.

Différentes formes d'un polynôme de $\mathbb{C}[X]$ Il y a deux façons complètement différentes de voir un polynôme de $\mathbb{C}[X]$:

- son écriture développée avec des coefficients ;
- sa forme factorisée avec le coefficients dominant et les racines.

Il faut impérativement jongler entre ces deux visions, cela permet d'avoir de nouveaux angles d'attaque.

Calcul d'un produit fini, ou plus généralement d'une somme de produits finis Penser à utiliser les formules de Viète pour les racines d'un polynôme pour calculer des produits finis ou des sommes de produits finis. Cela n'a d'intérêt que si le polynôme en question est simple.

Application. Montrer que

$$\forall n \in \mathbb{N}^*, \prod_{k=1}^{n-1} \sin\left(\frac{k}{n}\pi\right) = n2^{n-1}$$

Pour cela, considérer les racines du polynôme

$$\frac{(X+1)^n - 1}{X}$$

Coefficients inversés L'opération pour inverser les coefficients d'un polynôme P est

$$X^n P\left(\frac{1}{X}\right)$$

En jouant avec le forme factorisée, on remarque qu'inverser l'ordre des coefficients du polynôme revient à inverser ses racines.

Remarque. L'application :

$$P \mapsto X^n P\left(\frac{1}{C}\right)$$

est une symétrie de $\mathbb{K}_n[X]$.

Méthode de travail dans $\mathbb{Z}/p\mathbb{Z}[X]$ Soit p un nombre premier. Pour travailler dans $\mathbb{Z}/p\mathbb{Z}[X]$, on utilise des propriétés d'arithmétique pour montrer un résultat sur les entiers n modulo p, et on en déduit le résultat souhaité sur les polynômes (on remplace successivement X par tous les entiers modulo p et on vérifie que c'est toujours vrai).

Application. D'après le petit théorème de Fermat, on a :

$$\forall x \in \mathbb{Z}/p\mathbb{Z},\ x^p = x$$

On en déduit, dans $\mathbb{Z}/p\mathbb{Z}[X]$:

$$X^p - X = \overline{0} = X(X - \overline{1}) \times \ldots \times (X - \overline{p-1})$$

Ainsi, $A \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})$ est diagonalisable si, et seulement si, $A^p = A$ car elle est diagonalisable si, et seulement si, elle est annulée par un polynôme scindé à racines simples. (**VERIFIER CE RESULTAT**)

Racines dans $\mathbb{Q}$ **ou non** Si on veut étudier le caractère rationnel des racines de

$$P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$$

avec $a_n \neq 0$, on suppose que $\alpha = \dfrac{p}{q}$ avec $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ et $p \wedge q = 1$ est racine de P. On écrit alors :

$$\sum_{k=0}^{n} a_k \left(\frac{p}{q}\right) = P(\alpha) = 0$$

On multiplie alors par q^n puis on utilise la divisibilité par p et le lemme de Gauss. Par exemple, une telle racine rationnelle doit vérifier :

$$\begin{cases} p \mid a_0 \\ q \mid a_n \end{cases}$$

Application. Pour montrer que $\sqrt{2}$ est irrationnel, on peut montrer que $X^2 - 2$ est irréductible dans $\mathbb{Q}[X]$ en prouvant qu'il n'admet pas de racine rationnelle avec la méthode précédent. En effet, on rappelle qu'un **polynôme de degré 2 ou 3 est irréductible si, et seulement si, il n'admet pas de racine dans le corps de base, et ce quel que soit le corps considéré**.

Application. Permet de deviner que $1/2$ peut être racine de $1 - X - X^2 - 2^3$, ce qu'il faut ensuite vérifier.

Utilisation de la forme P'/P Si $P = \prod(X-\lambda)^\alpha$, alors :

$$\frac{P'}{P} = \sum \frac{\alpha}{X-\lambda}$$

Cette formule peut permettre d'évaluer rapidement $P'(x)$. On peut d'ailleurs encore dériver pour obtenir une expression plus sale avec P''. Dans les cas où P est assez simple, cette méthode aide grandement.

Application. Polynômes de Hilbert : $P = \binom{X}{n} = \dfrac{X(X-1)\dots(X-n+1)}{n!}$

Application. En probabilités, sert pour calculer l'espérance et la variance à partir de la fonction génératrice.

Travail avec des fractions rationnelles Quand on travaille avec des fractions rationnelles, essayer de se ramener le plus vite possible à des polynômes, sur lesquels on a plus de propriétés. Notamment, si on a

$$F(X) = \frac{A(X)}{B(X)}$$

avec A et B des polynômes, il faut souvent commencer par écrire A(X) = F (X)B(X) et éventuellement utiliser l'expression des coefficients d'un produit de Cauchy.

4.3 Exercices classiques

Restes de divisons euclidiennes

Soit $P \in \mathbb{K}[X]$ et $(a,b) \in \mathbb{K}^2$ distincts.

1. Déterminer le reste de la division euclidienne de P par $(X-a)(X-b)$
2. Déterminer le reste de la division euclidienne de P par $(X-a)^2$

Démonstration. Quel est le degré du reste ? Utiliser des évaluations précises et/ou la dérivation suivie d'une évaluation. Ne pas tenter l'algorithme sur un polynôme quelconque dans un corps quelconque !!! On va plutôt utiliser le fait que le reste est à chaque fois de la forme $\lambda X + \mu$ avec $(\lambda,\mu) \in \mathbb{K}^2$.

1. On peut fixer $Q \in \mathbb{K}[X]$ tel que $P = (X-a)(X-b)Q + (\lambda X + \mu)$. En évaluant en a et en b, on obtient $\lambda a + \mu = P(a)$ et $\lambda b + \mu = P(b)$. De simples combinaisons linéaires permettent de conclure.
2. Là encore, on peut fixer $Q \in \mathbb{K}[X]$ tel que $P = (X-a)^2Q + (\lambda X + \mu)$. Toutefois, on ne peut plus réaliser deux évaluations. Cependant, une évaluation en a fournit déjà

$\square$

Pas de racine multiple

Soit $n \geq 2$ un entier naturel. On considère le polynôme

$$P = \sum_{k=0}^{n} \frac{X^k}{k!}$$

Le polynôme P admet-il une racine multiple ?

Démonstration. La réponse est non. Pour le prouver, raisonner par l'absurde et considérer une racine multiple z de P. Par caractérisation de la multiplicité des racines, z est racine de P'. Or, on a immédiatement :

$$P' = \sum_{k=0}^{n-1} \frac{X^k}{k!}$$

En soustrayant les égalités $P(z) = 0$ et $P'(z) = 0$, on obtient que $\dfrac{z^n}{n!} = 0$. Par intégrité de $\mathbb{C}$, $z = 0$. Or, z n'est clairement pas racine de P car $P(0) = 1$. Donc 0 n'est même pas racine mais est racine multiple, ce qui est **absurde**. Ainsi, pas de racine multiple pour P. On remarquera que cet exercice fonctionne car $n \geq 2$ donc $n - 1 \geq 1$ donc on a le "droit" à P' quand on applique la caractérisation de la multiplicité des racines. $\square$

P scindé sur $\mathbb{R} \Longrightarrow P'$ scindé sur $\mathbb{R}$

Soit $P \in \mathbb{R}[X]$ un polynôme scindé.

1. Supposons que P est à racines simples. Montrer que P' est scindé.
2. Le résultat est-il toujours valable lorsque les racines de P ne sont plus nécessairement simples ?

Démonstration. Le maître mot : théorème de Rolle.

1. Ordonner les racines de P et utiliser le théorème de Rolle entre deux racines successives de P.
2. Réutiliser l'idée précédente en faisant attention à la multiplicité potentielle des racines.Le résultat reste valable.

$\square$

Coefficients rationnels

Soit $P \in \mathbb{C}[X]$ tel que $\forall x \in \mathbb{Q},\ P(x) \in \mathbb{Q}$. Montrer que P est à coefficients rationnels.

Démonstration. Considérer n le degré du polynôme puis utiliser les polynômes interpolateurs de Lagrange. associés à $1, \ldots, n$. $\square$

Irréductible sur $\mathbb{Q}$ implique racines simples

Soit $P \in \mathbb{Q}[X]$ irréductible et a une racine complexe de P. Montrer que a est racine simple de P.

Démonstration. Puisque P est irréductible, $P \wedge P' = 1$ puisque cette quantité doit être unitaire, diviser P et $\deg(P') < \deg(P)$. Par conséquent, $X - a$ ne divise pas P' est a est racine simple de P par théorème de cours. ☐

Conséquence de l'exercice précédent

Soit $P \in \mathbb{Q}[X]$ de degré 5. Supposons que P admette une racine double a complexe. Montrer que P possède une racine dans $\mathbb{Q}$.

Démonstration. Par contraposée de l'exercice précédent, P n'est pas irréductible et on peut l'écrire sous la forme $P = QR$. SPG, on peut supposer P, Q et R unitaires. Si Q ou R est de degré 1, il n'y a rien à prouver, donc on peut supposer par l'absurde Q et R de degré supérieur à 1 et irréductibles. Ensuite, puisque $Q \neq R$ comme $\deg(P) = 5$, Q et R sont premiers entre eux car leur PGCD vaut 1, Q ou R. Mais si $\deg(Q) = 2$, comme Q et R sont irréductibles, d'après l'exercice précédent, on a nécessairement $Q(a) = R(a) = 0$ ce qui est absurde. Cela est aussi absurde si $\deg(Q) = 3$ car on a alors $\deg(R) = 2$. ☐

Polynômes à valeurs dans les nombres premiers

On note $\mathcal{P}$ l'ensemble des nombres premiers. Trouver tous les polynômes $A \in \mathbb{Z}[X]$ tels que $\forall n \in \mathbb{N},\ A(n) \in \mathcal{P}$.

Démonstration. Utiliser l'astuce classique pour les polynômes Q à coefficients dans $\mathbb{Z}$: pour tous a et b entiers, $b - a$ divise $Q(b) - Q(a)$. On montre par analyse-synthèse que seuls les polynômes constants égaux à des nombre premiers conviennent.

- **Analyse** : Soit A qui convienne et on pose $p = A(0)$. Soit $n \in \mathbb{N}^*$. En vertu de la remarque introductive, on sait que $np - 0$ divise $A(np) - A(0) = A(np) - p$. Ainsi, on peut fixer m dans $\mathbb{Z}$ tel que $A(np) - p = mnp$. Puis on obtient, $A(np) = (mn + 1)p$ donc p divise $A(np)$. Or, $A(np) \in \mathcal{P}$, donc nécessairement, $A(np) = p$. La suite $(np)_{n\in\mathbb{N}}$ étant injective, A et le polynôme constant égal à p coïncident en une infinité de points et sont donc égaux.
- **Synthèse** : Réciproquement, pour tout nombre premier p, le polynôme contant égal à p convient.

☐

Lemme d'Eisenstein

Soit p un nombre premier et $P \in \mathbb{Z}[X]$ **unitaire** qu'on écrit sous la forme

$$P = \sum_{k=0}^{n} a_k X^k$$

Supposons que l'on ait :

- $\forall k \in [\![0, n-1]\!],\ p \mid a_k$;
- $p^2 \nmid a_0$.

Alors P est irréductible dans $\mathbb{Z}[X]$.

Démonstration. Supposons par l'absurde que P puisse s'écrire sous la forme $P = AB$ avec A et B des polynômes non constants à coefficients entiers. On passe au quotient et on se place dans $\mathbb{Z}/p\mathbb{Z}[X]$. $\mathbb{Z}/p\mathbb{Z}[X]$ est un anneau intègre puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps. Or, on a :

$$X^n = \overline{P} = \overline{A} \times \overline{B}$$

puisque p divise les coefficients de P qui ne correspondent pas au terme de degré N. Par conséquent, on a $\overline{A} = X^i$ et $\overline{B} = X^j$ avec $i + j = n$ ainsi que $i \geqslant 1$ et $j \geqslant 1$. Ainsi, les coefficients de degré 0 de A et de B sont divisibles par p. Or, le coefficient de degré 0 de P est égal au produit de celui de A par celui de B. Par conséquent, $p^2 \mid a_0$, ce qui est absurde. $\square$

Contenu

Soit $A \in \mathbb{Z}[X]$ et $B \in \mathbb{Z}[X]$. On note respectivement $C(A)$ et $C(B)$ les PGCD des coefficients de A et de B, appelés **contenus** des polynômes A et B. Alors :

$$C(AB) = C(A)C(B)$$

Démonstration. On procède en deux étapes.

- Supposons $C(A) = C(B) = 1$. Par l'absurde, supposons $C(AB) \neq 1$. Prenons alors p un nombre premier qui divise $C(AB)$. Alors, en passant au quotient dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a $\overline{0} = \overline{AB} = \overline{A} \times \overline{B}$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre donc $\overline{A} = \overline{0}$ ou $\overline{B} = \overline{0}$, et donc p divise $C(A)$ ou $C(B)$, ce qui est absurde. Donc $C(AB) = 1$.
- Dans le cas général, on écrit $A = C(A)A'$ et $B = C(B)B'$ avec $C(A') = C(B') = 1$ (en effet, $C(nP) = |n|C(P)$). Alors, par le cas précédent :

$$C(AB) = C\big(C(A)C(B)A'B'\big) = C(A)C(B)C(A'B') = C(A)C(B)$$

$\square$

CNS pour être scindé sur $\mathbb{R}$

Soit $P \in \mathbb{R}[X]$ unitaire de degré $n \geqslant 1$. Alors, P est scindé sur $\mathbb{R}$ si, et seulement si,

$$\forall z \in \mathbb{C},\ |P(z)| \geqslant |\mathrm{Im}(z)|^n$$

Démonstration. On procède par double implication :

- Sens direct : si P est scindé sur $\mathbb{R}$, on écrit
$$P = \prod_{k=1}^{n} (X - \lambda_k)$$
Alors pour tout $z \in \mathbb{C}$:
$$|P(z)| = \prod_{k=1}^{n} |z - \lambda_k| \geqslant \prod_{k=1}^{n} |\mathrm{Im}(z - \lambda_k)| = \prod_{k=1}^{n} |\mathrm{Im}(z)| = |\mathrm{Im}(z)|^n$$
- Sens réciproque : notons λ_k les racines *a priori* complexes de P après l'avoir scindé sur $\mathbb{C}$. On a alors :
$$|\mathrm{Im}(\lambda_k)|^n \leqslant |P(\lambda_k)| = 0$$
Puisque $n \geqslant 1$, on en déduit que $\mathrm{Im}(\lambda_k) = 0$ et donc que $\lambda_k \in \mathbb{R}$, si bien que P est scindé sur $\mathbb{R}$.

□

Caractérisation d'un corps par la principalité de son anneau de polynômes

Soit A un anneau. Montrer que A est un corps si, et seulement si, $A[X]$ est principal.

Démonstration. Les sens direct est un théorème de cours. Réciproquement, supposons que $A[X]$ soit principal. Il ne nous reste plus qu'à montrer l'inversibilité des éléments non nuls. Soit $a \in A \setminus \{0\}$. On considère I l'idéal engendré par a et X. Alors il existe $P \neq 0$ tel que $I = P \times A[X]$. Puisque $a \in I$, $P \mid a$ donc P constant et, abusivement, $P = p \in A$. De plus, puisque $X \in I$, on en déduit que $P \mid X$. Par conséquent, il existe $Q \in A[X]$, de coefficient dominant $q \in A$ tel que $PQ = X$. En passant aux coefficients dominants, on obtient $pq = 1$ et p est inversible. Or, de même, il existe b tel que $a = pb$. Or, P est constant et appartient à I, donc il existe $c \in A$ tel que $P = p = ac$. On en déduit que $p = pbc$ donc b et c sont inversibles. Par conséquent, $a = pb$ est inversible comme produit d'inversibles. □

Cyclicité de $\mathbb{Z}/p\mathbb{Z}^*$

Soit p un nombre premier. Montrer que $\mathbb{Z}/p\mathbb{Z}^*$ est un groupe cyclique.

Démonstration. □

Chapitre 5

Matrices, déterminants

5.1 Points méthode

Multiplication par une matrice diagonale

Multiplier une matrice M à gauche par une matrice diagonale revient à multiplier les lignes de M par les scalaires de la diagonale. Multiplier une matrice M à droite par une matrice diagonale revient à multiplier les colonnes par les scalaires de la diagonale.

Changement de base

En notant $P = M_{\mathcal{B}}(\mathcal{B}') = M_{\mathcal{B}',\mathcal{B}}(\mathrm{id})$, on a :

$$X = PX'$$

Si de plus on considère $A = M_{\mathcal{B},\mathcal{C}}(u)$, $A' = M_{\mathcal{B}',\mathcal{C}'}(u)$ et $Q = M_{\mathcal{C}}(\mathcal{C}')$, on a alors :

$$A' = Q^{-1}AP$$

Système linéaire et inverse (1)

Pour montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est inversible et calculer son inverse, on peut résoudre le système $AX = Y$ en le ramenant à un système triangulaire par l'algorithme du pivot de Gauss. L'expression de X en fonction de Y donne alors la matrice A^{-1}.

Système linéaire et inverse (2)

Si, quel que soit $Y \in \mathbb{K}^n$, le système carré $AX = Y$ entraîne une relation du type $X = \ldots$, alors A est inversible et l'expression de X en fonction de Y donne l'inverse de A.

Multiplication par une matrice diagonale par blocs

Multiplier une matrice par une matrice diagonale par blocs $\mathrm{Diag}(A_1, \ldots, A_n)$:

- à gauche revient à multiplier les lignes par les blocs diagonaux A_i ;
- à droite revient à multiplier les colonnes par les blocs diagonaux A_j.

5.2 Astuces

Astuce fondamentale de François Moulin, version matrices carrées Si on pense pouvoir faire un exercice en utilisant des matrices carrées, c'est qu'il faut utiliser des endomorphismes ! Du moins, il faut très rapidement passer du côté des endomorphismes et cela se déroule mieux en général. Évidemment, cela ne tient que pour quelque chose d'un peu abstrait.

Remarque. Attention, cette astuce et sa jumelle peuvent mener à des contradictions logiques majeures si on atteint le niveau de directement penser à changer de point de vue.

Formules de changement de base Bien connaître ses formules de changement de base.

Définition du déterminant Bien se souvenir de la définition du déterminant par les formes n-linéaires alternées.

Idées pour les calculs de déterminant Pour calculer un déterminant, on pourra :

1. Faire des combinaisons linéaires, même très originales ;
2. Se ramener à un déterminant par blocs ;
3. Développer par rapport aux lignes et aux colonnes ;
4. Utiliser la formule des signatures (uniquement pour des exercices théoriques !)

Autre méthode de calcul de déterminant Pour calculer le déterminant d'une matrice A un peu compliquée, essayer de l'écrire comme un produit $B \times C$ avec B et C des matrices dont le déterminant se calcule plus facilement. Le déterminant de A est alors le produit des deux déterminants.

Application. Calcul du déterminant de Smith.

Multilinéarité Souvent, si on repère que toutes les colonnes s'écrivent à partir d'une seule et même colonne, utiliser la multilinéarité du déterminant peut être une bonne idée.

Application. Calculer le déterminant de la matrice :

$$\begin{pmatrix} a_1 + b_1 & b_1 & \ldots & b_1 & b_1 \\ b_2 & a_2 + b_2 & & b_2 & b_2 \\ \vdots & & \ddots & & \vdots \\ b_n & b_n & \ldots & b_n & a_n + b_n \end{pmatrix}$$

Résolution d'un système de Cramer par les formules de Cramer On considère le système de Cramer $AX = B$ avec $A = (C_1|\dots|C_n)$ une matrice inversible, B un vecteur colonne et X le vecteur des inconnues. L'unique solution est donnée par les formules de Cramer :

$$x_i = \frac{\det(C_1, \dots, C_{i-1}, B, C_{i+1}, \dots, C_n)}{\det(A)}$$

En pratique, il est **obligatoire** d'utiliser cette méthode pour les système 2×2 (et c'est même une CNS pour utiliser cette méthode d'après François Moulin).

Matrices de permutation Penser aux matrices de permutations (*ie* les matrices qui codent une permutation de $\mathcal{S}_n$) : on peut les introduire pour créer des exemples et des contre-exemples. Bien penser à leur interprétation en termes de permutations d'une base.

Application. Fait partie de l'exercice pour montrer que tout hyperplan de $\mathcal{M}_n(\mathbb{C})$ rencontre $\mathcal{GL}_n(\mathbb{C})$ dès que $n \geqslant 2$.

Matrices extraites Penser aux propriétés des déterminants extraits et des matrices extraites.

Application. Exercice des $2n + 1$ cailloux

Coefficients -1,0 ou 1 Pour une matrice à coefficients valant -1, 0 ou 1, il est avantageux de plonger notre matrice dans $\mathbb{Z}/2\mathbb{Z}$, cela ne change pas la parité du déterminant. Ainsi, si on prouve dans $\mathbb{Z}/2\mathbb{Z}$ que notre déterminant est non nul, il est non nul dans $\mathbb{Z}$ car impair et la matrice est inversible.

Application. Exercice des 2n+1 cailloux

Coefficients -1 ou 1 Pour une matrice à coefficients valant exclusivement -1 ou 1, penser à effectuer des transvections car $(\pm 1) \pm (\pm 1)$ vaut -2, 0 ou 2. On peut ensuite factoriser des 2 dans le déterminant.

Application. Si A a uniquement des coefficients valant -1 ou 1 et est de taille n, alors 2^{n-1} divise $\det(A)$.

Matrices de rang 1 Si M est une matrice de rang 1, alors

$$M^2 = \mathrm{Tr}(M)M$$

Pour cela, on montre qu'il existe deux vecteurs X et Y tels que $M = XY^T$ grâce à l'hypothèse de rang 1. En fait, plus généralement, il n'existe que deux types de matrices de rang 1 (à similitude près) : celles avec un λ en haut en $(1,1)$, ou celles avec un 1 en $(1,2)$.

Déterminant et trace On se donne $\mathcal{B} = (e_1, \dots, e_n)$ une base de E de dimension n, ainsi que u un endomorphisme de E. Alors, pour tous $(x_1, \dots, x_n)$:

$$\sum_{j=1}^{n} \det_{\mathcal{B}}(x_1, \dots, x_{j-1}, u(x_j), x_{j+1}, \dots, x_n) = \mathrm{Tr}(u) \det_{\mathcal{B}}(x_1, \dots, x_n)$$

Pour montrer cela, il suffit de remarquer que le membre de gauche est une forme n-linéaire alternée, donc il est proportionnel au déterminant dans la base $\mathcal{B}$. Ensuite, il suffit d'évaluer sur la base pour montrer que cette constante vaut la trace de u (en développant les déterminants par multilinéarité après avoir décomposé les $u(x_j)$ sur la base $\mathcal{B}$).

Application. Permet de montrer que le wronskien vérifie une certaine équation différentielle et d'en obtenir une formule (*cf* exercices classiques d'équations différentielles).

Exercices du type "$A^2B = A$" Pour des exercices du type "$\mathrm{rg}(A) = \mathrm{rg}(B)$ et $A^2 = B^2$" ou encore "$A^2B = A$, réfléchir sur les inclusions de noyaux et d'image, passer aux applications linéaires canoniquement associées puis manipuler des bases bien choisies.

5.3 Exercices classiques

SEV engendré par les matrices de projecteurs

Déterminer le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ engendré par les matrices de projecteurs.

Démonstration. Les $E_{i,i}$ sont des matrices de projecteur. De plus, si $i \neq j$, $E_{i,i} + E_{i,j}$ est aussi une matrice de projecteur. Donc Les $E_{i,j}$ pour $i \neq j$ sont aussi dedans par différence. Le sous-espace vectoriel cherché est donc $\mathcal{M}_n(\mathbb{K})$. □

Idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$

Un idéal bilatère de $\mathcal{M}_n(\mathbb{K})$ est un SEv $\mathcal{I}$ de $\mathcal{M}_n(\mathbb{K})$ tel que :

$$\forall A \in \mathcal{I},\ \forall M \in \mathcal{M}_n(\mathbb{K}),\ AM \in \mathcal{I} \text{ et } MA \in \mathcal{I}$$

1. Montrer qu'un idéal bilatère non nul contient une matrice de rang 1. puis qu'il contient toutes les matrices de rang 1.
2. Déterminer l'ensemble des idéaux bilatères de $\mathcal{M}_n(\mathbb{K})$.
3. Montrer que tout endomorphisme d'algèbre de $\mathcal{M}_n(\mathbb{K})$ est injectif.

Démonstration.

1. Il contient une matrice non nulle, et on se ramène au fait qu'il contient une matrice J_r. Ensuite, on peut faire des opérations élémentaires matriciellement pour se ramener à J_1. Puis cet idéal contient toute matrice de rang 1 en multipliant par des matrices inversibles à droite et à gauche. Donc il contient tous les $E_{i,i}$ et est alors égal à $\mathcal{M}_n(\mathbb{K})$.
2. Ce sont donc exactement $\{0\}$ et $\mathcal{M}_n(\mathbb{K})$ tout entier.
3. Le noyau d'un tel morphisme est un idéal bilatère. Or, ce noyau n'est pas égal à $\mathcal{M}_n(\mathbb{K})$ puisque l'image de I_n est I_n. Donc son noyau est $\{0\}$ et ce morphisme est bien injectif.

□

Inverse de la matrice antédiagonale

Soient $a_1, \dots, a_n$ des complexes non nuls. donner l'inverse de la matrice antédiagonale :

$$A = \begin{pmatrix} (0) & & a_n \\ & \iddots & \\ a_1 & & (0) \end{pmatrix}$$

Démonstration. Son inverse est la matrice antédiagonale

$$B = \begin{pmatrix} (0) & & a_1^{-1} \\ & \iddots & \\ a_n^{-1} & & (0) \end{pmatrix}$$

On peut le vérifier par un calcul direct ou le voir en interprétant la matrice antédiagonale comme la matrice d'une inversion des vecteurs de la base, pondérée par les coefficients a_i. □

Nilpotence de combinaisons linéaires

Soit A et B dans $\mathcal{M}_n(\mathbb{K})$. On suppose qu'il existe au moins $n+1$ scalaires $\lambda_0, \dots, \lambda_n \in \mathbb{K}$ pour lesquels $A + \lambda B$ test nilpotente. Montrer que A et B sont nilpotentes.

Démonstration. Remarquons que les $A + \lambda_i B$ sont nécessairement d'indice de nilpotence inférieure à n. On considère

$$P = (A + X.B)^n \in \mathcal{M}_n(\mathbb{K}(X))$$

On note $P_{i,j}$ le coefficient d'indices (i, j) de P. Alors tous les $P_{i,j}$ sont de degré au plus n et s'annulent en $n+1$ points distincts, donc tous les $P_{i,j}$ sont nuls. Donc P est la matrice nulle. En particulier, en substituant 0 à X, on en déduit que A est nilpotente. En factorisant de force dans $P(\lambda)$ par λ et puisqu'il y a une infinité de scalaires non nuls, on en que $\tilde{P} = (X.A + B)^n$ est aussi nul, donc que B est nilpotente. □

Penser aux images et noyaux

Soit A et B dans $\mathcal{M}_n(\mathbb{C})$ de même rang telles que $A^2B = A$. Montrer que $B^2A = B$.

Démonstration. Traduire les hypothèses en termes d'applications linéaires. En déduire que $\mathrm{Im}(a)$ et $\mathrm{Ker}(a)$ son supplémentaires, puis raisonner matriciellement. □

Propriétés d'un morphisme multiplicatif sur $\mathcal{M}_n(\mathbb{C})$

Soit $f : \mathcal{M}_n(\mathbb{C}) \to \mathbb{C}$ non constante telle que :

$$\forall (A, B) \in \mathcal{M}_n(\mathbb{C})^2,\ f(AB) = f(A)f(B)$$

1. Montrer que $A \in \mathcal{M}_n(\mathbb{C})$ est inversible si, et seulement si, $f(A) \neq 0$. On pourra penser aux matrices nilpotentes.
2. Trouver tous les $X \in \mathcal{M}_n(\mathbb{C})$ tels que :

$$\forall M \in \mathcal{M}_n(\mathbb{C}),\ f(M + X) = f(M) + f(X)$$

Démonstration. Déjà on remarque que $f(0) = f(0)^2$ donc $f(0) = 0$ ou $f(0) = 1$. De même pour I_n. Or, il est impossible que $f(0) = 0$ sinon f serait constante égale à $f(0)$ car 0 est absorbant pour $\times$. De même, on a nécessairement $f(I_n) = 1$.

1. Dans le sens direct, c'est immédiat car alors $f(A)f(A^{-1}) = 1$ donc les deux sont non nuls. Dans le sens réciproque, on raisonne par contraposée. Si A est non inversible, A est équivalente à une matrice J_r avec $r < n$. Mais cette J_r est équivalente à une matrice B_r dont la diagonale supérieure ne contient que r 1 et des 0, qui est nilpotente. Par conséquent, $f(B_r)^n = 0$. Donc $f(A)^n = 0$ par commutativité de $\mathbb{C}$. Donc $f(A) = 0$.
2. Nécessairement, en écrivant $X = PJ_rQ$ et $M = P(I_n - J_r)Q$, on obtient par hypothèse $r = 0$ ou $r = n$, donc $X + 0$ ou $X \in \mathcal{GL}_n(\mathbb{C})$. Réciproquement, 0 convient, mais pour les matrices inversibles c'est pkus compliqué. I_n ne convient pas lorsque $n \geqslant 2$ (prendre $-E_{1,1}$) et si $n \geqslant 1$, on ne peut pas dire grand-chose.

□

Similitude et surcorps

Montrer que si A est B dans $\mathcal{M}_n(\mathbb{R})$ sont semblables dans $\mathcal{M}_n(\mathbb{C})$, alors elles sont aussi semblables dans $\mathcal{M}_n(\mathbb{R})$. Même question (mais c'est plus dur) avec $\mathbb{K}$ et $\mathbb{L}$ un surcorps de $\mathbb{K}$ (on pourra commencer par le cas où $\mathbb{L}$ est de dimension finie sur $\mathbb{K}$).

Démonstration. On commence par le cas de $\mathbb{R}$ et $\mathbb{C}$ qui est le cas "usuel".

- On fixe $P \in \mathcal{GL}_n(\mathbb{C})$ telle que $PB = AP$. On écrit $P = P_1 + iP_2$ avec P_1 et P_2 à coefficients réels. On obtient alors :

$$\begin{cases} P_1 B = AP_1 \\ P_2 B = AP_2 \end{cases}$$

  Pour $\lambda \in \mathbb{C}$, on pose $P_\lambda = P_1 + \lambda P_2$ et on veut montrer qu'il existe un λ réel tel que P_λ soit inversible. Par l'absurde, si ce n'était pas le cas, le déterminant de P_λ, polynomial en λ, serait nul sur $\mathbb{R}$ qui est infini donc sur $\mathbb{C}$ ce qui est absurde car il n'est pas nul en i.
- On suppose $\dim_{\mathbb{K}}(\mathbb{L}) = n < +\infty$ et on écrit $P = l_1 P_1 + \ldots + l_n P_n$ avant de considérer

$$P = \lambda_1 P_1 + \ldots + \lambda_n P_n$$

et φ qui à $(\lambda_1, \dots, \lambda_n)$ associe le déterminant de P. C'est un polynôme à n indéterminées. On montre alors par récurrence sur n que

$$\forall Q \in \mathbb{L}[X_1, \dots, X_n],\ (\forall (x_1, \dots, x_n) \in \mathbb{K}^n,\ Q(x_1, \dots, x_n) = 0) \implies Q = 0$$

OK pour l'initialisation, pour l'hérédité, on fixe $x_0 \in \mathbb{K}$ et par hypothèse de récurrence

$$Q(x_0, X_1, \dots, X_n) = 0$$

Puis on a donc

$$Q(X_0, x_1, \dots, x_n)$$

qui s'annule en une infinité de points (tous les x_0) donc $Q(X_0, x_1, \dots, x_n) = 0$ quel que soit le $n-uplet$. On en déduit que $Q(X_0, \dots, X_n)$ est le polynôme nul. Avec ce lemme, on conclut de même que dans le premier point.

- Dans le cas général, on considère $F = \mathrm{Vect}(P_{i,j})$ puis on utilise le cas précédent avec une base de F.

□

Un grand classique : vers la densité des matrices inversibles

Soit $A \in \mathcal{M}_n(\mathbb{K})$ où $\mathbb{K}$ est un corps infini. Montrer qu'il existe une infinité de $\lambda \in \mathbb{K}$ tels que $\lambda I_n - A$ soit inversible.

Démonstration. L'application qui à λ associe le déterminant de $\lambda I_n - A$ est polynomiale en λ. Elle est non nulle car de degré $n \geqslant 1$ (sinon l'exercice n'a pas d'intérêt). donc elle possède un nombre fini de racines, c'est-à-dire qu'il existe une infinité de λ tels que le déterminant de $\lambda I_n - 1$ soit non nul, *ie* que $\lambda I_n - A$ soit inversible. □

Déterminant de l'application transposition

Calculer le déterminant de l'endomorphisme qui à une matrice associe sa transposée.

Démonstration. L'essentiel est de mettre la base canonique de $\mathcal{M}_n(\mathbb{K})$ dans le bon ordre. On met d'abord les $E_{i,i}$, puis on met ensemble les $E_{i,j}$ et $E_{j,i}$. On trouve en calculant le déterminant par blocs dans cette base :

$$(-1)^{n(n-1)/2}$$

□

Vers les polynômes caractéristiques

Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$ et $B \in \mathcal{M}_{n,p}(\mathbb{K})$. En effectuant dans les deux sens le produit par blocs entre les matrices :

$$\begin{pmatrix} I_n & B \\ A & \lambda I_p \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} \lambda I_n & 0 \\ -A & I_p \end{pmatrix}$$

montrer que

$$\forall \lambda \in \mathbb{K},\ \lambda^n \det(\lambda I_p - AB) = \lambda^p \det(\lambda I_n - BA)$$

Démonstration. Effectuer les deux produits par blocs. On trouve des matrices triangulaires par blocs. Calculer les deux déterminants, qui sont égaux par commutativité de $\mathbb{K}$. On trouve bien la formule demandée. □

Application. Permet de montrer que $\chi_{AB} = \chi_{BA}$ en prenant $p = n$.

Une généralisation du déterminant 2×2

Soit $(A, B, C, D) \in \mathcal{M}_n(\mathbb{K})^4$ tel que $CD = CD$. Montre que

$$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BC)$$

On pourra commencer par le cas où D est inversible.

Démonstration. Effecteur des transvections par blocs en multipliant :

- à droite par $\begin{pmatrix} D & 0 \\ -C & I_n \end{pmatrix}$
- à gauche par $\begin{pmatrix} I_n & 0 \\ 0 & D^{-1} \end{pmatrix}$

puis calculer le déterminant obtenu. Dans le cas général, utiliser la densité des matrices inversibles (en considérant $D_X = D - X.I_n$ par exemple). □

Presque une identité remarquable et un déterminant 2×2 sans commutation

Soit $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$ et $M = \begin{pmatrix} A & B \\ B & A \end{pmatrix}$. Montrer que

$$\det(M) = \det(A + B)\det(A - B)$$

Démonstration. Effectuer les transvections par blocs suivantes :

- $C_1 \leftarrow C_1 - C_2$, codée par une multiplication à droite par

$$\begin{pmatrix} I_n & 0 \\ -I_n & I_n \end{pmatrix}$$

- puis $L_2 \leftarrow L_1 + L_2$ codée par une multiplication à gauche par

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

Calculer ensuite le déterminant des matrices obtenues. □

Coefficients entiers et parité pour le déterminant

Soit $A \in \mathcal{M}_n(\mathbb{Z})$ ayant tous les coefficients diagonaux impairs et tous les coefficients non diagonaux pairs. Montrer que A est inversible dans $\mathcal{M}_n(\mathbb{R})$.

Démonstration. Déjà, $\det(A) \in \mathbb{Z}$ et, si on note $\overline{A}$ la matrice des classes des coefficients de A dans $\mathbb{Z}/2\mathbb{Z}$, la formule des signatures prouve que

$$\overline{\det(A)} = \det(\overline{A})$$

Or, $\overline{A} = I_n$ donc $\det(\overline{A}) = \overline{1}$. Par conséquent, $\det(A)$ est impair donc non nul donc A est inversible dans $\mathcal{M}_n(\mathbb{R})$. □

Bizarre...

Soit A et B dans $\mathcal{M}_n(\mathbb{R})$ telles que $A^2 + B^2 = \sqrt{3}(AB - BA)$ et $AB - BA$ soit inversibles. Montrer que n est un multiple de 6.

Démonstration. L'astuce est de calculer $(A + iB)(A - iB)$. L'hypothèse nous donne :

$$(A + iB)(A - iB) = (\sqrt{3} - i)(AB - BA) = 2e^{-i\pi/6}(AB - BA)$$

Or, la formule des signatures donne rapidement

$$\overline{\det(A + iB)} = \det(A - iB)$$

Par conséquent, $\det((A + iB)(A - iB)) \in \mathbb{R}$. Or,

$$\det((A + iB)(A - iB)) = 2^n e^{-in\pi/6} \underbrace{\det(AB - BA)}_{\in \mathbb{R}^*}$$

Par conséquent, $e^{-in\pi/6} \in \mathbb{R}$ donc 6 divise n. □

Déterminant et matrice de rang 1

Soit $n \in \mathbb{N}^*$ et $A \in \mathcal{M}_n(\mathbb{K})$ de rang 1. Montrer que

$$\det(I_n + A) = 1 + \operatorname{Tr}(A)$$

Démonstration. Comme la matrice est de rang 1, elle possède une colonne non nulle et on peut exprimer toutes les autres colonnes en fonction de cette colonne principale. Alors, on peut développer le déterminant souhaité par multilinéarité, et à ce moment là, beaucoup de termes disparaissent par le caractère alterné du déterminant. Après quelques calculs, on obtient le résultat voulu. □

Matrices à diagonale dominante

Une matrice à diagonale dominante est inversible.

Démonstration. On raisonne par l'absurde en considérant un élément non nul X du noyau de A. On écrit la relation $AX = 0$ puis on s'intéresse à la ligne de l'égalité précédente qui correspond au x_i de module maximal non nul et on obtient une absurdité grâce au fait que la diagonale est dominante. □

Application. Disque de Gershgoring.

Puissances de la matrice des coefficients binomiaux

Calculer les puissances A^k de la matrice $A = \left(\binom{i}{i}\right)_{0 \leqslant i,j \leqslant n}$ pour $k \in \mathbb{Z}$.

Démonstration. Pour cela, on interprète cette matrice comme la matrice de l'endomorphisme

$$T: \begin{array}{ccc} \mathbb{K}_n[X] & \longrightarrow & \mathbb{K}_n[X] \\ P & \longmapsto & P(X+1) \end{array}$$

dans la base canonique de $\mathbb{K}_n[X]$. Par conséquent, la puissance k de A correspond à $P \mapsto P(X+k)$, que l'on sait très facilement calculer. $\square$

Un peu de matrices à coefficients dans $\mathbb{Z}$

Soit $n \in \mathbb{N}^*$. Soit $M \in \mathcal{M}_n(\mathbb{Z})$. Montrer que

$$M \in \mathcal{GL}_n(\mathbb{Z}) \Longleftrightarrow \det(M) = \pm 1$$

où on a posé

$$\mathcal{GL}_n(\mathbb{Z}) = \{A \in \mathcal{M}_n(\mathbb{Z}) \mid \exists B \in \mathcal{M}_n(\mathbb{Z}),\ AB = I_n\}$$

Démonstration. Pour $\Longrightarrow$, utiliser le fait que le déterminant de M doit être une unité de $\mathbb{Z}$. Pour $\Longleftarrow$, utiliser la formule de la comatrice et le fait que le déterminant est polynomial. $\square$

Représentation des formes linéaires sur $\mathcal{M}_n(\mathbb{K})$

Soit ψ une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$. Montrer qu'il existe une unique matrice $A \in \mathcal{M}_n(\mathbb{K})$ telle que

$$\forall M \in \mathcal{M}_n(\mathbb{K}),\ \psi(M) = \mathrm{Tr(AM)}$$

Démonstration. Considérer pour tout $A \in \mathcal{M}_n(\mathbb{K})$ l'application

$$f_A: \begin{array}{ccc} \mathcal{M}_\backslash(\mathbb{K}) & \longrightarrow & \mathbb{K} \\ M & \longmapsto & \mathrm{Tr}(AM) \end{array}$$

puis considérer

$$\varphi: \begin{array}{ccc} \mathcal{M}_n(\mathbb{K}) & \longrightarrow & \mathcal{M}_n(\mathbb{K})^* \\ A & \longmapsto & f_A \end{array}$$

Déjà, il est claire que les f_A sont bien des formes linéaires et que φ est bien définie et linéaire. De plus, on montre que φ est injective car si $\forall M \in \mathcal{M}_n(\mathbb{K}),\ \mathrm{Tr}(AM) = 0$, alors en utilisant des matrices d'opérations élémentaires et en annulant certaines lignes ou colonnes, on montre que A est nulle. Si $\mathbb{K} = \mathbb{R}$, il est plus rapide de le faire avec $M = A^T$, et si $\mathbb{K} = \mathbb{C}$, il est plus rapide de le faire avec $M = \overline{A}^T$ (cela correspond aux produits scalaires). Par égalité de dimension, φ est donc un isomorphisme, ce qui conclut. $\square$

Application. Sert énormément pour des exercices qui traitent des hyperplans de matrices. Voici une liste non exhaustive : trouver toutes les formes linéaires sur $\mathcal{M}_n(\mathbb{K})$ telles que $f(AB) = f(A)f(B)$; montrer qu'un hyperplan contient une matrice inversible pour $n \geqslant 2$; montrer qu'il n'existe pas d'hyperplan stable par produit pour $n \geqslant 3$; détermination des hyperplans stables par conjugaison matricielle (PMP^{-1}).

$H \cap \mathcal{GL}_n(\mathbb{C})$ pour $n \geqslant 2$

Tout hyperplan de $\mathcal{M}_n(\mathbb{K})$ contient une matrice inversible pour $n > 1$

Démonstration. On prend la forme linéaire non nulle dont H est le noyau. On représente cette forme linéaire par $M \mapsto \mathrm{Tr}(AM)$ avec A non nulle. Par équivalence, on se ramène à chercher une matrice inversible N telle que $\mathrm{Tr}(J_r N) = 0$. On pourra considérer pour N la matrice du cycle $(1\ 2\ \ldots\ n)$. □

Déterminants en vrac

Soit $n \in \mathbb{N}^*$. Calculer

1. $\det((i^j)_{1\leq i,j\leq n})$
2. $\det((\max(i,j))_{1\leq i,j\leq n})$

Démonstration. Représenter le début de la matrice peut aider...

1. Faire sortir un i de chaque ligne par multilinéarité. On obtient alors $n!$ fois un déterminant de Vandermonde qui vaut $\prod_{1\leq i<j\leq n}(j-i) = \prod_{j=2}^{n}\prod_{i=1}^{j-1}(j-i) = \prod_{j=1}^{n-1} j!$. On en tire le résultat final :
$$\det((i^j)_{1\leq i,j\leq n}) = \prod_{k=1}^{n} k!$$
2. C'est surtout ici que la représentation de la matrice aide : la matrice est "en escalier". Cela peut aider à savoir quelles transvections faire. On pourra formaliser avec une récurrence si on le souhaite.

□

Déterminant de Smith

Calculer le déterminant de Smith :
$$\det\,(i \wedge j)_{(1\leqslant i,j\leqslant n)}$$

Démonstration. Utiliser la formule
$$n = \sum_{d|n} \varphi(d)$$
Introduire la notation $\delta_{i|j}$ qui vaut 1 si i divise j et 0 sinon. Ainsi, on peut interpréter $i \wedge j$ comme le terme d'un produit matriciel. Dessiner les matrices correspondantes, dont on montre qu'elles sont

triangulaires à cause des $\delta_{i|j}$. On obtient :

$$\det{(i \wedge j)}_{(1 \leqslant i,j \leqslant n)} = \prod_{k=1}^{n} \varphi(k)$$

□

Déterminant de Cauchy

Montrer par récurrence la formule

$$C_n = \frac{V(a_1, \dots, a_n)V(b_1, \dots, b_n)}{\prod_{i,j}(a_i + b_j)}$$

C'est la formule du déterminant de Cauchy.

Démonstration. On multiplie toutes les colonnes par $a_n + b_j$, puis on soustrait la dernière colonne aux autres avant de factoriser les termes communs aux lignes et aux colonnes pour finalement développer par rapport à la dernière ligne. On obtient la relation de récurrence :

$$C_n = \frac{1}{a_n + b_n} \left(\prod_{i=1}^{n-1} \frac{(a_n - a_i)(b_n - b_i)}{(a_n + b_i)(a_i + b_n)} \right) C_{n-1}$$

□

Déterminant d'un produit de Kronecker

Pour $A \in \mathcal{M}_m(\mathbb{K})$ et $B \in \mathcal{M}_n(\mathbb{K})$, on a la formule :

$$\det(A \otimes B) = \det(A)^n \det(B)^m$$

Démonstration. En effet, on utilise la relation fonctionnelle $(AC) \otimes (BD) = (A \otimes B) \times (C \otimes D)$ avec des matrices identités. Le plus dur est alors de montrer que $A \otimes B$ est semblable à $B \otimes A$, ce qui permettra de conclure. Pour cela, prendre une base adaptée à la structure de produit tensoriel, et, au lieu de sommer d'abord sur les indices des premières composantes de cette famille produit tensoriel, sommer sur l'autre composante. Cela permet de passer de $A \otimes B$ à $B \otimes A$ en changeant de base, donc ces matrices sont semblables et ont le même déterminant. On conclut en appliquant ceci avec les matrices identités car le déterminant de $I \otimes B$ se calcule très bien comme déterminant diagonal par blocs. □

Comatrice du produit

Soit $A, B \in \mathcal{M}_n(\mathbb{C})$. Montrer que

$$\mathrm{Com}(AB) = \mathrm{Com}(A)\mathrm{Com}(B)$$

En déduire que si A et B commutent, alors $\mathrm{Com}(A)$ et $\mathrm{Com}(B)$ commutent.

Démonstration. Commencer par le cas où les deux matrices sont inversibles. Le résultat s'obtient alors rapidement avec la formule des comatrices en fonction des déterminants et des transposées. Pour le cas général, utiliser la densité des matrices inversibles dans les matrices (définir les matrices $A_z = A + zI_n$ et $B_z = B + zI_n$) puis définir des polynômes coefficient par coefficient pour les matrices $\mathrm{Com}(A_zB_z)$ et $\mathrm{Com}(A_z)Com(B_z)$ et montrer qu'ils sont égaux car ils le sont en une infinité de points. Enfin, évaluer en 0 pour conclure. □

Le problème des $2 + 1$ vaches/cailloux

Voici la généralisation du célèbre problème des 11 vaches. Soit $n \geq 2$.

1. Soit $M \in \mathcal{M}_n(\mathbb{Z})$ dont tous les coefficients valent ± 1 sauf ceux sur la diagonale qui valent 0. Montrer que $\det(M) \neq 0$.
2. Soit un groupe de $2n + 1$ vaches (ou cailloux, au choix) tel que dès que l'on retire une vache, on peut toujours former parmi les $2n$ restantes deux groupes de n vaches dont les sommes des poids des vaches par groupes sont égales. Montrer que toutes les vaches ont le même poids. Il est conseillé de traduire matriciellement le problème, la première question n'est pas là pour rien... On pourra montrer que l'image de la matrice considérée est de dimension $2n$.

Démonstration. Si on n'a pas de chance, c'est sans la première question !

1. Passer dans $\mathbb{Z}/2\mathbb{Z}$
2. Montrer que la matrice considérée est de rang supérieur à $2n$ en utilisant la question précédente, puis montrer que le noyau est de dimension supérieure ou égale à 1 car il contient le vecteur colonne composé uniquement de 1. Conclure en remarquant que le vecteur "poids des vaches" est dans le noyau. Il s'écrit donc comme une dilatation du vecteur colonne comportant uniquement des 1 : toutes les vaches ont donc le même poids.

□

Une somme étrange (pas classique du tout mais marrant)

Soit $n \geqslant 1$. Pour tout $\sigma \in \mathfrak{S}_n$, on note $\mathrm{inv}(\sigma)$ le nombre de points de $[\![1, n]\!]$ invariants par σ. Calculer :

$$\sum_{\sigma \in \mathfrak{S}_n} \frac{\varepsilon(\sigma)}{\mathrm{inv}(\sigma) + 1}$$

Démonstration. Écrire

$$\frac{1}{\mathrm{inv}(\sigma) + 1} = \int_0^1 x^{\mathrm{inv}(\sigma)}\ dx$$

puis utiliser la linéarité de l'intégrale. S'intéresser au polynôme obtenu sous le symbole d'intégration. Interpréter ce polynôme comme un déterminant (suite de l'indication : celui de la matrice comportant des 1 partout et une diagonale de x). Calculer ensuite ce déterminant par opérations. □

Chapitre 6

Réduction

6.1 Points méthode

Équation aux éléments propres pour un endomorphisme

Pour rechercher les éléments propres d'un endomorphisme u (valeurs propres et sous-espaces propres associés), on peut résoudre l'équation $u(x) = \lambda x$, appelée équation aux éléments propres.

Équation aux éléments propres pour une matrice

Pour rechercher les éléments propres d'une matrice A, on peut résoudre l'équation $AX = \lambda X$, appelée équation aux éléments propres.

Polynôme caractéristique dans $\mathcal{M}_2(\mathbb{K})$

Le polynôme caractéristique de $A \in \mathcal{M}_2(\mathbb{K})$ est :

$$X^2 - \mathrm{Tr}(A)X + \det(A)$$

On utilise impérativement cette expression quand on travaille dans $\mathcal{M}_2(\mathbb{K})$.

Calcul alternatif

Parfois, il est plus intéressant de calculer $\det(A - \lambda I_n) = (-1)^n \chi_A(\lambda)$ plutôt que $\det(\lambda I_n - A) = \chi_A(\lambda)$ (par exemple pour une matrice compagnon).

Importance d'un polynôme caractéristique factorisé

Puisque les racines du polynôme caractéristique sont les valeurs propres, il est important d'obtenir le polynôme caractéristique sous forme factorisée. On réalise dans les cas concret cet objectif en calculant le déterminant de $A - \lambda I_n$ par opérations élémentaires afin (suivant les cas) :

- de faire apparaître des facteurs communs dans les lignes ou les colonnes ;
- de se ramener à une matrice triangulaire, au moins en partie.

On pourra notamment utiliser des combinaisons linéaires qui traduisant des relations de liaison entre les colonnes, ou encore passer à la transposée si ces relations de liaison sont sur les lignes.

Expression dans le cas diagonalisable

Soit $A \in \mathcal{M}_n(\mathbb{K})$ diagonalisable et $(E_1, \ldots, E_n)$ une base de $\mathbb{K}^n$ constituée de vecteurs propres de A associés aux valeurs propres $\lambda_1, \ldots, \lambda_n$. Si on pose p la matrices dont les colonnes sont $E_1, \ldots, E_n$, alors :

$$A = PDP^{-1} \text{ ou } D = \mathrm{Diag}(\lambda_1, \ldots, \lambda_n)$$

CS de diagonalisabilité

Pour montrer qu'une endomorphisme d'un espace vectoriel de dimension n, ou une matrice de taille n, est diagonalisable, il suffit de montrer que la somme des dimensions de ses sous-espaces propres est supérieure ou égale à n.

Savoir si un endomorphisme est diagonalisable

Pour savoir si un endomorphisme u est diagonalisable, on peut calculer son polynôme caractéristique.

- S'il n'est pas scindé, alors u n'est pas diagonalisable.
- Sinon, pour toute valeur propre multiple, on compare $\dim(E\lambda(u))$ et $m(\lambda)$, par exemple en calculant le rang de $u - \lambda \mathrm{Id}_E$.

Processus de trigonalisation

Une base trigonalisation commençant par un vecteur propre, pour trigonaliser un endomorphisme u, on commence souvent par compléter un vecteur propre de u en une base de E, dans laquelle la matrice de u est donc de la forme

$$\begin{pmatrix} \lambda & L \\ 0 & A \end{pmatrix} \in \mathcal{M}_n(\mathbb{K}) \text{ où } A \in \mathcal{M}_{n-1}(\mathbb{K}) \text{ et } L \in \mathcal{M}_{n-1,1}(\mathbb{K})$$

Il suffit alors de montrer que l'on peut prendre A triangulaire supérieure pour conclure. Comme la matrice A n'est pas *a priori* la matrice d'un endomorphisme, on raisonne le plus souvent en trigonalisant la matrice A (ou alors on fait le terroriste en composant par une projection sur un hyperplan pour se ramener à un endomorphisme).

6.2 Astuces

6.2.1 Généralités

Projecteurs spectraux Ce sont les projecteurs associés à la décomposition en sous-espaces propres

$$E = \bigoplus_{i=1}^{r} E_{\lambda_i}(u)$$

lorsque l'endomorphisme u est diagonalisable. On les note $p_1, \ldots, p_r$. On a $u = \lambda_1 p_1 + \ldots + \lambda_r p_r$ et on peut montrer par caractérisation par les supplémentaires que

$$\forall n \in \mathbb{N},\ u^n = \lambda_1^n p_1 + \ldots + \lambda_r^n p_r$$

Par linéarité, cette relation s'étend à tous les polynômes. Cela permet efficacement de calculer les puissances d'une matrice. Les polynômes spectraux sont des polynômes en u : on utilise la relation vraies sur tous les polynômes et on prend en particulier les polynômes interpolateurs de Lagrange associés aux valeurs propres distinctes.

Polynôme annulateur et matrice inversible Si P est un polynôme annulant une matrice carrée A avec

$$P = \lambda \prod_j (X - x_j)$$

alors il existe un indice j tel que $A - x_j I$ soit non inversible. On regarde pour cela le déterminant de $P(A)$ et on utilise l'intégrité. Si P/λ est le polynôme minimal de A, c'est même vrai pour tout indice j !

Endomorphisme réel sur un espace de dimension impaire Une matrice réelle ou un endomorphisme réel sur un espace de dimension finie impaire admet au moins une valeur propre réelle (car le polynôme caractéristique est de degré impair) donc un vecteur propre réel, et même au moins une valeur propre de multiplicité impaire.

Utilisation des polynômes interpolateurs de Lagrange Si on a comme hypothèse un prédicat P qui vérifie une propriété du type :

$$\forall k \in \mathbb{N},\ P(A^k)\ \ldots$$

il peut être fort utile de s'intéresser à des polynômes interpolateurs de Lagrange et utiliser de la linéarité.

Application. Une matrice carrée A vérifiant $\forall k \in \mathbb{N}^*,\ \mathrm{Tr}(A^k) = 0$ est nilpotente. Remarquer que cela peut aussi se faire avec un déterminant de Vandermonde.

Utilisation de la linéarité Si on dispose d'une hypothèse en :

$$\forall k \in \mathbb{N},\ A^k = \text{ Truc linéaire en } A$$

Alors on peut en déduire que

$$\forall P \in \mathbb{K}[X],\ P(A) = P(\text{Truc linéaire en } A)$$

car on a la coïncidence de deux applications linéaires sur la base canonique des polynômes. En particulier, il peut être utile de considérer ensuite le polynôme minimal ou le polynôme caractéristique.

Application. Si A est diagonalisable (resp. trigonalisable), alors $M \mapsto AM$ est diagonalisable (resp. trigonalisable).

Le polynôme minimal est irréductible sur une algèbre intègre Si A est une algèbre intègre, le polynôme minimal d'un élément de A est nécessairement irréductible. Sinon, l'intégrité permettrait de contredire sa minimalité.

Application de la réduction en dimension infinie Voici un des rares usages de la réduction en dimension infinie : on rappelle que si f est un endomorphisme, une famille $(v_i)_{i\in I}$ de vecteurs propres de f associés à des valeurs propres distinctes est libre. Ceci peut notamment servir pour des fonctions où on pense à l'endomorphisme de dérivation, éventuellement itéré !

Application. La famille $(x \mapsto e^{ax})_{a\in\mathbb{R}}$ est libre car tous ses éléments sont des vecteurs propres de l'endomorphisme de dérivation de $\mathcal{C}^\infty$ associés à des valeurs propres distinctes.

Application. De même, la famille $(x \mapsto \sin(ax))_{a\in\mathbb{R}}$ est libre, mais on utilise ici l'endomorphisme de double dérivation $f \mapsto f''$.

Cotrigonalisation Deux endomorphismes scindés qui commutent sont trigonalisables dans une même base. On a le même résultat pour une partie de $\mathcal{L}(E)$ formée d'endomorphismes scindés qui commutent deux à deux. Etapes de la démonstration :

1. Montrer que deux endomorphismes qui commutent admettent un vecteur propre commun (les sous-espaces propres sont stables).
2. Procéder par récurrence forte sur la dimension de l'espace. Soit tous les endomorphismes sont des homothéties, et c'est évident, soit il y en a un, qu'on note u, qui ne l'est pas. Il existe alors $\lambda \in \mathrm{Sp}(u)$ tel que

$$\dim(E_\lambda) < \dim(E)$$

   On peut alors utiliser l'hypothèse de récurrence avec $E = H \oplus E_\lambda$. En notant π la projection sur H parallèlement à E_λ, on se ramène à l'hypothèse de récurrence en considérant les $\tilde{v} = \pi \circ v_{|H}$.

Sinon, on peut remarquer que le résultat est clairement équivalent à sa version matricielle et utiliser des matrices pour l'hérédité, ce qui est plus claire que les projections.

Codiagonalisation Deux endomorphismes diagonalisables qui commutent sont diagonalisables dans une même base. On a le même résultat pour une partie de $\mathcal{L}(E)$ formée d'endomorphismes diagonalisables qui commutent deux à deux. On procède de façon similaire à la démonstration de la cortigonalisation, mais l'hérédité est plus simple, il n'y a pas besoin de considérer une projection.

Décomposition de Dunford (HP, très utile) Soit A une matrice dont le polynôme caractéristique est scindé. Alors, il existe un unique couple de matrices (D, N) tel que D soit diagonalisable, N soit nilpotente, $DN = ND$ et on ait :

$$A = D + N$$

L'existence provient de la décomposition en sous-espaces caractéristiques.

Décomposition de Jordan (fortement HP)

6.2.2 Exponentielles de matrices

$\exp(A)$ **est un polynôme en** A Montrons que $\exp(A) \in \mathbb{K}[A]$. Les sommes partielles sont dans $\mathbb{K}[A]$. Or, $\mathbb{K}[A]$ est un SEV de dimension finie de $\mathcal{M}_n(\mathbb{K})$, donc il est fermé. Par conséquent, $\exp(A) \in \mathbb{K}[A]$. Et par suite :

$$\exists P \in \mathbb{K}[X],\ \exp(A) = P(A)$$

Exponentielle d'une matrice diagonale On a la formule :

$$\exp(\mathrm{Diag}(\lambda_i)) = \mathrm{Diag}(e^{\lambda_i}$$

En effet, il suffit de passer par les sommes partielles et de passer à la limite.

Exponentielle d'une matrice triangulaire L'exponentielle d'une matrice triangulaire est une matrice triangulaire dont les éléments diagonaux sont les exponentielles des coefficients diagonaux de la matrice de départ.

Exponentielle et similitude Si $A = P^{-1}BP$, alors

$$\exp(A) = P^{-1}\exp(B)P$$

On repasse par la définition avec les sommes partielles en utilisant le fait que $(P^{-1}BP)^k = P^{-1}B^kP$. La continuité de l'application de conjugaison par P permet de conclure.

Déterminant d'une exponentielle On a la formule :

$$\forall A \in \mathcal{M}_n(\mathbb{C}),\ \det(\exp(A))e^{\mathrm{Tr}(A)}$$

En effet, cela est immédiat en trigonalisant A et en utilisant les deux points précédents.

Utilisation de la décomposition de Dunford Quand on prend des exponentielles de matrices, notamment pour les équations différentielles, penser à utiliser la décomposition de Dunford (l'exponentielle d'une matrice diagonalisable s'exprime simplement, celle d'une matrice nilpotente est un polynôme en cette matrice).

Décomposition de Dunford de l'exponentielle Soit A une matrice dont la décomposition de Dunford s'écrit $A = D + N$ avec D diagonalisable, N nilpotente d'indice n et $DN = ND$. Alors, la décomposition de Dunford de $\exp(A)$ est :

$$\exp(A) = \exp(D) + \exp(D)NP(N)$$

où $P = \displaystyle\sum_{k=0}^{n-2} \frac{X^k}{(k+1)!}$. En effet, on a $\exp(A) = \exp(D)\exp(N)$, on sait que $\exp(D)$ est diagonalisable, et on sait que

$$\exp(N) = \sum_{k=0}^{n-1} \frac{N^k}{k!} = I + NP(N)$$

Par conséquent, comme $\exp(D)$ est un polynôme, elle commute avec N et $P(N)$, donc $\exp(D)NP(N)$ est nilpotente car N l'est. L'unicité de la décomposition de Dunford conclut.

Application. Si A une matrice complexe vérifie $\exp(2\pi A) = I$, alors A est diagonalisable et $\mathrm{Sp}(A) \subset i\mathbb{Z}$. En effet, avec $A = D + N$ la décomposition de Dunford de A, celle de $2\pi A$ est $2\pi D + 2\pi N$ puis par unicité de la décomposition de Dunford de $\exp(2\pi A)$, on obtient :

$$\exp(2\pi D) = I \text{ et } \exp(2\pi D)2\pi NP(2\pi N) = 0$$

La première égalité fournit que pour toute valeur propre λ de A (*ie* de D), on a $e^{2\pi\lambda} = 1$ donc $\lambda \in i\mathbb{Z}$. Et, avec la deuxième, puisque $\exp(2\pi D)$ est inversible, $NP(2\pi N) = 0$. Or, $P(2\pi N)$ est aussi inversible (I plus une matrice nilpotente, télescopage), donc $N = 0$. Par conséquent, A est diagonalisable (car $A = D$) et $\mathrm{Sp}(A) \subset i\mathbb{Z}$.

Exponentielle de matrices antisymétriques L'exponentielle d'une matrice symétrique réelle. En particulier, si

$$A = \begin{pmatrix} 0 & -t \\ t & 0 \end{pmatrix}$$

alors on a :

$$\exp(A) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$

Démonstration. Si $B \in \mathcal{A}_n(\mathbb{R})$, alors $\det(\exp(B)) = e^{\mathrm{Tr}(B)} = e^0 = 1$ et

$$\exp(B)\exp(B)^T = \exp(B)\exp(B^T) = \exp(B)\exp(-B) = \exp(0) = I_n$$

si bien que $B \in \mathcal{SO}_n(\mathbb{R})$. De plus, si on considère A comme dans l'énoncé, on a :

$$A^{2k} = (-1)^k t^{2k} I_2 \quad \text{et} \quad A^{2k+1} = (-1)^k t^{2k+1} A$$

donc on obtient le résultat en appliquant la définition de l'exponentielle matricielle et en reconnaissant le développement en série entière du cosinus et du sinus. □

Utilisation de la dérivation Quand on voit des exponentielles de matrices qui ne commutent pas, on peut introduire une fonction de la variable réelle et la dériver. En effet, puisque la dérivée de $t \mapsto e^{tA}$ est $t \mapsto Ae^{tA} = e^{tA}A$, on peut placer les matrices où on le souhaite. De façon générale, quand on dérive $t \mapsto e^{tA}$, toujours se demander où est-ce qu'il vaut mieux placer A.

Application. Si on considère $f : t \mapsto e^{itB}e^{-itA}$, alors on a :

$$f'(t) = ie^{itB}(B - A)e^{itA}$$

On peut alors intégrer, passer à la norme, utiliser des propriétés de développements asymptotiques, etc.

6.3 Exercices classiques

Matrices singulières et plans vectoriels

Montrer que tout plan vectoriel de $\mathcal{M}_n(\mathbb{C})$ ($n \geqslant 2$) contient au moins une matrice singulière non nulle (une matrice singulière est une matrice non inversible).

Démonstration. On considère (A, B) une base d'un tel plan. Si B est singulière, OK. On peut donc supposer B inversible. Alors :

$$\forall \lambda \in \mathbb{C},\ \det(A = \lambda B) = \underbrace{\det(B)}_{\neq 0} \underbrace{\det(\lambda I_n - B^{-1}A)}_{\text{de degré } n}$$

D'après le théorème de d'Alembert-Gauss, il existe donc $\lambda \in \mathbb{C}$ tel que $\det(A + \lambda B) = 0$. Et $A + \lambda B \neq 0$ car $1 \neq 0$ et (A, B) est libre. Donc $A + \lambda B$ est bien une matrice singulière non nulle. $\square$

$\det(A + N)$: commutation ; nilpotence et inversibilité

Soit $N \in \mathcal{M}_n(\mathbb{K})$ une matrice nilpotente. Que dire de $\det(A + N)$ pour $A \in \mathcal{GL}_n(\mathbb{K})$ commutant avec N ?

Démonstration. On commence par le cas simple où $A = I_n$. En trigonalisant N, $I_n + N$ est semblable à une matrice triangulaire supérieure avec des 1 sur la diagonale donc

$$\det(I_n + N) = 1 = \det(I_n)$$

Dans le cas général, on écrit

$$\det(A + N) = \det(A)\det(I_n + A^{-1}N)$$

Or, A et N commutent, donc A^{-1} et N commutent et $A^{-1}N$ est nilpotente. D'après le cas précédent, on en déduit que

$$\det(A + N) = \det(A) \times 1 = \det(A)$$

$\square$

$\det(A+N)$ avec commutation et nilpotence

Soit $N \in \mathcal{M}_n(\mathbb{K})$ une matrice nilpotente. Montrer que si $A \in \mathcal{M}_n(\mathbb{K})$ commute avec N, alors $\det(A) = 0 \implies \det(A+N) = 0$ (voir l'exercice précédent).

Première méthode. Raisonnement par densité avec $A_\lambda = A - I\lambda$ qui est inversible au voisinage de 0 et commute avec N. On utilise l'exercice précédent et on conclut par continuité du déterminant ou polynomialité. □

Deuxième méthode (sans utiliser l'exercice précédent). On considère a et n les endomorphismes canoniquement associés. Alors par commutation $\mathrm{Ker}(a)$ est stable par n. Dans une base adaptée à $\mathrm{Ker}(a)$:

$$A = \begin{pmatrix} (0) & (*) \\ (0) & (*) \end{pmatrix} \quad \text{et} \quad N = \begin{pmatrix} P & (*) \\ (0) & (*) \end{pmatrix}$$

Donc

$$A + N = \begin{pmatrix} P & (*) \\ (0) & (*) \end{pmatrix}$$

Or, l'induit de n sur $\mathrm{Ker}(a)$ est aussi nilpotent et $\mathrm{Ker}(a)$ n'est pas l'espace nul donc P est non inversible. Un déterminant triangulaire par blocs conclut. □

Sous-espaces stables par un endomorphisme nilpotent

En dimension finie égale à n, si u est nilpotent d'indice n, les sous-espaces stables par u sont exactement les $\mathrm{Ker}(u^k)$ pour $k \in [\![0, n]\!]$.

Démonstration. En effet, soit F un sous-espace stable par u de dimension k. Alors $\chi_{u_F} = X^k$ donc $u_F^k = 0$ donc $F \subset \mathrm{Ker}(u^k)$, et on a l'égalité par dimension (en utilisant la concavité des noyaux itérés). □

Caractérisation des matrices nilpotentes

Si $A \in \mathcal{M}_n(\mathbb{C})$ est une matrice carrée telle que $\forall k \in \mathbb{N}^*,\ \mathrm{Tr}(A^k) = 0$, alors A est nilpotente.

Démonstration. On trigonalise puis deux méthodes sont possibles : utiliser un déterminant de Vandermonde ou des polynômes interpolateurs de Lagrange. □

Remarque. Le résultat reste vrai si cette égalité n'est vrai que pour $k \in [\![1, n]\!]$. Cependant, cela est beaucoup difficile à démontrer puisque cela fait appel aux fonctions symétriques élémentaires et aux formules de Newton (*cf* le premier DM de l'année).

Remarque. L'idée de la démonstration avec les polynômes interpolateurs de Lagrange sert souvent lorsqu'on à un prédicat P avec une hypothèse en $\forall k,\ P(k)$.

Trace et nilpotence (version énervée du précédent)

1. Montrer que $A \in \mathcal{M}_n(\mathbb{C})$ est nilpotente si, et seulement si, pour tout $k \in [\![1, n]\!]$, $\mathrm{Tr}(A^k) = 0$.
2. Montrer que A et B dans $\mathcal{M}_n(\mathbb{C})$ ont même polynôme caractéristique si, et seulement si, pour tout $k \in \mathbb{N}$, $\mathrm{Tr}(A^k) = \mathrm{Tr}(B^k)$.
3. (Très difficile) Montrer, plus généralement, que A et B dans $\mathcal{M}_n(\mathbb{C})$ ont même polynôme caractéristique si, et seulement si, pour tout $k \in [\![1, n]\!]$, $\mathrm{Tr}(A^k) = \mathrm{Tr}(B^k)$.
4. Application : montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{C})$ telle que $\forall k \in [\![1, n-1]\!]$, $\mathrm{Tr}(A^k) = 0$ et $\mathrm{Tr}(A^n) \neq 0$ est nécessairement diagonalisable.

Démonstration.

1. Dans le sens direct, trigonaliser A : toutes ses valeurs propres sont nulles et les traces des puissances valent des sommes de 0 donc 0. Dans le sens réciproque, on trigonalise A puis on fait apparaître une matrice de Vandermonde avec les puissances des valeurs propres distinctes, qui multipliée par le vecteur des valeurs propres multipliées par leurs multiplictés fait 0. On en déduit que la seule valeur propre est 0 ce qui conclut.
2. Dans le sens direct, A et B ont donc les même valeurs propres. On trigonalise et le résultat s'obtient facilement. Dans le sens réciproque, on note λ_i et μ_i les valeurs propres respectives de A et B comptées avec multiplicité. Par linéarité, on a l'égalité :
$$\forall P \in \mathbb{C}[X],\ \sum_{i=1}^{n} P(\lambda_i) = \sum_{i=1}^{n} P(\mu_i)$$
car cette relation est linéaire en P et on a l'égalité sur la base canonique de $\mathbb{C}[X]$ en traduisant l'hypothèse après trigonalisation. En utilisant les polynômes interpolateurs de Lagrange associés à la réunion des spectre de A et B, on trouve que tout élément de cette réunion à même multiplicité chez A et chez B. Donc A et B ont même polynôme caractéristique.
3. Le sens direct est toujours immédiat. Dans le sens réciproque, on cette fois seulement :
$$\forall P \in \mathbb{C}_n[X],\ \sum_{i=1}^{n} P(\lambda_i) = \sum_{i=1}^{n} P(\mu_i)$$
et on veut montrer que
$$\prod_{i=1}^{n}(X - \lambda_i) = \prod_{i=1}^{n}(X - \mu_i)$$
ce qui revient à une égalité des fonctions symétriques élémentaires. Or, on a l'égalité des sommes de Newton. Il suffit alors de prouver que les sommes de Newton et les fonctions symétriques élémentaires s'expriment les unes en fonction des autres. Cela se fait, mais c'est long et difficile. Se référer au premier DM de l'année.
4. On pose $x = \mathrm{Tr}(A^n) \neq 0$. On considère alors :
$$B = \frac{x}{\sqrt[n]{n}}\mathrm{Diag}(\omega, \dots, \omega^{n-1})$$

avec $\omega = e^{i2\pi/n}$. Alors les traces des k premières puissances de B sont égales aux traces de k premières puissances de A. Donc A et B ont même polynôme caractéristique. Or, B est diagonalisable, donc A aussi. Autre façon de faire : $X^n - \gamma^n = 0$. On considère C la matrice compagnon de ce polynôme, et C convient (ses puissances décalent les diagonales).

□

Application de l'exercice précédent

Soit $(A, B) \in \mathcal{M}_n(\mathbb{C})^2$ tel que A et $AB - BA$ commutent. Montrer en utilisant l'exercice précédent que $AB - BA$ est nilpotente.

Démonstration. Il suffit de montrer que les traces des puissances sont nulles. Or pour $k \in \mathbb{N}$:

$$\begin{aligned}(AB - BA)^{k+1} &= (AB - BA)(AB - BA)^k \\ &= AB(AB - BA)^k - BA(AB - BA)^k \\ &= A\left[B(AB - BA)^k\right] - \left[B(AB - BA)^k\right] A\end{aligned}$$

par commutation. Donc $\mathrm{Tr}((AB - BA)^{k+1}) = 0$. Donc $AB - BA$ est nilpotente. □

Degré du PGCD des polynômes caractéristiques

Soit A et B dans $\mathcal{M}_n(\mathbb{K})$. on suppose qu'il existe X dans $\mathcal{M}_n(\mathbb{K})$ de rang r tel que $AX = XB$. Montrer que le PGCD de χ_A et χ_B est de degré au moins r.

Démonstration. Sr ramener à $X = J_r$ par équivalence. Ensuite, écrire A et B par blocs. La condition donne le fait que les blocs supérieures gauches de A et B sont égaux, que le bloc supérieure droit de B est nul et que le bloc inférieur gauche de A est nul. Donc le polynôme caractéristique du bloc supérieur gauche divise les polynômes caractéristiques de A et de B, donc leur PGCD. □

Polynôme caractéristique de $AM + B$ et nilpotence

Soit A et B deux matrices de $\mathcal{GL}_n(\mathbb{C})$.

1. On suppose que $\forall M \in \mathcal{M}_n(\mathbb{C}),\ \chi_{AM+B} = \chi AM$. Montrer que B est nilpotente. Montrer que
$$\forall M \in \mathcal{M}_n(\mathbb{C}),\ \mathrm{Tr}(BAM) = 0$$
En conclure que $BA = 0$.
2. Réciproquement, on suppose B nilpotente et $BA = 0$. Montrer que
$$\forall M \in \mathcal{M}_n(\mathbb{C}),\ \chi_{AM+B} = \chi_{AM}$$

Démonstration. 1. Pour montrer que B est nilpotente, prendre $M = 0$ et utiliser le théorème de Cayley-Hamilton. Ensuite, en trigonalisant, on a :

$$\forall k \in \mathbb{N}^*,\ \mathrm{Tr}((AM + B)^k) = \mathrm{Tr}((AM)^k)$$

Or, comme B est nilpotente, on a

$$\forall k \in \mathbb{N}^*,\ \mathrm{Tr}(B^k) = 0$$

Pour $k = 2$, on obtient :

$$\mathrm{Tr}((AM)^2) + \mathrm{Tr}(AMB) + \mathrm{Tr}(BAM) + \underbrace{\mathrm{Tr}(B^2)}_{=0} = \mathrm{Tr}((AM)^2)$$

donc $2\mathrm{Tr}(BAM) = 0$ et on conclut car $\mathbb{C}$ est de caractéristique nulle. Ensuite, c'est l'exercice classique : ici prendre $M = (\overline{BA})^T$ va plus vite.

2. Réciproquement, on calcule en utilisant le fait pour $\lambda \in \mathbb{C}^*$, $B - \lambda I_n$ est inversible. Alors :

$$\begin{aligned}\det(\lambda I - B - AM) &= \lambda^n \det(I - (\lambda I - B)^{-1}AM) \\ &= \lambda^n \det\left(I - \frac{1}{\lambda}AM\right) \\ &= \det(\lambda I - AM)\end{aligned}$$

puisque $(\lambda I - B) = \lambda A$ par hypothèse donc

$$(\lambda I - B)^{-1}A = \frac{1}{\lambda}A$$

On conclut puisque $\mathbb{C}$ est infini.

□

Endomorphismes cycliques

Soit u un endomorphisme d'un espace vectoriel E de dimension finie n. On suppose que u est cyclique, *ie* qu'il existe un vecteur x de E tel que

$$E = \mathrm{Vect}(x, u(x), \ldots, u^{n-1}(x))$$

Montrer que les sous-espaces vectoriels de E stables par u sont en nombre fini et tous de la forme $\mathrm{Vect}\{u^k(y) \mid k \in \mathbb{N}\}$ avec $y \in E$.

Démonstration. S'intéresser à des polynômes annulateurs. □

Produit de n nilpotentes qui commutent

Soit $A_1, \ldots, A_n$ des matrices nilpotentes de $\mathcal{M}_n(\mathbb{K})$ qui commutent deux à deux. Montre que $A_1 A_1 \cdots A_n = 0$.

Démonstration. Les noyaux sont stables par commutation. La nilpotence diminue strictement le rang à chaque nouvelle matrice. il est plus facile de le formaliser en termes d'applications linéaires (sinon, cela est rapide en les cotrigonalisant). □

Application du cours

La matrice $A = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 4 & 5 & 6 \\ 0 & 0 & 7 & 8 \\ 0 & 0 & 0 & 9 \end{pmatrix}$ est-elle diagonalisable ? A quelle condition la matrice $B = \begin{pmatrix} \lambda I_p & X \\ (0) & \mu I_q \end{pmatrix}$ avec $X \in \mathcal{M}_{p,q}(\mathbb{K})$ et $(\lambda, \mu) \in \mathbb{K}^2$ est-elle diagonalisable ?

Démonstration.

- Elle est triangulaire supérieure donc son polynôme caractéristique est

$$\chi_A = X(X-4)(X-7)(X-9)$$

  Il est scindé à racines simples donc A est diagonalisable.
- Si $\lambda = \mu$, B est diagonalisable si, et seulement si, $X = 0$. Si $\lambda \neq \mu$, B est toujours diagonalisable (passer par la dimension des sous-espaces propres).

$\square$

Une matrice tridiagonale symétrique

On considère

$$A = \begin{pmatrix} 0 & 1 & & (0) \\ 1 & 0 & \ddots & \\ & \ddots & \ddots & 1 \\ (0) & & 1 & 0 \end{pmatrix}$$

1. Déterminer les valeurs propres et les vecteurs propres de A en utilisant une suite récurrente. On pourra commencer par chercher les valeurs propres réelles en les mettant sous la forme $2\cos(\theta)$ ou $\pm 2\cosh(\theta)$.
2. Déterminer une matrice de passage P convenable et son inverse (on pourra calculer $P^T P$).

Démonstration. Remarquons que la matrice est symétrique réelle donc orthodiagonalisable : ainsi, toutes ses valeurs propres sont réelles et on peut trouver une matrice de passage orthogonale, ce qui explique les indications.

1. L'équation aux éléments propres fournit la relation de récurrence linéaire suivante pour $AX = \lambda X$:

$$\forall k \in [\![1, n]\!],\ x_{k-1} + x_{k+1} = \lambda x_k$$

   Si $|\lambda| < 2$, on écrit $\lambda = 2\cos(\theta)$ et

$$\forall x \in [\![1, n]\!],\ x_k = A\cos(k\theta) + B\sin(k\theta)$$

   Or, $x_0 = A = 0$ et

$$x_{n+1} = \underbrace{B}_{\neq 0} \sin((n+1)\theta) = 0$$

donc

$$\theta = \frac{l\pi}{n+1}$$

On a donc les vecteurs propres

$$X_k^{(l)} = \begin{pmatrix} \sin\left(\frac{l\pi}{n+1}\right) \\ \vdots \\ \sin\left(\frac{ln\pi}{n+1}\right) \end{pmatrix}$$

et la matrice de passage

$$P = \left(\sin\left(\frac{kl\pi}{n+1}\right)\right)_{1\leqslant k,l\leqslant n}$$

Ensuite, si $|\lambda| > 2$, on a une matrice à diagonale domianante donc inversible donc pas de valeur propre. Mais de toute façon, on a déjà n valeurs propres distinctes donc il n'y en a pas d'autre.

2. En calculant (formules de trigo et sommes géométriques d'exponentielles), on trouve $P^T P = \dfrac{n}{2} I_n$. On prend finalement

$$\tilde{P} = \sqrt{\frac{2}{n}} P \in \mathcal{O}_n(\mathbb{R})$$

comme matrice de passage.

□

Une CNS de diagonalisabilité

Soit u un endomorphisme d'un $\mathbb{C}$-espace vectoriel de dimension finie. montrer que u est diagonalisable si, et seulement si, tout sous-espace vectoriel stable par u admet un supplémentaire stable par u.

Démonstration. Dans le sens direct, si u est diagonalisable et F est stable par u, alors u_F est diagonalisable. on complète une base de diagonalisation deu_F avec des vecteurs propres de u pour obtenir un supplémentaire stable par u. Réciproquement, supposons que tout SEV stable par u admette un supplémentaire stable par u. On pose

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

qui est un SEV stable par u. Alors il admet G un supplémentaire stable par u. Or, il ne peut y avoir de vecteurs propres dans G car ils sont tous dans F. Donc puisqu'on travaille sur $\mathbb{C}$, $G = \{0\}$. Donc

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

et u est bien diagonalisable. □

Une CNS de diagonalisabilité sur $\mathbb{C}$ qui abaisse les puissances

Soit $M \in \mathcal{M}_n(\mathbb{C})$ et $p \in \mathbb{N}^*$. Montrer que M est diagonalisable si, et seulement si, M^p est diagonalisable et $\operatorname{Ker}(M) = \operatorname{Ker}(M^p)$.

Démonstration. Le sens direct est immédiat. Dans le sens réciproque, s'intéresser à des supplémentaires du noyau. Sur celui-ci ; utiliser un polynôme annulateur □

Utilisation d'une matrice compagnon

1. Soit $P = \prod_{k=1}^{n}(X - z_k) \in \mathbb{Z}[X]$ avec $(z_1, \ldots, z_n) \in \mathbb{C}^n$. Montrer que pour tout $N \in \mathbb{N}$, le polynôme $\prod_{k=1}^{n}(X - z_k^N)$ est aussi à coefficients entiers. Indication : considérer la matrice compagnon de P.
2. Application : montrer que si un polynôme à coefficients entiers a toutes ses racines complexes de module inférieur ou égal à 1, alors ses racines non nulles sont des racines de l'unité.

Démonstration. 1. On note M ma matrice compagnon de P qui est à coefficients dans $\mathbb{Z}$. Comme les racines du polynôme sont les valeurs propres de la matrice compagnon, M est semblable à $\tilde{M}$, triangulaire supérieure avec les z_k sur sa diagonale. Par conséquent, $M^N \in \mathcal{M}_n(\mathbb{Z})$ est semblable à une matrice triangulaire supérieure avec ses coefficients diagonaux égaux aux z_k^N. L'égalité des polynômes caractéristiques fournit :

$$\prod_{k=1}^{n}(X - z_k^N) = \chi_{M^N} \in \mathbb{Z}[X]$$

donc on a bien le résultat.

2. Montrons qu'il existe un nombre fini de $P \in \mathbb{Z}[X]$ unitaires de degré n dont toutes les racines sont dans le disque unité. Pour cela, il suffit de borner les fonctions symétriques élémentaires σ_k car les coefficients viennent de ces fonctions. Or :

$$|\sigma_k| \leqslant \sum_{i_1 < \ldots < i_k} \underbrace{|z_{i_1} \cdots z_{i_k}|}_{\leqslant 1} \leqslant \binom{n}{k}$$

Il y a donc un nombre fini de coefficients, donc un nombre fini de polynômes. Soit P correspondant à l'énoncé et $k \in [\![1, n]\!]$. Alors la suite $(z_k^N)_{N \in \mathbb{N}}$ est à valeurs dans un ensemble fini donc le principe des tiroirs permet de conclure.

□

Dimension trop grande $\implies$ une nilpotente non nulle

Soit V un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ de dimension strictement supérieure à $\dfrac{n(n+1)}{2}$. Montrer que V contient une matrice nilpotente non nulle.

Démonstration. Considérer l'intersection avec l'ensemble des matrices triangulaires supérieures. Cette intersection n'est pas réduite à l'espace nul car la somme des dimensions est strictement supérieure à n. Ainsi, V contient une matrice triangulaire supérieure stricte non nulle, donc une matrice nilpotente non nulle. □

Remarque. Dans ce genre d'exercices, toujours considérer une intersection avec un ensemble de matrices de référence possédant la propriété recherchée.

Utilisation d'un polynôme annulateur

Condition sur $n \in \mathbb{N}^*$ pour qu'il existe $A \in \mathcal{M}_n(\mathbb{R})$ telle que $A^2 + 2A + 5I_n = 0$?

Démonstration. Un polynôme annulateur a des racines complexes conjuguées non réelles et la matrice est diagonalisable dans $\mathbb{C}$. Les multiplicités en tant que valeurs propres des racines complexes sont égales à celles des conjuguées, donc la dimension est paire. Réciproquement, lorsque la dimension est paire, on construit un bloc 2×2 de la forme :

$$A = \begin{pmatrix} 0 & -5 \\ 1 & -2 \end{pmatrix}$$

qui convient : on peut le vérifier par le calcul ou plutôt (et c'est mieux) le voir comme la matrice compagnon du polynôme $X^2 + 2X + 5$. On généralise ensuite par blocs. □

Facteur irréductible du polynôme minimal

Soit u un endomorphisme d'un $\mathbb{K}$-espace vectoriel admettant un polynôme minimal Π. Montrer que si Π admet u facteur irréductible P de degré p, alors E admet un sous-espace vectoriel de dimension p stable par u. On pourra prendre un vecteur non nul de $\mathrm{Ker}(P(u))$.

Norme d'algèbre et rayon spectral

Soit N une norme d'algèbre sur $\mathcal{M}_n(\mathbb{C})$ et $\rho(A)$ le rayon spectral de la matrice A. Alors, $\rho(A) \leqslant N(A)$.

Démonstration. A COMPLETER □

Décomposition de Jordan-Dunford multiplicative

Soit E un $\mathbb{K}$-ev de dimension finie $n \geqslant 1$ et $f \in \mathcal{GL}(E)$. Supposons χ_f scindé. Montrer qu'il existe un unique couple $(d, u) \in \mathcal{GL}(E)^2$ tel que :

- d est diagonalisable ;
- u est unipotent, *ie* il existe $m \in \mathbb{N}^*$ tel que $(u - \mathrm{id})^m = 0$;
- $f = d \circ u = u \circ d$.

Montrer de plus que d et u sont des polynômes en f.

Existence. On écrit la décomposition de E en sous-espaces caractéristiques de f :

$$E = \bigoplus_{i=1}^{s} F_{\lambda_i}$$

On note π_i la projection sur F_{λ_i} parallèlement à la somme des autres sous-espaces caractéristiques. On pose alors

$$d = \sum_{i=1}^{s} \lambda_i \pi_i$$

d est inversible, il suffit de considérer une base de trigonalisation associées à la décomposition en sous-espaces caractéristiques, et on voit alors que d est aussi diagonalisable. On pose ensuite :

$$u = d^{-1} \circ f$$

u est unipotente car dans cette base, sa matrice est triangulaire supérieure avec uniquement des 1 sur la diagonale. Puisque les π_i sont des polynômes en f, d l'est aussi. Comme $\mathbb{K}[d]$ est une algèbre et d est inversible, $d^{-1} \in \mathbb{K}[d]$ donc *a fortiori* $d^{-1} \in \mathbb{K}[f]$, et ainsi u est un polynôme en f. Par conséquent, u et d commutent et par construction $f = d \circ u$. □

Unicité. On considère un couple (d_1, u_1) qui vérifie les mêmes hypothèses. Alors u, u_1, d et d_1 commutent tous entre eux car ce sont des polynômes en f. On pose alors $g = u_1^{-1} u = d_1 d^{-1}$. g est alors diagonalisable car d_1 et d^{-1} sont codiagonalisables car commutent. Puis, u et u_1^{-1} sont cotrigonalisables donc g est trigonalisable et ses valeurs propres sont les produits des valeurs propres de u et u_1^{-1}, donc 1. Donc g est unipotente. Comme le seul endomorphisme unipotent et diagonalisable est id (car $g - \mathrm{id}$ est nilpotent est diagonalisable donc nul), on en déduit que $g = \mathrm{id}$ donc $u = u_1$ et $d = d_1$. □

Chapitre 7

Topologie générale

7.1 Points méthode

Montrer une divergence

Pour montrer qu'une suite est divergente, il suffit de montrer que la suite considérée possède au moins deux valeurs d'adhérence.

Montrer la convergence par une série télescopique

Pour montrer la convergence d'une suite $(u_n)_{n\in\mathbb{N}}$, il faut penser à étudier éventuellement la convergence de la série $\sum\limits_{n\geqslant 1}(u_{n+1}-u_n)$.

Montrer une non domination de normes

Dans la pratique, pour montrer que N_1 n'est pas dominée par N_2, on cherche souvent une suite qui, au choix :

- tend vers 0 pour N_2 mais pas pour N_1 ;
- est bornée pour N_2 mais qui ne l'est pas pour N_1.

Choix de la norme dans $\mathbb{K}^n$

Dans $\mathbb{K}^n$, on se demandera régulièrement quelle norme parmi la norme 1, la norme 2 et la norme infinie, est la plus adaptée à la situation.

Comparaison de normes

Comparer des normes N_1 et N_2 signifie déterminer si N_1 (respectivement N_2) est dominée par N_2 (respectivement N_1).

7.2 Astuces

Matrices utiles pour la conjugaison (important !) Pour travailler sur les classes de conjugaison de matrices, il peut être utile de conjuguer par la matrice

$$Q_\varepsilon := \begin{pmatrix} 1 & & & \\ & \varepsilon & & \\ & & \ddots & \\ & & & \varepsilon^{n-1} \end{pmatrix}$$

On conservera cette notation pour la suite. Notamment, si notre matrice est trigonalisable, cela est très pratique.

Application. Une matrice est nilpotente ssi la matrice nulle adhère à sa classe de similitude

Application. La classe de similitude d'une matrice diagonalisable est fermée (RESULTAT A VERIFIER)

Adhérence d'un SEV L'adhérence d'un sev est un sev. Passer par une caractérisation séquentielle pour la partie linéarité.

Application. Un hyperplan est fermé ou dense : son adhérence est un sev donc est soit lui-même (fermé), soit égale à l'espace entier (dense).

Utilisation de l'équivalence des normes Que ce soit sur les matrices, des endomorphismes d'un espace de dimension finie ou encore un $\mathbb{K}_n[X]$, penser à utiliser l'équivalence des normes pour choisir une norme pratique au vu de la situation.

Norme subordonnée à la norme 1 On note N la norme matricielle subordonnée à la norme 1. Alors :

$$N(M) = \max_{j \in [\![1,n]\!]} \left(\sum_{i=1}^{n} |m_{i,j}| \right)$$

On obtient l'inégalité assez facilement et il faut considérer un vecteur particulier pour l'égalité.

Application. Cette norme est sous-multiplicative et est liée directement aux coefficients de la matrice : si tous les coefficients sont majorés par ε en valeur absolue, alors la norme est majorée par $n\varepsilon$. C'est donc la norme à utiliser avec les matrices Q_ε.

7.3 Exercices classiques

Théorème de Gauss-Lucas

Les racines de P' sont dans l'enveloppe convexe de P lorsque $P \in \mathbb{C}[X]$.

Démonstration. Scinder P sur $\mathbb{C}[X]$ et utiliser la formule de P'/P. Prendre ensuite une racine de P' non racine de P, la mettre dans la formule précédente et utiliser la formule de l'inverse d'un nombre complexe en fonction de son conjugué et de son module carré. Passer au conjugué. Éclater pour obtenir une combinaison convexe des racines de P, et vérifier que c'est bien un barycentre à coefficients positifs. $\square$

Intersection finie d'ouverts denses

Une intersection finie d'ouverts denses est un ouvert dense.

Démonstration. Procéder par récurrence, il suffit donc de prouver que c'est le cas pour deux. On utilise la densité du premier pour obtenir une première intersection, puis appliquer la densité du second avec cette première intersection. $\square$

Normes faisant converger (X^k) vers n'importe quel polynôme

Il existe des normes sur $\mathbb{R}[X]$ qui font converger la suite $(X^k)_{k\in\mathbb{N}}$ vers n'importe quel polynôme.

Démonstration. Si on prend une base (Y_k), la norme

$$N\left(\sum_{k=0}^{+\infty} a_k Y_k\right) = \sum_{k=0}^{+\infty} \frac{|a_k|}{2^k}$$

fait converger la suite (Y_k) vers 0. Et si on prend un polynôme P non nul, la famille $(Z_k) = (X^0, \ldots, X^{\deg(P)-1}, P, X^{\deg(P)+1}, \ldots)$ est une base de $\mathbb{K}[X]$. Alors, la norme

$$N\left(\sum_{k=0}^{+\infty} a_k Z_k\right) = \left|\sum_{k=0}^{+\infty} a_k\right| + \sum_{\substack{k=0 \\ k\neq\deg(P)}}^{+\infty} \frac{|a_k|}{2^k}$$

fait converger (X^k) vers P. $\square$

Algèbre normée de dimension finie et unités

Si $N(a) < 1$ (avec N une norme sous-multiplicative), alors $1 - a \in \mathcal{U}(A)$, d'inverse la somme de série des a^n

Démonstration. La série des a^n est absolument convergente donc convergente en dimension finie. On vérifie que c'est bien l'inverse par continuité du produit (bilinéarité en dimension finie). $\square$

Application. L'ensemble des unités d'un telle algèbre est un ouvert : en effet, si $a \in \mathcal{U}(a)$, remarquer que $a + h = a(1 - (-a^{-1}h))$ et prendre h pour rentrer dans les hypothèses de norme strictement plus petite que 1.

Valeurs d'adhérence

L'ensemble des valeurs d'adhérence de la suite (u_n) est

$$\mathrm{Adh}(u) = \bigcap_{n \in \mathbb{N}} \overline{\{u_p | p \geqslant n\}}$$

C'est donc un fermé comme intersection de fermés.

Démonstration. C'est une simple réériture de la définition des valeurs d'adhérence. □

Chapitre 8

Topologie et continuité

8.1 Points méthode

Continuité d'une fonction de plusieurs variables

La continuité d'une fonction de plusieurs variables ne se ramène **JAMAIS** uniquement à la continuité de fonctions d'une variable. On essaye alors d'utiliser les théorèmes généraux, et on effectue des majorations pour les prolongements par continuité.

Utilisation de la lipschitzianité

Pour montrer qu'une application est continue, on commence souvent par regarder si elle est lipschitzienne car si c'est le cas, c'est en général la manière la plus rapide de justifier la continuité.

Prouver une non continuité

Pour prouver qu'une application linéaire n'est pas continue, on peut prouver qu'elle n'est pas continue en 0. Comme $u(0) = 0$ par linéarité, il suffit d'exhiber une suite (x_n) tendant vers 0 mais telle que la suite $(u(x_n))$ ne tende pas vers 0. Sinon, on peut chercher une suite (x_n) telle que $(u(x_n))$ ne soit pas bornée.

Calcul d'une norme subordonnée

Pour montrer que la norme subordonnée de u vaut C, on commence généralement par montrer que $\forall x \in E,\ \|u(x)\| \leqslant C\|x\|$, puis :

- si l'on y arrive, on exhiber un vecteur x non nul vérifiant $\|u(x)\| = C\|x\|$;
- sinon, on cherche une suite (x_n) de vecteurs non nuls telle que $\dfrac{\|u(x_n)\|}{\|x_n\|} \to C$.

8.2 Astuces

Exploitation de la propriété de continuité Pour exploiter la propriété de continuité $\forall \varepsilon > 0,\ \exists \delta,\ \ldots$, il peut être utile de prendre $\varepsilon = 1$ (voire 12).

Continuité du passage à l'inverse matriciel L'application

$$\begin{array}{rcl} \mathcal{GL}_n(\mathbb{K}) & \longrightarrow & \mathcal{GL}_n(\mathbb{K}) \\ A & \longmapsto & A^{-1} \end{array}$$

est continue lorsque $\mathbb{K} = \mathbb{R}$ ou $\mathbb{K} = \mathbb{C}$.

Démonstration. Utiliser la formule de la comatrice. La comatrice et le déterminant sont continus car polynomiaux. □

8.3 Exercices classiques

Chapitre 9

Compacité, connexité par arcs

9.1 Points méthode

Montrer une non compacité

Une méthode classique pour montrer qu'une partie (non fermée bornée) est non compacte est d'essayer d'en exhiber une suite (u_n) vérifiant $\forall p \neq q,\ d(u_p, u_q) \geqslant \alpha$, où α est un réel strictement positif.

Montrer une convergence dans un compact

Pour montrer qu'une suite (u_n) à valeurs dans un compact converge vers l, on peut montrer que toute valeur d'adhérence de (u_n) est égale à l.

Utilisation des fonctions coordonnées

On considère f à valeurs dans un espace de dimension finie égale à n et f_i ses fonctions coordonnées dans une base de l'espace d'arrivée.

- f admet une limite finie en a adhérent à A si, et seulement si, f_i admet une limite finie pour tout $i \in [\![1, n]\!]$.
- f est continue sur A si, et seulement si, toutes les fonctions f_i sont continues sur A.
- On a le même résultat en remplaçant "continue" par "uniformément continue" ou "lipschitzienne".

9.2 Astuces

Montrer une connexité par arcs On commence toujours par vérifier si l'ensemble n'est pas étoilé par rapport à un de ses points ou carrément convexe. Ensuite, on regarde s'il peut être interprété comme l'image d'un connexe par arcs par une application continue. Sinon, on revient à la définition et on improvise selon la situation (on peut utiliser des théorèmes de structure par exemple pour les matrices inversible).

Déterminer des composantes connexes par arcs / Montrer une non connexité par arcs On exhibe une application continue adaptée aux objets considérés (le déterminant pour les matrices inversibles, la trace pour les projecteurs et les symétries). Si l'image de l'ensemble a plus de deux composantes connexes par arcs, alors l'ensemble de départ n'est pas connexe par arcs, et il a autant de composantes connexes par arcs qu'il y a de composantes connexes par arcs dans l'image.

Tout ouvert de $\mathbb{R}$ est réunion au plus dénombrable d'intervalles ouverts Les composantes connexes par arcs de cet ouvert sont des intervalles ouverts par résultat de cours. On cale alors un rationnel par composante connexe par arcs, ce qui prouve qu'il ya un nombre au plus dénombrable de composantes connexes par arcs.

Application. Cette méthode de caler un rationnel dans un sous-ensemble pour montrer qu'il y a un nombre au plus dénombrable de trucs est assez générale. Par exemple, cela permet de montrer qu'une fonction monotone admet un nombre au plus dénombrable de points de discontinuité.

Extraction double Si on dispose de deux suites (u_n) et (v_n) à valeurs dans des compacts K_1 et K_2 et si on veut prendre une extraction qui converge pour les deux suites, il est plus rapide de considérer la suite $((u_n, v_n))$ à valeurs dans le compact $K_1 \times K_2$ que d'extraire de l'une, puis d'extraire de nouveau.

$\mathbb{C}$ privé d'une partie dénombrable Si D est une partie dénombrable de $\mathbb{C}$, alors $C \setminus D$ est connexe par arcs. Démonstration (faire un dessin) : on se donne x et y des complexes de $\mathbb{C} \setminus D$ et on note Δ la médiatrice de $[x, y]$. Pour tout m, on définit p_m comme la concaténation du segment $[x, m]$ avec le segment $[m, y]$. Comme il y un un nombre indénombrable de p_m et que D est dénombrable, il existe un m_0 tel que p_{m_0} soit entièrement contenu dans $\mathbb{C} \setminus D$. Ainsi, $\mathbb{C} \setminus D$ est connexe par arcs.

Montrer une non compacité Pour montrer qu'une partie n'est pas compacte ou créer une absurdité, on peut utiliser/créer une suite dont on ne pourra pas extraire une suite convergente : il s'agit d'une suite (u_n) telle qu'il existe $\varepsilon > 0$ tel que

$$\forall (m, n) \in \mathbb{N}^2,\ m \neq n \implies d(u_m, u_n) \geqslant \varepsilon$$

Application. Permet de montrer la précompacité d'un ensemble compact (tout compact est recouvert par un nombre fini de boules ouvertes de même rayon pour un rayon strictement positif quelconque) $\rightarrow$ *cf* la partie exercices classiques.

9.3 Exercices classiques

Compacité de $\mathcal{O}_n(\mathbb{R})$ et $\mathcal{U}_n(\mathbb{C})$

$\mathcal{O}_n(\mathbb{R})$ et $\mathcal{U}_n(\mathbb{C})$ sont compacts.

Démonstration. Ce sont des fermés bornés en dimension finie, donc compacts. Le caractère fermé s'obtient car ce sont les images réciproques de fermés par des applications continues. Le caractère borné s'obtient en considérant les colonnes par exemple. En fonction de la norme choisie, les bornes peuvent varier. □

Application. La compacité de $\mathcal{O}_n(\mathbb{R})$ permet de prolonger des théorèmes d'existence de plusieurs décompositions dans le chapitre d'espace euclidiens

Théorème des compacts emboîtés

Une suite décroissante de compacts (K_n) tous non vides est d'intersection non vide.

Démonstration. En effet, prendre $\forall,\ x_n \in K_n$. Alors la suite (x_n) est à valeurs dans K_0 donc admet une valeur d'adhérence x. On montre que x appartient à tous les K_p. Si $n \geqslant p$, alors $x_{\varphi(n)} \in K_p$ car

$$\varphi(n) \geqslant \varphi(p) \geqslant p$$

donc par le caractère caractère fermé de K_p, $x \in K_p$. Donc x appartient à l'intersection des K_n, qui est donc non vide. □

Application. Premier théorème de Dini, variante dénombrable du point fixe de Kakutani

Précompacité

Si A est compacte, pour tout $\varepsilon > 0$, il existe une parie finie F de A telle que

$$A \subset \bigcup_{x \in C} B(x, \varepsilon)$$

On dit que A est **précompacte**.

Démonstration. Raisonner par l'absurde et construire par récurrence une suite d'éléments qui sont deux à deux à distances au moins égale à ε. Cette suite ne peut pas admettre de valeur d'adhérence, ce qui est absurde. □

Application. Preuve du théorème de Borel-Lebesgue ; permet de faire des extractions diagonales.

Théorème de Borel-Lebesgue

A est compacte si, et seulement si, de tout recouvrement de A par des ouverts, on peut extraire un sous-recouvrement fini ouvert de A.

Application. Lemme de Croft ; variante quelconque du point fixe de Kakutani.

Théorème de Riesz

Un espace vectoriel normé est de dimension finie si, et seulement si, sa sphère unité est compacte.

Connexité par arcs des matrices nilpotentes et non inversibles

L'ensemble des matrices nilpotentes et des l'ensemble des matrices non inversibles sont connexes par arcs.

Démonstration. Ils sont étoilés par rapport à la matrice nulle. □

Connexité par arcs de $\mathcal{GL}_n(\mathbb{C})$

L'ensemble $\mathcal{GL}_n(\mathbb{C})$ est connexe par arcs.

Démonstration. Pour deux matrices inversibles A et B à coefficients complexes, priver $\mathbb{C}$ de l'ensemble fini des racines de

$$\det((1-z)A + zB)$$

qui est polynomial en z, ce qui reste alors connexe par arcs. On relie alors nos matrices par un chemin continu. □

Composantes connexes par arcs de $\mathcal{GL}_n(\mathbb{R})$

En revanche, $\mathcal{GL}_n(\mathbb{R})$ n'est pas connexe par arcs. Les composantes connexes par arcs de $\mathcal{GL}_n(\mathbb{R})$ sont exactement les matrices de déterminant strictement positif et les matrices de déterminant strictement négatif.

Démonstration. Pour la non connexité par arcs, son image par le déterminant (continu) possède deux composantes connexes par arcs, $\mathbb{R}_+^*$ et $\mathbb{R}_-^*$. Pour obtenir les composantes connexes par arcs, on peut appliquer un théorème de structure sur les matrices inversible (suite de transpositions avec une dilatation en dernier) et relier continument toutes ces matrices les unes aux autres. □

Connexité par arcs des matrices symétriques et leurs variantes

$S_n(R)$, $S_n^+(\mathbb{R})$ et $S_n^{++}(\mathbb{R})$ sont connexes par arcs.

Démonstration. Ils sont convexes. □

Matrices bistochastiques

L'ensemble des matrices bistochastiques, *ie* des matrices à coefficient positifs dont la somme des coefficients pour chaque ligne et chaque colonne fait 1, est une ensemble compact et convexe (donc *a fortiori* connexe par arcs).

Démonstration. Cet ensemble est fermé et borné en dimension finie donc compact. La convexité se vérifie à la main. □

Application. Important : utilisation des matrices orthogonales et bistochastiques Se souvenir que si on a une matrice orthogonale, la matrice dont les coefficients sont les carrés des coefficients de la matrice orthogonale est bistochastique.

Théorème de Kakutani

Pour un compact convexe non vide K, une application linéaire continue qui stabilise K admet un point fixe.

Démonstration. Pour cela, introduire

$$v_n = \frac{1}{n+1} \sum_{k=0}^{n} u^k$$

qui stabilise aussi K par convexité. Alors $u(v_n(x)) - v_n(x)$ tend vers 0 avec $x \in K$ car K est non vide. Or, $v_n(x)$ admet une valeur d'adhérence, et on conclut que cette valeur d'adhérence est un point fixe de u par continuité. $\square$

Application. Dans le cas où on a une famille d'endomorphismes qui commutent, on peut montrer qu'ils ont un point fixe commun. En effet, l'ensemble des points fixes de la première est alors convexe compact non vide et on recommence. En fonction du nombre d'applications dont on dispose, on peut conclure par récurrence si on en a un nombre fini, par les compacts emboîtés si on en a un nombre dénombrable, voire avec Borel-Lebesgue si on n'est pas dans les cas précédents.

Chapitre 10

Espaces euclidiens

10.1 Points méthode

Matrices orthogonalement semblables

Pour montrer que deux matrices A et B de $\mathcal{M}_n(\mathbb{R})$ sont orthogonalement semblables, on pourra montrer qu'il existe une base orthonormée de $\mathbb{R}^n$ dans laquelle l'endomorphisme canoniquement associé à A a pour matrice B.

10.2 Astuces

Stricte convexité de la sphère unité Pour un EVN (donc pour un espace euclidien), la boule unité est strictement convexe (le faire par contraposée).

Application. Si $[u, v] \subset \mathcal{O}(E)$, alors $u = v$.

Nouveau produit scalaire Si $(\cdot|\cdot)$ est un produit scalaire sur E, on peut définir un produit scalaire sur $E \times \mathbb{R}$ par :

$$\langle (x, \lambda), (y, \mu) \rangle := (x|y) + \lambda\mu$$

Application. Montrer que si $(x_i|x_j) = -1$ pour $i \neq j$, alors

$$\sum_{i=1}^{n} \frac{1}{1 + \|x_i\|^2} \leqslant 1$$

On pourra utiliser l'inégalité de Bessel.

Une CS d'orthogonalité Si $\|x\| = \|y\|$, alors $x + y \perp x - y$ (se voit bien graphiquement), le faire en développant le produit scalaire.

Application. Un endomorphisme qui conserve la norme est une constante fois un endomorphisme orthogonal : en effet, l'étude précédente montre dans une analyse qu'un tel endomorphisme est de norme constante sur les sphère, et on se ramène à un endomorphisme de norme 1 sur la sphère unité par homogénéité.

Une façon de montrer qu'un endomorphisme est nul Dans un espace préhilbertien, pour montrer qu'un endomorphisme est nul, on peut montrer qu'il est à la fois symétrique et antisymétrique.

Obtenir une forme plus simple d'une forme linéaire Pour "décomposer" une forme linéaire, on peut lui donner une nouvelle forme plus agréable, on introduit un produit scalaire et on s'assure d'être en dimension finie. On peut alors utiliser le théorème de représentation !

Utilisation d'un autre produit scalaire De façon générale, introduire un produit scalaire bien choisi, même si ce peut être difficile, est souvent utile car on dispose alors de plus d'outils !

Utilisation du théorème de représentation Si l'énoncé concerne en parallèle des formes linéaires et des espaces euclidiens, penser au théorème de représentation.

Symétrisation d'un problème avec des matrices symétriques définies positives Lorsqu'on travaille avec des matrices symétriques réelles définies positives, on peut écrire $A = S^2$ avec $S \in \mathcal{S}_n^{++}(\mathbb{R})$ pour ensuite écrire :

$$A + B = S(I + S^{-1}BS^{-1})S$$

Cela permet notamment de passer au déterminant pour se ramener à un cas plus simple.

Prouver un résultat sur $\mathcal{S}_n^+(\mathbb{R})$ par densité Pour prouver un résultat dans $\mathcal{S}_n^+(\mathbb{R})$, on peut commencer par le prouver dans $\mathcal{S}_n^{++}(\mathbb{R})$ puis l'étendre par continuité puisque $\mathcal{S}_n^{++}(\mathbb{R})$ est dense dans $\mathcal{S}_n^+(\mathbb{R})$.

Le rayon spectral est une norme sur $\mathcal{S}_n(\mathbb{R})$ On note ρ le rayon spectral. Il est bien à valeurs dans $\mathbb{R}_+$. Si $\rho(A) = 0$ et $A \in \mathcal{S}_n(\mathbb{R})$, alors A est diagonalisable et toutes ses valeurs propres sont nulles, donc $A = 0$. Puisque $\mathrm{Sp}(\lambda A) = \lambda \mathrm{Sp}(A)$, on obtient immédiatement l'homogénéité. En utilisant la norme 2 canonique et le fait que le rayon spectral d'une matrice symétrique est le maximum de la quantité $|X^T AX|$ pour X de norme 1, on obtient l'inégalité triangulaire.

Matrices orthogonales et triangulaires Ce sont les matrices avec uniquement des -1 ou des 1 sur la diagonale et des 0 partout ailleurs.

Trigonalisation en base orthonormée Si une matrice réelle est trigonalisable, alors elle est trigonalisable dans une base orthonormée, il suffit d'appliquer un processus d'orthonormalisation de Gram-Schmidt à la matrice de passage pour la trigonalisation.

Application. Pour une matrice trigonalisable sur $\mathbb{R}$ de valeurs propres λ_i, $A \in S_n(\mathbb{R})$ ssi

$$Tr\left(AA^T\right) = \sum_i \lambda_i^2$$

Le sens direct est immédiat avec le théorème spectral. Pour le sens réciproque, trigonaliser en base orthonormée.

Topologie de $S_n(\mathbb{R})$, $S_n^+(\mathbb{R})$ et $S_n^{++}(\mathbb{R})$ $S_n^+(\mathbb{R})$ est un fermé relatif de $S_n(\mathbb{R})$ comme l'intersection des noyaux des applications

$$X \mapsto (X|MX)$$

pour $X \in \mathbb{R}^n$. $S_n^{++}(\mathbb{R})$ est connexe par arcs car convexe. L'adhérence de $S_n^{++}(\mathbb{R})$ dans $S_n(\mathbb{R})$ est $S_n^+(\mathbb{R})$. $S_n^{++}(\mathbb{R})$ est un ouvert relatif de $S_n(\mathbb{R})$: en effet, on montre que son complémentaire dans $S_n(\mathbb{R})$ est fermé par caractérisation séquentielle et avec une suite de vecteurs de norme 1 (on utilise la compacité de la sphère unité de R^n).

10.3 Exercices classiques

Racine carrée

On a :

$$\forall u \in S^+(E),\ \exists! v \in S^+(E),\ u = v^2$$

Démonstration. Pour l'existence, orthodiagonaliser et prendre les racines carrées des valeurs propres. Pour l'unicité, on peut montrer que tout candidat est nécessairement égal à notre candidat proposé dans l'existence. Pour cela, on remarque que toute racine carré commute avec l'endomorphisme de départ, puis on considère les endomorphismes induits sur les sous-espaces propres. Les induits des racines carrées sont aussi des endomorphismes symétriques positifs, et alors on ne peut avoir que le candidat proposé dans l'existence. □

Remarque. Souvent, seul l'existence est utile, et cela est pratique car elle se démontre très rapidement.

Remarque. On a évidemment l'équivalent matriciel.

Application. Pseudo-réduction simultanée ; décomposition polaire ; en général, elle permet de symétriser un problème en prenant multipliant par la racine carrée à gauche et à droite

Décomposition polaire

Pour une matrice inversible M :

$$\exists! O \in \mathcal{O}_n(\mathbb{R}),\ \exists! S \in S_n^+(\mathbb{R}),\ M = OS$$

Démonstration. Appliquer l'existence unicité de la racine carrée à $M^T M$. L'existence reste vraie pour une matrice non inversible en utilisant la densité des matrices inversibles et la compacité de $\mathcal{O}_n(\mathbb{R})$. □

Application. Tout sous-groupe compact de $\mathcal{GL}_n(\mathbb{R})$ qui contient $\mathcal{O}_n(\mathbb{R})$ est égal à $\mathcal{O}_n(\mathbb{R})$

Décomposition OT

Pour M une matrice inversible, il existe $O \in \mathcal{O}_n(\mathbb{R})$ et T une matrice triangulaire supérieure telles que

$$M = OT$$

avec unicité de plus si on impose que les coefficients diagonaux de T soient strictement positifs.

Démonstration. L'existence reste vraie pour des matrices non inversibles avec la densité des matrices inversibles et la compacité de l'ensemble des matrices orthogonales. Pour le démontrer, appliquer un processus de Gram-Schmidt aux colonnes de la matrice M, qui forment bien une base puisque la matrice M est inversible. □

Application. Inégalité de Hadamard :

$$|\det(M)| \leqslant \prod_{j=1}^{n} \|C_j\|$$

avec les C_j les colonnes de la matrice M. pour cela, reprendre la démonstration de la décomposition OT avec le processus de Gram-Schmidt.

Matrices de Gram

C'est la matrice $G(x_k) = ((x_i|x_j))_{1\leqslant i,j\leqslant n}$. On note $\mathrm{Gram}(x_k) = \det(G(x_k))$. Ses colonnes forment une famille libre ssi la famille (x_i) est libre. Son rang ne change par si on ajoute à un x_i une combinaison linéaire de tous les autres x_k pour $k \neq i$. Le rang de la matrice de Gram est égal au rang de la famille. C'est une matrice symétrique positive. Si F est un sous-espace vectoriel dont y_1, ..., y_p est une base, on a la formule :

$$d(x, F)^2 = \frac{\mathrm{Gram}(x, y_1, \ldots, y_p)}{\mathrm{Gram}(y_1, \ldots, y_p)}$$

(commencer par le cas où $x \in F^\perp$ puis utiliser la projection orthogonal qui s'exprime comme x plus une combinaison linéaire des y_i). Le déterminant de Gram est le carré du produit mixte des vecteurs.

CNS pour qu'un projecteur soit orthogonal

Un projecteur p d'un espace euclidien est orthogonal si, et seulement si,

$$\forall x \in E,\ \|p(x)\| \leqslant \|x\|$$

Démonstration. Pour le prouver, pour $x \in \mathrm{Ker}(p)$ et $y \in \mathrm{Im}(p)$, on étudie $t \mapsto \|tx + y\|^2$ qui admet un minimum en 0 et est dérivable en 0 ce qui donne la condition de nullité du produit scalaire. □

Application. Si une composée de projecteurs orthogonaux est un projecteur, alors c'est un projecteur orthogonal.

Endomorphisme de trace nulle

Pour u un endomorphisme de trace nulle, il existe un vecteur normé x tel que $(u(x)|x) = 0$.

Démonstration. En effet, pour une BON (e_k), on doit avoir $(u(e_i)|e_i) \geqslant 0$ et $(u(e_j)|e_j) \leqslant 0$ pour un i et un j. On fait alors tourner ces vecteurs (ou on les relie rectilignement mais il faut alors renormaliser après) et on utilise le théorème des valeurs intermédiaires. □

Application. Une matrice réelle de trace nulle est orthogonalement semblable à une matrice de diagonale nulle (récurrence)

Endomorphisme toujours symétrique $u^* \circ u$

On a l'égalité $\mathrm{Ker}(u) = \mathrm{Ker}(u^* \circ u)$.

Démonstration. L'inclusion directe est imédiate, et l'inclusion réciproque s'obitient en calculant $\|x\|^2$ avec la définition de l'adjoint. On en déduit l'égalité

$$\mathrm{Im}(u^*) = \mathrm{Im}(u^* \circ u)$$

avec l'inclusion réciproque immédiate et le théorème du rang (en dimension finie donc). □

CS de linéarité

Si

$$\forall x, y,\ (u(x)|y) = (x|v(y))$$

alors u et v sont linéaires.

Démonstration. Revenir à la définition et effectuer les calculs qui correspondraient à la linéarité. □

Application. Montre la linéarité de l'adjoint dans le théorème de représentation de Riesz

Co-orthodiagonalisation

Une famille d'endomorphismes symétriques qui commutent deux à deux sont diagonalisables dans une même base orthonormée.

Démonstration. Récurrence sur la dimension. □

AA^T vs A^TA

AA^T et A^TA sont orthogonalement semblables.

Démonstration. Elles ont le même polynôme caractéristique donc les mêmes valeurs propres comptées avec multiplicité (de façon générale, $\chi_{AB} = \chi_{BA}$, mais il y a peut être plus rapide ici). Elle sont donc orthogonalement semblables à une même matrice diagonale, donc sont semblables. □

Propriété des endomorphismes de norme triple inférieure à 1

Soit u un endomorphisme de E euclidien de norme triple inférieure à 1. Alors :

$$E = \mathrm{Ker}(u - \mathrm{id}) \overset{\perp}{\oplus} \mathrm{Im}(u - \mathrm{id})$$

Démonstration. On peut construire

$$v_n = \frac{1}{n+1} \sum_{k=0}^{n} u^k(x)$$

qui vaut x sur $\mathrm{Ker}(u - \mathrm{id})$ et tend vers 0 sur $\mathrm{Im}(u - \mathrm{id})$. Cela permet de montrer que

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

v_n tend alors vers la projection sur $\mathrm{Ker}(u-\mathrm{id})$ parallèlement à $\mathrm{Im}(u-\mathrm{id})$. De plus, v_n est de norme triple inférieure à 1, donc la projection vers laquelle elle tend aussi. Cette projection est donc une projection orthogonale (*cf* une caractérisation de cette section), donc la somme directe prouvée précédemment est orthogonale. □

Réduction des endomorphismes antisymétriques

On dit que u est antisymétrique lorsque $\forall x,\ (u(x) \mid x) = 0$. Alors, la matrice d'un endomorphisme antisymétrique est diagonale par blocs, avec des blocs nuls ou des blocs de la forme

$$\begin{pmatrix} 0 & -a \\ a & 0 \end{pmatrix}$$

Démonstration. On procède par récurrence en distinguant si on possède un plan stable ou une droite stable. On utilise le fait que $(u(x)|y) = -(x|u(y))$. □

Continuité de l'application racine carrée sur les matrices symétriques positives

Démonstration. On prend A_p qui tend vers A. On montre que toutes les valeurs d'adhérence de $A_p^{1/2}$ sont nécessairement $B^{1/2}$ par unicité de la limite et compacité des ensembles mis en jeu (on a alors affaire à des fermés bornés car le spectre des matrices est borné). □

Blocs principaux de matrices symétriques positives

Les blocs principaux d'une matrice symétrique positive (resp. strictement positive) sont positifs (resp.strictement positifs). Réciproquement, une matrice symétrique dont tous les blocs principaux ont des déterminants strictement positifs est définie positive. Le résultat est faux pour des déterminants positifs.

Démonstration. Pour la première affirmation, il suffit de compléter le vecteur par un vecteur avec des 0. Pour la deuxième, faire une récurrence et des produits par blocs assez moches. □

AB diagonalisable

Si $A \in S_n^{++}(\mathbb{R})$ et $B \in S_n(\mathbb{R})$ alors AB est dz.

Démonstration. En effet, avec C la racine carrée de A (donc inversible), on écrit :

$$AB = C(CBC)C^{-1} = CP^T DPC^{-1}$$

avec le théorème spectral appliqué à B. □

Inégalités sur des déterminants (convexité ou sommes) dans $S_n^+(\mathbb{R})$

Soient A et B des matrices de $S_n^+(\mathbb{R})$. Alors on a :

$$\det(A+B) \geqslant \det(A) + \det(B)$$

et

$$\forall t \in [0,1], \quad \sqrt[n]{\det((1-t)A+tB)} \geqslant (1-t)\sqrt[n]{\det(A)} + t\sqrt[n]{\det(B)}$$

(**DERNIER RESULTAT A A VERIFIER**)

Démonstration. Procéder en augmentant la difficulté des cas peu à peu et en utilisant la racine carré. Sinon, utiliser la pseudo-réduction simultanée, ce qui permet de sauter des étapes par rapport à la première méthode. □

Egalités de Courant-Fischer

On prend $u \in S(E)$ avec E euclidien de dimension n. On note $\lambda_1 \leqslant \ldots \leqslant \lambda_n$ ses valeurs propres. On note $\mathcal{F}_k$ l'ensemble des sev de E de dimension k. Alors

$$\lambda_k = \inf_{F \in \mathcal{F}_k} \sup_{x \in S \cap F} (x|u(x))$$

Démonstration. Pour cela, prendre une BON de dz de u et montrer que $S \cap F$ a une intersection avec $\mathrm{Vect}(e_k, \ldots, e_n)$ non nulle (Grassmann) puis prendre un vecteur de norme 1 dedans, ce qui montre que tous les sup sont atteints. Pour le sens réciproque, s'intéresser à $\mathrm{Vect}(e_1, \ldots, e_k)$ et faire le produit scalaire (comme dans le cours). Pour montrer la deuxième égalité :

$$\lambda_{n+1-k} = \sup_{F \in \mathcal{F}_k} \inf_{x \in S \cap F} (x|u(x))$$

on peut appliquer la première égalité à $-u$, ce qui échange essentiellement les sup et les inf. □

Application. Inégalité d'entrelacement, inégalités de Weyl

Rayon spectral et norme d'opérateur

On considère E un espace euclidien muni d'une norme euclidienne $\|\cdot\|$ et N la norme d'opérateur associée. Soit $u \in \mathcal{L}(E)$, dont on note $\rho(u)$ le rayon spectral, *ie* la valeur absolue de la plus grande valeur propre.

1. Si $u \in \mathcal{S}(E)$, alors $N(u) = \rho(u)$.
2. De façon générale, $N(u) = \sqrt{\rho(u^* \circ u)}$.

Démonstration. On utilise le théorème spectral.

1. Considérer une base d'orthodiagonalisation, prendre la norme puis minorer les λ^2 par $\rho(u)^2$.
2. Utiliser le résultat précédent en remarquant que $u^* \circ u$ est symétrique (positif même) et utiliser le fait que
$$\|u(x)\|^2 = (u(x) \mid u(x)) = (x \mid u^* \circ u(x))$$

□

Endomorphismes normaux

Dans un espace euclidien, un endomorphisme est dit normal lorsqu'il commute avec son adjoint. Dans $\mathcal{M}_n(\mathbb{R})$, une matrice est dite normale lorsqu'elle commute avec sa transposée.

1. Donner des exemples d'endomorphismes normaux.
2. Déterminer les matrices normales de $\mathcal{M}_2(\mathbb{R})$
3. Soit u un endomorphisme normal et F un sous-espace vectoriel stable par u. Montrer que $F^\perp$ est stable par u.
4. Démontrer que pour tout endomorphisme normal, il existe une base orthonormée dans laquelle sa matrice est diagonale par blocs de la forme
$$\mathrm{Diag}(a_1 R_{\theta_1}, \ldots, a_p R_{\theta_p}, \lambda_1, \ldots, \lambda_q)$$
où les R_θ sont des matrices de rotation. Retrouver le théorème spectral et le théorème de structure des isométries vectorielles.
5. Montre qu'un endomorphisme u est normal si, et seulement si, u^* est un polynôme en u.
6. Démontrer que le produit de deux matrices normales qui commutent est un matrice normale.

Démonstration. Cet exercice est fondamental car il généralise les notions du cours, et se généralise dans le cadre des espace hermitiens. Remarquons tout de suite qu'être normal pour un endomorphisme équivaut au fait que sa matrice soit normale dans n'importe quelle base.

1. Les endomorphismes symétriques et antisymétriques.
2. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{R})$. Alors M est normale si, et seulement si :
$$\begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix} = \begin{pmatrix} a^2+c^2 & ab+cd \\ ab+cd & b^2+d^2 \end{pmatrix}$$

c'est-à-dire si, et seulement si :

$$\begin{cases} c = b \text{ ou } c = -b \\ ab + cd = ac + bd \end{cases}$$

ou encore

$$\begin{cases} c = b \\ b(a+d) = b(a+d) \end{cases} \quad \text{ou} \quad \begin{cases} c = -b \\ b(a-d) = b(d-a) \end{cases}$$

Ce sont donc exactement les matrices de la forme :

$$M = \begin{pmatrix} a & b \\ b & d \end{pmatrix} \text{ ou } M = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

3. On écrit
$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}$$
la matrice de u dans une base adaptée à $F \oplus F^\perp$. Alors M^T est la matrice de u^* dans cette même base. Or, puisque u est normal, M et M^T commutent. Par conséquent :
$$\begin{pmatrix} AA^T + BB^T & BD^T \\ DB^T & DD^T \end{pmatrix} = \begin{pmatrix} A^TA & A^TB \\ B^TA & B^TB + D^TD \end{pmatrix}$$
En particulier, $AA^T + BB^T = A^TA$ donc en passant à la trace, $\mathrm{Tr}(BB^T) = 0$. On en déduit que $B = 0$ en explicitant les coefficients de BB^T (classique). Ainsi, M est diagonale par blocs donc $F^\perp$ est stable par u.

4. Il s'agit d'une récurrence forte sur la dimension de l'espace comme dans le cours. L'initialisation est immédiate. Pour l'hérédité, on distingue deux cas et on utilise 3. :
   - si u possède une droite stable, on utilise 3. et on écrit sa matrice dans la base adaptée à la droite et son orthogonal. Cette matrice est diagonale par blocs d'après 3., et le bloc en bas à droite est aussi normal par un produit par blocs, et on conclut par hypothèse de récurrence.
   - sinon, u possède un plan stable, et on fait de même. On utilise alors la question 2 : si la matrice qui correspond au plan est symétrique, on prend une base orthonormée (on n'a pas forcément besoin du théorème spectral, on peut le faire à la main) et dans l'autre cas, on renormalise avec $\sqrt{a^2 + b^2}$ pour faire apparaître une matrice de rotation. On conclut de même par hypothèse de récurrence.

   Remarquons que les λ sont les valeurs propres de u. Alors, pour une isométrie vectorielle, les valeurs propres valent 1 ou -1 et le déterminant vaut 1 donc les a valent 1. Pour les endomorphismes symétriques, les matrices de rotation doivent être symétriques donc diagonales et on obtient bien le théorème spectral.

5. Le sens réciproque est immédiat. Dans le sens direct, utiliser la question 4 est diagonaliser par blocs la matrice de u en base orthonormée puis utiliser une interpolation de Lagrange.

6. On considère $A \in \mathcal{M}_n(\mathbb{R})$ et $B \in \mathcal{M}_n(\mathbb{R})$ telles que $AB = BA$. On note u et v les endomorphismes canoniquement associés à A et B. Alors u et v sont normaux et $uv = vu$. De plus,

par 5., il existe P et Q tels que $u^* = P(u)$ et $v^* = Q(v)$. Alors, il est clair que $uv^* = v^*u$, $u^*v = vu^*$ et $u^*v^* = v^*u^*$. Par conséquent :

$$\begin{aligned}(uv)(uv)^* &= (uv)(v^*u^*)\\ &= u(vv^*)u^*\\ &= u(v^*v)u^*\\ &= (uv^*)(vu^*)\\ &= (v^*u)(u^*v)\\ &= v^*(uu^*)v\\ &= v^*(u^*u)v\\ &= (v^*u^*)(uv)\\ &= (uv)^*(uv)\end{aligned}$$

donc uv est normal et par conséquent AB est normale.

□

Caractérisation des endomorphismes orthogonaux

Soit E un espace euclidien et $u : E \to E$ une fonction telle que

- $u(0) = 0$;
- $\forall (x, y) \in E^2,\ \|u(x) - u(y)\| = \|x - y\|$

Montrer que f est un endomorphisme orthogonal. On pourra d'abord montrer que f conserve le produit scalaire.

Démonstration. En utilisant le fait $u(0) = 0$, il est immédiat que f conserva la norme. Par polarisation, on en déduit que f conserve le produit scalaire. Ensuite, on note $e = (e_1, \dots, e_n)$ une base orthonormée de E. Par conservation du produit scalaire, $u(e)$ est une base orthonormée de E. Ainsi :

$$\forall x \in E,\ u(x) = \sum_{k=1}^{n} (u(x), u(e_k))\, u(e_k)$$

(expression dans une base orthonormée). Or, par conservation du produit scalaire :

$$\forall x \in E,\ u(x) = \sum_{k=1}^{n} (x, e_i)\, u(e_i)$$

et cette dernière expression est linéaire en x par linéarité à gauche du produit scalaire, si bien que u est linéaire. Ainsi, u est linéaire et conserve la norme, donc $u \in \mathcal{O}(E)$. □

Chapitre 11

Inégalités : minorations et majorations

Utilisation du binôme de Newton Pour majorer ou minorer $(1+u)^n - 1$, penser au binôme de Newton et écrire :

$$(1+u)^n - 1 = \sum_{k=1}^{n} \binom{n}{k} u^k$$

Ensuite, majorer ou minorer en ne conservant que certains termes de la somme.

Minoration d'une somme géométrique Pour $t \geqslant 0$, l'inégalité arithmético-géométrique permet d'obtenir l'inégalité :

$$\sum_{k=0}^{n} t^k \geqslant (n+1)t^{n/2}$$

En général, cette inégalité est très utile et permet parfois de conclure un exercice à elle seule.

Exponentielles négatives Pour des exponentielles négatives, *ie* de la forme $e - ax$ avec $a > 0$, on peut obtenir des inégalités pour $x \geqslant 0$ *via* l'inégalité de Taylor-Lagrange puisque les dérivées n-èmes sont bornées.

Une inégalité utile Se souvenir que pour deux f et g des fonctions croissantes, on a toujours l'inégalité :

$$\forall (x,y),\ \ (f(y) - f(x))(g(y) - g(x)) \geqslant 0$$

Application. Pour f et g croissantes continues par morceaux sur $[0,1]$, on a :

$$\int_0^1 f \times \int_0^1 g \leqslant \int_0^1 fg$$

On a un résultat analogue sur les espérances (qui permet d'ailleurs de démontrer le résultat précédent sur les intégrales en passant par les sommes de Riemann).

Inégalité de Jensen pour les espérances Si X est une variable aléatoire discrète réelle d'espérance finie à valeurs dans un intervalle I et si est f est une fonction convexe sur I, alors :

$$\mathbb{E}(f(X)) \geqslant f(\mathbb{E}(X))$$

Démonstration. On sait alors que $\mathbb{E}[X] \in I$. Par conséquent, il existe $C \in \mathbb{R}$ telle que

$$\forall x \in I, \ f(x) \geqslant f(\mathbb{E}[X]) + C(x - \mathbb{E}[X])$$

Il suffit alors de composer par X et d'utiliser la croissance de l'espérance en utilisant le fait que $X - \mathbb{E}[X]$ est centrée. □

Inégalité de Jensen pour les intégrales Si $f : [a,b] \to I$ est continue par morceaux et $\varphi : I \to \mathbb{R}$ est convexe, alors :

$$\varphi\left(\int_a^b f\right) \leqslant \int_a^b \varphi \circ f$$

Démonstration. Passer par les sommes de Riemann et utiliser l'inégalité de Jensen dans les sommes de Riemann. Passer à la limite dans l'inégalité pour conclure. □

Cosinus hyperbolique et exponentielle En utilisant un développement en série entière et le fait que

$$\forall k \in \mathbb{N}, \ (2k)! \geqslant 2^k k!$$

on peut montrer que

$$\forall t \in \mathbb{R}, \ \cosh(t) \leqslant e^{t^2/2}$$

Application. Cette inégalité est très utile en probabilités pour démontrer des inégalités de concentration à partir de l'inégalité de Markov.

Utilisation particulière de l'inégalité de Cauchy-Schwarz On peut appliquer l'inégalité de Cauchy-Schwarz avec uniquement des 1 pour obtenir :

$$\left(\sum_{i=1}^n x_i\right)^2 \leqslant n \sum_{i=1}^n x_i^2$$

1-lipschitzianité du sinus On a

$$\forall x \in \mathbb{R}, \ |\sin(x)| \leqslant |x|$$

Pour le redémontrer rapidement, utiliser l'inégalité des accroissements finis.

Inégalités de convexité Pour les inégalités de convexités avec des fonctions usuelles, penser à faire un schéma pour faire apparaître les tangentes, mais aussi les cordes ! On obtient par exemple :

$$\forall x \in \left[0, \frac{\pi}{2}\right], \ \frac{2x}{\pi} \leqslant \sin(x) \leqslant x$$

$$\forall x \in [0,1], \ 1 + x \leqslant e^x \leqslant 1 + (e-1)x$$

Racines n-èmes de produits de sommes pour des inégalités faisant intervenir des racines n-èmes de produits de sommes, on peut utiliser le fait que la fonction

$$x \mapsto \ln(1 + e^x)$$

est convexe sur $\mathbb{R}$ (le prouver en la dérivant deux fois). Cela permet notamment d'obtenir, pour a_i et b_i des réels positifs, l'inégalité :

$$\sqrt[n]{\prod_{i=1}^{n} a_i} + \sqrt[n]{\prod_{i=1}^{n} b_i} \leqslant \sqrt[n]{\prod_{i=1}^{n} (a_i + b_i)}$$

Renormalisation Lorsqu'on souhaite démontrer des inégalités assez complexes, penser à renormaliser pour obtenir une inégalité plus simple à démontrer.

Application. Inégalités de de Hölder et de Minkowski

Convexité de la norme au carré L'application $x \mapsto \|x\|^2$ est convexe.

Démonstration. L'inégalité triangulaire et l'homogénéité donnent l'inégalité sans les carrés, puis on utilise la convexité de la fonction $x \mapsto x^2$. □

Utilisation des coordonnées polaires pour des fonctions de deux variables Pour une fonction de deux variables réelles, pour chercher des *extrema*, des majorations ou des minoration s sur un cercle, on peut essayer de passer en coordonnées polaires : $x = r\cos(\theta)$, $y = r\sin(\theta)$ puis faire de la trigonométrie.

Log-convexité Si f est de classe $\mathcal{C}^2$ à valeurs dans $\mathbb{R}_+^*$, alors $\ln \circ f$ est convexe si, et seulement si,

$$(f')^2 \leqslant f \times f''$$

Cette inégalité peut parfois découler de l'inégalité de Cauchy-Schwarz, en particulier lorsque f est une intégrale à paramètre. L'équivalence se prouve en dérivant deux fois $\ln \circ f$.

Application. Fonction Gamma.

Chapitre 12

Suites et séries numériques

12.1 Points méthode

Utilisation d'une série télescopique

Pour étudier la convergence d'une suite $(u_n)_{n\in\mathbb{N}}$, il faut penser à étudier éventuellement la convergence de la série $\sum_{n\geqslant 1}(u_{n+1}-u_n)$.

Règle $n^\alpha u_n$

On a les différents cas.

- Si $\exists\alpha > 1\ :\ n^\alpha u_n \to 0$, alors $\sum u_n$ converge absolument.
- Si $\exists\alpha \leqslant 1\ :\ n^\alpha u_n \to +\infty$, alors $\sum u_n$ diverge.
- Si $\exists M \geqslant m > 0\ :\ m \leqslant n^\alpha u_n \leqslant M$, alors $\sum u_n$ est de même nature que $\sum n^{-\alpha}$.

Comparaison série/intégrale

Pour une comparaison série intégrale avec monotonie, on fait un dessin !

Équivalent d'un reste

Lorsque u_{n+1}/u_n admet une limite non nulle différente de 1, pour trouver un équivalent du reste, on peut sommer l'équivalent $u_{n+1} \sim lu_n$. Si (u_n) et positive sommable et vérifie ces conditions, on peut montrer alors que

$$R_n \sim \frac{u_n}{1-l}$$

Étude d'une suite récurrente

Dans l'ordre :

- Faire un dessin ;
- Trouver un intervalle stable ;
- Déterminer le signe de $f - \mathrm{id}$, la potentielle croissance de f (assure la monotonie de la suite) ou la potentielle décroissance de f (assure les monotonies de (u_{2n}) et (u_{2n+1})) ;
- Résoudre $f(x) = x$ et utiliser la continuité.

12.2 Astuces

Fonction de décalage Quand on travaille sur des sommes avec des suites : parfois introduire le shift, à savoir l'application $(u_n)_{\in\mathbb{N}} \mapsto (u_{n+1})_{n\in\mathbb{N}}$. Il s'agit d'un endomorphisme de $\mathbb{K}^{\mathbb{N}}$, et avec un peu de chance on pourra ensuite utiliser la formule du binôme de Newton sur les endomorphismes.

Étude de produits infinis Pour l'étude d'un produit infini, on veut passer au logarithme mais il faut s'assurer que tous les facteurs sont strictement positifs avant. Sinon, on peut songer à les grouper : par exemple si les facteurs de $\prod\limits_{k\geqslant 0} a_k$ sont tous strictement négatifs, alors on peut considérer

$$\sum_{k\geqslant 0} \ln(a_{2k}a_{2k+1})$$

Astuce pour ne pas s'embêter avec une somme Quand on travaille avec $\sum\limits_{k=1}^{n} a_k$, pour éviter d'avoir une discussion à faire, on peut décider de prendre $a_k = 0$ pour $k > n$ et travailler directement sur $\sum\limits_{k=1}^{+\infty} a_k = \sum\limits_{k=1}^{n} a_k$

Conjugué algébrique et binôme de Newton Quand on voit la suite $((1+\sqrt{2})^n)_{n\in\mathbb{N}}$, il faut penser à introduire $((1-\sqrt{2})^n)_{n\in\mathbb{N}}$ (c'est le conjugué algébrique !). L'avantage est que le binôme de Newton assure que $(1+\sqrt{2})^n + (1-\sqrt{2})^n$ est un entier ! Il faut penser à la même chose face à $(1+\sqrt{k})^n$ en général.

Application. Pour approfondir, on pourra remarquer que remplacer une suite géométrique de raison $1+\sqrt{2}$ par une suite géométrique de raison $1-\sqrt{2}$ permet de mieux contrôler : en effet, $|1-\sqrt{2}| < 1$ donc cette suite géométrique tend vers 0.

Utilisation d'un $\ln$ Pour montrer l'existence d'une limite d'une suite (u_n) ou d'une fonction f strictement positive, on peut montrer que la suite des logarithmes converge : on peut établir la convergence de $(\ln(u_n))_n$ ou bien de $\ln(f)$.

Application. Produits infinis typiquement, on ne peut pas faire autrement.

Utilisation des DL dans un cadre plus large Si on a besoin de faire un développement limité pénible dans le cadre d'une preuve plus large, ne pas s'embêter à calculer les coefficients s'ils ne sont pas triviaux : on les note α, β, etc. pour faire les calculs et on les détermine après si besoin.

Utilisation des restes Pour des séries dans lesquelles des restes (éventuellement d'autres séries !) interviennent dans le terme général, penser à utiliser le fait que $u_n = R_n - R_{n+1}$

Application. Nature des séries $\sum \frac{u_n}{S_n^\alpha}$ lorsque $\sum u_n$ diverge en fonction de α, et un résultat avec des restes dans l'autre cas. (VERIFIER QUE C EST BIEN DANS LE BON SENS)

Amélioration du critère de divergence Pour montrer que $\sum u_n$ diverge, on peut montrer qu'une tranche $\sum\limits_{k=a(n)}^{b(n)} u_k$ ne converge pas vers zéro (par exemple en minorant le module ou la valeur absolue) quand $n \to +\infty$, en choisissant bien a et b telles que $a(n) \to +\infty$ et $b(n) \to +\infty$ avec $(b(n)-a(n))$ bornée. On étend ainsi le critère de divergence grossière, qui ne considère qu'un unique terme, pour considérer toute une tranche.

Pousser un développement asymptotique plus loin Pour l'étude des suites implicites, idées pour obtenir un DL ou un DA à l'ordre suivant : par exemple pour

$$u_n = \alpha + \frac{1}{n} + o\left(\frac{1}{n}\right)$$

il y a deux possibilités : on peut chercher un équivalent de $un - \alpha - \frac{1}{n}$ ou bien de $n(u_n - \alpha) - 1$. Penser aux deux et utiliser le plus simple !

Passer un équivalent au $\ln$ Si (a_n) et (b_n) sont à valeurs strictement positives et tendent vers 0 ou $+\infty$, alors

$$a_n \sim b_n \Longrightarrow \ln(a_n) \sim \ln(b_n)$$

En effet, la différence est un $o(\ln(a_n))$.

Règle de Raabe-Duhamel (HP) Soit (u_n) une suite à valeurs strictement positives vérifiant :

$$u_n = 1 - \frac{\alpha}{n} + o\left(\frac{1}{n}\right)$$

On a les résultats suivants :

- si $\alpha > 1$, alors $\sum u_n$ converge ;
- si $\alpha < 1$, alors $\sum u_n$ diverge ;
- lorsque $\alpha = 1$, on ne peut pas conclure. Les séries de Bertrand couvrent tous les cas possibles.

Cela se prouve en comparant à $v_n = \frac{1}{n^\beta}$ pour β entre 1 et α, en faisant le quotient de de deux termes consécutifs de (v_n) et avec la règle de d'Alembert.

Utilisation d'un développement asymptotique du terme général

Sommation par tranches

Transformation d'Abel

Utilisation d'une primitive

Technique de l'équation différentielle Si notre suite est définie par récurrence, on peut essayer de trouver une équation différentielle discrète vérifiée par la suite. On intègre ensuite cette équation différentielle pour trouver la une expression approchée de ce que devrait être notre suite. On trouve ensuite un équivalent de la série télescopique associée, avant de somme les relations de comparaison. Auparavant, on aura étudié la monotonie de la suite ou sa convergence pour justifier les DL effectués plus tard. **Ainsi, pour déterminer cette équation différentielle, on doit effectuer des DL**.

Application. Voici un exemple expliqué : on prend $u_0 > 0$ et $u_{n+1} = \ln(1+u_n)$. Cette suite est bien définie et par concavité de ln elle décroît. Elle est minorée par 0 donc converge d'après le théorème de la limite monotone. cette limite est nécessairement 0, c'est le seul point fixe de $x \mapsto x - \ln(1+x)$. Ainsi :

$$u_{n+1} \approx u_n - \frac{u_n^2}{2}$$

Ainsi, (u_n) vérifie une quasi équation différentielle de la forme :

$$u' = -\frac{u^2}{2}$$

En intégrant, on obtient qu'on devrait avoir

$$\frac{1}{u} = \frac{x}{2}$$

On étudie alors la suite télescopique de $v_n = \dfrac{1}{u_{n+1}} - \dfrac{1}{u_n}$ En effet, on a alors :

$$v_n = \frac{1}{u_n}\left(\frac{1}{1 - \frac{u_n}{2} + o(u_n)} - 1\right) = \frac{1}{u_n}\left(1 + \frac{u_n}{2} + o(u_n) - 1\right) \xrightarrow[n\to+\infty]{} \frac{1}{2}$$

En somme ensuite les relations de comparaison (ou on utilise le théorème de Cesaro) pour obtenir, après passage à l'inverse :

$$u_n \sim \frac{2}{n}$$

Application. Suite définies par $u_{n+1} = u_n + \dfrac{1}{u_n}$, $u_{n+1} = u_n + e^{-u_n}$, $u_{n+1} = u_n + \ln(u_n)$ (très difficile, pour l'équation différentielle, connaître l'équivalent du dilogarithme avec la fonction de répartition des nombres premiers et l'équivalent de cette fonction de répartition en $x/\ln(x)$).

12.3 Exercice classiques

Produit de Cauchy et Cesàro

Soit $(a_n)_{n\in\mathbb{N}}$ et $(b_n)_{n\in\mathbb{N}}$ deux suites complexes et soit (a,b) $\mathbb{C}^2$ tels que $a_n \underset{n\longrightarrow+\infty}{\longrightarrow} a$ et $b_n \underset{n\longrightarrow+\infty}{\longrightarrow} b$. On pose

$$\forall n\in\mathbb{N},\ u_n = \frac{1}{n+1}\sum_{k=0}^{n} a_k b_{n-k}$$

Montrer que $u_n \xrightarrow[n\to+\infty]{} ab$

Démonstration. Adapter la preuve de Cesàro vue en cours (oui, les ε sont de sortie...). Cette fois, il faut couper aux deux extrémités de la somme, on ne pourra contrôler que le milieu. □

Cesàro binomial

Soit $(a_n)_{n\in\mathbb{N}}$ une suite complexe convergente complexe de limite l. Montrer que

$$\frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}a_k \xrightarrow[n\to+\infty]{} l$$

On pourra commencer par le cas où $l=0$.

Démonstration. Adapter la preuve vue en classe de Cesàro vue en classe. Dans un premier temps, supposons que $l=0$. Soit $\varepsilon>0$. Par hypothèse, il existe un rang $n_1\in\mathbb{N}$ tel que

$$\forall n\in\mathbb{N},\ n\geqslant n_1 \Longrightarrow |a_n|\leqslant\frac{\varepsilon}{2}$$

Fixons un tel rang. Aussi, il existe un rang $n_2\in\mathbb{N}$ tel que

$$\forall n\in\mathbb{N},\ n\geqslant n_2 \Longrightarrow \Big|\frac{1}{2^n}\sum_{k=0}^{n_1}\binom{n}{k}a_k\Big|\leqslant\frac{\varepsilon}{2}$$

puisqu'on a une somme d'un nombre fini de termes qui sont tous dominés par n^{n_1}, donc ces termes sont tous négligeables devant 2^n. Fixons un tel rang. Ensuite, posons $n_0=\max(n_1,n_2)$. Soit $n\geqslant n_0$.

On a alors :

$$\begin{aligned}
\left|\frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}a_k\right| &\leqslant \left|\frac{1}{2^n}\sum_{k=0}^{n_1}\binom{n}{k}a_k\right| + \frac{1}{2^n}\sum_{k=n_1+1}^{n}\binom{n}{k}|a_k| \\
&\leqslant \frac{\varepsilon}{2} + \frac{1}{2^n}\sum_{k=n_1+1}^{n}\binom{n}{k}\frac{\varepsilon}{2} \\
&\leqslant \frac{\varepsilon}{2} + \frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k}\frac{\varepsilon}{2} \\
&\leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2}\frac{1}{2^n}\sum_{k=0}^{n}\binom{n}{k} \\
&\leqslant \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\
&\leqslant \varepsilon
\end{aligned}$$

On a bien le résultat souhaité.

Désormais, ne nous restreignons plus au cas $l = 0$. Il suffit alors d'appliquer le résultat qui précède à la suite $(a_n - l)_{n\in\mathbb{N}}$ qui tend bien vers 0. Une simple somme de limites permet alors de conclure. □

Lemme de Fekete

Soit $(u_n)_{n\in\mathbb{N}^*}$ sous-additive, *ie* telle que $\forall (p,q) \in \mathbb{N}^2,\ up+q \leqslant u_p + u_q$. Alors on a :

$$\frac{u_n}{n} \xrightarrow[n\to+\infty]{} l \quad \text{où} \quad l = \inf_{n\in\mathbb{N}^*}\frac{u_n}{n} \in \mathbb{R}\cup\{-\infty\}$$

Démonstration. On traite séparément plusieurs cas :

- si $l = 0$, on passe par les ε en prenant n_0 tel que u_{n_0}/n_0 soit ε proche de l. On effectue alors une division euclidienne de n par n_0 et on majore par sous-additivité et une inégalité de partie entière.
- si $l \in \mathbb{R}$, on se ramène au cas précédent en posant $v_n = u_n - ln$ qui est tout aussi sous-additive.
- si $l = -\infty$, on utilise la même idée que dans le premier cas, mais il faut faire un peu plus attention car l'inégalité de partie entière s'inverse puisque la suite est à valeurs négatives APCR.

□

Application. Sert pas mal dans des exercices assez complexes de probabilités où on demande une limite de $\mathbb{P}(X = n)^{1/n}$ par exemple : en effet, si on peut passer au ln, il y a des chances que la nouvelle suite soit sous-additive.

Suites réelles décroissantes sommables

Soit $(a_n)_{n\in\mathbb{N}}$ une suite réelle décroissante dont la série de terme général converge. Alors :

$$a_n = o\left(\frac{1}{n}\right)$$

Démonstration. En effet, on travaille sur une tranche de Cauchy de taille n et on utilise la décroissance de la suite. Cela donne le résultat pour $(2nu_{2n})$. On l'obtient alors facilement en majorant pour $((2n+1)u_{2n+1})$, et cela permet de conclure. □

Théorème de Riemann

Soit $\sum a_n$ une série réelle semi-convergente. Montrer que pour tout $x \in \mathbb{R}$, il existe σ une permutation de $\mathbb{N}$ telle que

$$\sum_{n=0}^{+\infty} a_{\sigma(n)} = x$$

Démonstration. Cet exercice est redoutable. Il me semble que l'idée est de prouver dans un premier temps qu'il y a nécessairement une infinité de termes strictement négatifs et une infinité de termes strictement positifs. Ensuite, pour $x \in \mathbb{R}$, on construit notre bijection de la façon suivante :

- tant que la somme partielle est inférieure à x, on pioche dans les termes strictement positifs et on prend ce terme comme étant le suivant pour notre bijection ;
- si la somme partielle dépasse strictement x, on pioche dans les termes strictement positifs.

Il faut alors prouver que la fonction obtenue est bien une bijection. L'injectivité est rapide, mais la surjectivité est plus embêtante (je crois qu'on peut raisonner par l'absurde). Enfin, il faut montrer que la série obtenue par réordonnement converge et est de somme x, ce qui se comprend bien, mais il me semble là encore qu'on peut le prouver en raisonnant par l'absurde. □

Chapitre 13

Intégrales généralisées

13.1 Points méthode

Utilisation d'une série

Pour $N \in \mathbb{N}$ et $a > 0$, on a d'après la relation de Chasles :

$$\sum_{n=1}^{N} \int_{na}^{(n+1)a} f = \int_{a}^{(N+1)a} f$$

Par conséquent, si l'intégrale $\displaystyle\int_a^{+\infty} f$ converge alors la série $\displaystyle\sum \int_{na}^{(n+1)a} f$ converge. Ainsi, on peut utilise la divergence d'une série pour prouver la divergence d'une intégrale. Attention, la réciproque est fausse.

Utilisation d'une primitive

Si F est une primitive de f, alors l'intégrale $\displaystyle\int_a^b f$ converge si, et seulement si, F admet des limites finies en a et en b, et l'on a alors :

$$\int_a^b f = \lim_b F - \lim_a F$$

quantité alors notée $[F(t)]_a^b$.

Utilisation d'une série pour une fonction positive

Soit $a > 0$ et $f \in \mathcal{CM}([a, +\infty[, \mathbb{R}_+)$. Puisqu'on a pour tout $N \in \mathbb{N}$:

$$\sum_{n=1}^{N} \int_{na}^{(n+1)a} f = \int_{a}^{(N+1)a} f$$

on obtient dans $\overline{\mathbb{R}_+}$, par passage à la limite et positivité :

$$\sum_{n=1}^{+\infty} \int_{na}^{(n+1)a} f = \int_{a}^{+\infty} f$$

En particulier, la série $\sum \int_{na}^{(n+1)a} f$ et l'intégrale l'intégrale $\int_{a}^{+\infty} f$ ont même nature.

Continue positive non nulle

Si f est une fonction continue positive et non nulle sur I, alors $\int_I f > 0$.

Comment étudier l'intégrabilité

Pour étudier l'intégrabilité d'une fonction continue par morceaux sur un intervalle I, on peut s'intéresser au comportement asymptotique de f au voisinage des "bornes ouvertes" de I, puis utiliser le théorème de comparaison. En particulier, si l'intervalle I est ouvert, on étudiera séparément les deux bornes.

Intervalles bornés

On a les différents résultats.

- Si une fonction f est bornée au voisinage d'un point $b \in \mathbb{R}$, alors on a $f \underset{b}{=} O(1)$. La fonction constante égale à 1 étant intégrable sur tout intervalle borné, on en déduit que f est intégrable en b.
- En particulier, si $f \in \mathcal{CM}([a, b[, \mathbb{K})$ admet une limite finie en $b \in \mathbb{R}$, alors f est intégrable.

Utilisation de l'intégration par parties et d'un passage à la limite

En pratique, on peut commencer par intégrer par parties sur les primitives, puis passer à la limite. Il y a deux buts possibles :

- justifier une convergence ;
- effectuer un calcul.

Intégration des relations de comparaison : comparaison des restes

On peut appliquer le théorème si la fonction à laquelle on compare est de signe constant et intégrable.

Intégration des relations de comparaison : comparaison des intégrales partielles

On peut appliquer le théorème si la fonction à laquelle on compare est de signe constant et non intégrable.

13.2 Astuces

Attention ! L'étude d'une intégrabilité commence par **CONTINUE PAR MORCEAUX SUR** . . . et ensuite, discussion aux bornes.

Étude d'une intégrale semi-convergente Pour des intégrales semi-convergentes, on effectue en général une intégration par parties pour transformer l'intégrale en faisant apparaître une intégrale absolument convergente. Sinon, on pourra effectuer un développement asymptotique de la fonction, le dernier terme écrit étant :

- ou bien une fonction intégrable ;
- ou bien de signe constant (dans le cas où la fonction est à valeurs réelles).

Intégration par parties itérée sur un segment Soit I un intervalle de $\mathbb{R}$, $n \in \mathbb{N}$ ainsi que f et g de fonctions de classe $\mathcal{C}^n$ de I dans $\mathbb{R}$. Alors, pour tout $(a,b) \in I^2$:

$$\int_a^b f^{(n)} g = \left[\sum_{i=0}^{n-1} (-1)^i f^{(n-1-i)}(t) g^{(i)}(t) \right]_a^b + (-1)^n \int_a^b f g^{(n)}$$

Cette formule n'est pas au programme, mais elle peut souvent s'avérer utile. Pour la démontrer, faire une récurrence et des IPP (évidemment...).

Application. Il est notamment pratique de connaître cette formule car dans des cas particuliers, on peut rapidement se perdre avec l'expression exacte des dérivées d'une fonction, alors que si on applique la formule directement, on peut ensuite remplacer par les dérivées que l'on connaît bien, notamment si g est la fonction exponentielle.

Application. Preuve de l'irrationalité de e : une grosse formule avec des IPP itérées traîne au milieu et on s'y perd vite...

Intégrations par parties Dans les intégrations par parties, il faut parfois accepter de jouer avec des constantes d'intégration pour faire converger le crochet ou l'annuler.

Application. Voici un exemple classique :

$$\int_0^{+\infty} \frac{\sin(x)}{x} dx = \left[\frac{1-\cos(x)}{x} \right]_0^{+\infty} + \int_0^{+\infty} \frac{1-\cos(x)}{x^2} dx$$

Changements de variable usuels On a les changements usuels suivants :

- $1+t^2$: on pose $t=\tan(u)$;
- $\sqrt{t^2-1}$: on pose $t=\cosh(u)$;
- $\sqrt{1+t^2}$: on pose $t=\sinh(u)$.

Changement de variable autosimilaire On pourra parfois utilise le changement de variable autosimilaire :

$$u=\frac{1-t}{1+t}$$

Il se comporte bien avec certaines fractions rationnelles.

Règles de Bioche On considère $\int r(\sin(\theta),\cos(\theta),\tan(\theta))\,d\theta$ et on pose $R(\theta)=r(\sin(\theta),\cos(\theta),\tan(\theta))\,d\theta$. Alors, si R est invariante par :

- $\theta\to-\theta$, on pose $u=\cos(\theta)$;
- $\theta\to\pi-\theta$, on pose $u=\sin(\theta)$;
- $\theta\to\pi+\theta$, on pose $u=\tan(\theta)$;
- deux des trois invariances précédentes, alors aussi par la troisième et on pose alors $u=\cos(2\theta)$;
- sinon, tant pis, on pose $u=\tan\left(\frac{\theta}{2}\right)$.

Le quatrième est le plus rapide de très loin, puis ce sont les 3 premiers, et enfin le dernier. Il existe un exemple pour lequel le quatrième changement de variable aboutit à un dénominateur de degré 2, de degré 4 pour les 3 premiers, et de degré 8 pour le dernier. On comprend la puissance de ces règles.

Application. Primitives de $1/\sin$, de $1/\cos$. Calculs d'intégrales dégueulasses de fractions rationnelles de sin, cos et tan en tout genre.

Application. Sert dans un exercice de séries entières où traîne une intégrale de

$$\frac{1}{1+a\cos(t)}$$

Intégrale dans une intégrale Quand on a une intégrale avec une autre intégrale dedans, du type

$$\int\ldots\left(\int_0^x\ldots du\right)dx$$

on fait une intégration par partie pour dériver $x\mapsto\int_0^x\ldots du$ et se débarrasser de cette intégrale.

Utilisation d'une équation différentielle Pour trouver une expression plus simple d'une fonction du type $x\mapsto\int_0^x\ldots dt$, on peut la dériver et chercher à montrer qu'elle est solution d'une équation différentielle que l'on résout ensuite.

13.3 Exercices classiques

Formule de la moyenne

Soit f et g deux applications continues de $[a, b]$ avec $a < b$. On suppose que $\forall t \in [a, b],\ g(t) \geqslant 0$. Alors :

$$\exists c \in [a, b], \int_a^b f(t)g(t)\ dt = f(c) \int_a^b g(t)\ dt$$

Démonstration. f est continue sur le compact $[a, b]$ donc d'après le théorème des bornes atteintes, il existe $(\alpha, \beta) \in [a, b]^2$ tel que :

$$\forall t \in [a, b],\ f(\alpha) \leqslant f(t) \leqslant f(\beta)$$

Par positivité de g, on a :

$$\forall t \in [a, b],\ f(\alpha)g(t) \leqslant f(t)g(t) \leqslant f(\beta)g(t)$$

Par croissance de l'intégrale et linéarité de l'intégrale, on en déduit que

$$f(\alpha) \int_a^b g(t)\ dt \leqslant \int_a^b f(t)g(t)\ dt \leqslant f(\beta) \int_a^b g(t)\ dt$$

Si $\displaystyle\int_a^b g(t)\ dt = 0$, alors il suffit de prendre $c = a$ car tous les termes de l'inégalité précédente sont nuls. Sinon, $\displaystyle\int_a^b g(t)\ dt > 0$, si bien que l'encadrement obtenu précédemment se réécrit :

$$f(\alpha) \leqslant \frac{\int_a^b f(t)g(t)\ dt}{\int_a^b g(t)\ dt} \leqslant f(\beta)$$

Le théorème des valeurs intermédiaires permet alors de conclure. □

Remarque. La preuve s'adapte dans le cas où g est négative.

Application. Permet de déduire l'égalité de Taylor-Lagrange de la formule de Taylor avec reste intégrale lorsque f est de classe $\mathcal{C}^{n+1}$.

Où sont les intégrales ?

Montrer que $2 < \pi < 4$.

Démonstration. On note $f : x \mapsto \frac{1}{1+x^2}$. On remarque que sur sur le segment $[0, 1]$, on a $\frac{1}{2} < f < 1$. Il suffit alors d'intégrer sur ce segment avec la stricte croissance de l'intégrale, puis de multiplier le tout par 4. On peut aussi raisonner avec un quart de cercle ou un demi-cercle dans la plan, mais c'est alors un peu plus embêtant de justifier les inégalités. □

Chapitre 14

Fonctions vectorielles

14.1 Points méthode

Utilisation des fonctions coordonnées

Une fois une base de E de dimension finie fixée, pour établir des propriétés de l'intégrale d'une fonction $f : [a,b] \to E$, on peut souvent se ramener aux fonctions coordonnées.

14.2 Astuces

Morphismes continus Un morphisme continu de $(\mathbb{R},+)$ dans $(\mathbb{C},\times)$ est de classe $\mathcal{C}^1$. Pour montrer cela, on intègre par rapport à une variable pour obtenir une expression en fonction d'une primitive. Attention, il faut sûrement distinguer le cas d'un morphisme constant. Cette méthode se généralise à d'autres morphismes

Théorème de Rolle généralisé On se donne $(a,b) \in \overline{\mathbb{R}}^2$ avec $a < b$ et on prend f dérivable sur $]a,b[$. On suppose que f admet des limites à droite en a et à gauche en b qui sont égales. Alors :

$$\exists c \in [a,b],\ f'(c) = 0$$

Démonstration. f ne peut pas être injective, sinon elle serait strictement monotone par continuité et on ne pourrait avoir l'égalité des limites. Par conséquent, on fixe $(a',b') \in]a,b[^2$ tel que $f(a') = f(b')$ et on applique le théorème de Rolle (cas fini) à la restriction de f à $]a',b'[$. $\square$

14.3 Exercices classiques

Théorème de Darboux

Théorème du relèvement

Chapitre 15

Suites et séries de fonctions

15.1 Points méthode

Rédaction d'une convergence uniforme

Pour montrer la convergence uniforme de (f_n) vers f :

$$\|f_n(x) - f(x)\| \leqslant \underbrace{\text{quelque chose de petit}}_{\text{indépendant de } x}$$

En particulier, le quelque chose de petit pourra être une suite qui tend vers 0.

Établissement d'une convergence uniforme

Pour établir la convergence uniforme de la suite (f_n), on peut :

- commencer par déterminer une fonction f vers laquelle (f_n) converge simplement ;
- chercher ensuite à établir une majoration $\|f_n(x) - f(x)\| \leqslant \alpha_n$, valable à partir d'un certain rang, où (α_n) est une suite tendant vers 0 ;
- à défaut, par retour à la définition, obtenir, pour tout $\varepsilon > 0$, à partir d'un certain rang, la majoration $\|f_n(x) - f(x)\| \leqslant \varepsilon$ pour tout x.

Autre façon de montrer une convergence uniforme

Lorsque A est un intervalle de $\mathbb{R}$ et $F = \mathbb{R}$, l'étude des variations de $f_n - f$ peut permettre de calculer $\alpha_n = \mathcal{N}_\infty(f_n - f)$. Suivant que (α_n) tend vers 0 ou non, on peut conclure quant à la convergence uniforme de (f_n) vers f.

Montrer une non convergence uniforme

Pour montrer que la suite (f_n) ne converge pas uniformément vers f, il suffit d'exhiber une suite $(x_n) \in A^{\mathbb{N}}$ telle que $(f_n(x_n) - f(x_n))$ ne tend pas vers 0.

Utilisation des formules de Taylor

Lorsqu'on a établi une limite simple à l'aide d'une formule de Taylor-Young (souvent via un équivalent), il est judicieux de montrer la convergence uniforme à l'aide de l'inégalité de Taylor-Lagrange correspondante.

Établir une convergence uniforme au voisinage de tout point

Pour établir la convergence uniforme de la suite (f_n) au voisinage de tout point d'un intervalle de $\mathbb{R}$, il suffit de montrer que la suite (f_n) converge uniformément sur tout segment de cet intervalle.

Établir une convergence normale

Pour montrer que $\sum u_n$ converge normalement, il suffit d'exhiber une série $\sum a_n$ convergente telle que $\forall n \in \mathbb{N},\ \forall x \in A,\ \|u_n(x)\| \leqslant a_n$. Au niveau de la rédaction, cela donne :

$$\|u_n(x)\| \leqslant \underbrace{a_n}_{\text{indépendant de } x} \quad \text{sommable}$$

Convergence uniforme d'une série via la convergence normale

Pour montrer la convergence uniforme d'une série (par exemple pour montrer que sa somme est continue), on regarde d'abord s'il n'y a pas convergence normale, ce qui est plus simple puisqu'il suffit de considérer son terme général.

Convergence uniforme d'une suite par une série

Pour montrer que la suite (f_n) converge uniformément sur A (et montrer ainsi, par exemple, qu'elle admet une limite continue), il est souvent pratique de montrer que la série $\sum(f_{n+1} - f_n)$ converge normalement sur A.

CVU et CVN : sur des parties fermées

Pour montrer des convergences uniformes et des convergences normales, sauf rares exceptions, on se place sur des parties fermées de l'ensemble de définition.

Classe $\mathcal{C}^\infty$

Pour montrer que la limite d'une suite de fonctions de classe $\mathcal{C}^\infty$ est de classe $\mathcal{C}^\infty$, il suffit de montrer la convergence uniforme sur tout segment de toutes les suites dérivées.

Détermination d'un équivalent par le théorème d'interversion de limites

Pour déterminer un équivalent de la somme d'une série en une borne de son intervalle de définition, on peut deviner l'équivalent puis le démontrer à l'aide du théorème d'interversion de limites.

Détermination d'un équivalent par comparaison série/intégrale

Pour déterminer un équivalent de la somme d'une série en une borne de son intervalle, on peut utiliser une comparaison série/intégrale.

15.2 Astuces

Usage des théorèmes d'approximation uniforme on commence par montrer la propriété souhaitée pour une fonction constante (puis on étend aux fonctions en escalier), ou bien pour les fonctions polynomiales (qui sont de classe $\mathcal{C}^1$, ce qui permet de faire des intégrations par partie dans les intégrales, par exemple...) puis on généralise le résultat à une fonction quelconque en l'approchant par une fonction "simple" (en escalier, polynomiale).

Application. Lemme de Riemann-Lebesgue version segment. La version générale s'en déduit par interversion de limites.

Théorème de la double limite Le théorème de la double limite est valable pour des fonctions $f : A \to E$ avec E un espace vectoriel normé de dimension finie et A une partie quelconque d'un espace vectoriel normée de dimension finie. En particulier, on peut prendre $A = \mathbb{N}$ ou $\mathbb{Z}$ et appliquer ce théorème à des suites !

15.3 Exercices classiques

Premier théorème de Dini

On considère une suite décroissante de fonctions (f_n) sur un compact K qui converge simplement vers 0. Alors la convergence est uniforme.

Démonstration. Déjà, remarquons que toutes les f_n sont par conséquent positives. Il est possible de démontrer le résultat à la main en prenant les *maxima* sur le segment, mais il y a plus élégant. Soit $\varepsilon > 0$. On considère

$$K_n := \{x \in K \ : \ f_n(x) \geqslant \varepsilon\}$$

puis on raisonne par l'absurde. On suppose que tous ces compacts (fermés dans un compact) sont non vides. Alors, puisque (K_n) forme une suite décroissante de compacts, d'après le théorème des compacts emboîtés, on peut prendre x dans l'intersection de tous ces compacts. Mais alors il ne peut y avoir convergence simple en x. Cela est absurde. Ainsi, il existe un K_{n_0} vide, et par décroissance, tous les suivants le sont. On a donc bien convergence uniforme. □

Deuxième théorème de Dini

On considère une suite de fonctions (f_n) définies sur $[a, b]$ à valeurs réelles qui sont toutes croissantes et qui converge simplement vers f. Alors la convergence est uniforme.

Démonstration. A COMPLETER □

Réciproque d'un résultat classique

Soit $D = \{d_n | n \in \mathbb{N}\}$ un ensemble au plus dénombrable. Alors il existe une fonction f croissante dont l'ensemble des points de discontinuité est exactement D.

Démonstration. Pour tout $n \in \mathbb{N}$, on pose

$$f_n : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} 1/2^n \text{ si } x \geqslant d_n \\ 0 \text{ si } x < d_n \end{cases} \end{array}$$

Alors $f = \sum f_n$ converge simplement. En effet, pour $x \in \mathbb{R}$, on pose

$$I_x = \{n \in \mathbb{N} \ : \ d_n \leqslant x\}$$

Alors $f(x) = \sum_{i \in I_x} 2^{-i}$ qui est bien finie comme sous-famille de la famille $(2^{-n})_{n \in \mathbb{N}}$ qui est sommable. De plus, f est croissante comme limite simple de fonctions croissantes. Par conséquent, elle admet des limites à gauche et à droite en tout point. Soit $n \in \mathbb{N}$ et notons l_n cette limite. Il est clair que la limite à droite de f en d_n est supérieure à $f(d_n)$ par croissance. Or, pour $x < d_n$:

$$f(x) = \sum_{i \in I_x} 2^{-i} \leqslant \sum_{d_i < d_n} 2^{-i} = f(d_n) - \frac{1}{2^n}$$

Donc $l_n < f(d_n)$ et d_n est un point de discontinuité de f. Et, si $x \notin D$, on peut distinguer les cas :

- si x n'est pas un point d'accumulation de D, alors on a convergence normale au voisinage de x donc continuité car les f_i sont continues au voisinage de x ;
- si x est un point d'accumulation de D : on revient à la définition en prenant ε, puis on s'approche suffisamment de x pour que la différence causée par une $\sum_{j \in J} 2^{-j}$ soit inférieure à ε (possible car la série converge).

□

Chapitre 16

Intégrales à paramètres

16.1 Points méthode

Intégrale dont la borne dépend d'un paramètre

Il faut bien noter, dans l'énoncé du théorème de convergence dominée, que l'intervalle d'intégration est fixe. Prolonger la fonction par la fonction nulle ou effecteur un changement de variable permet parfois de contourner cette difficulté lorsque l'intervalle d'intégration dépend de n.

Justification d'une interversion série/intégrale

Lorsque le théorème d'intégration terme à terme ne s'applique pas, pour justifier une interversion série/intégrale, on pourra parfois, en notant S_n et R_n la somme partielle et le reste d'ordre n de la série de fonctions $\sum u_n$ de somme S, vérifier que :

$$\int_I R_n \xrightarrow[n\to+\infty]{} 0 \text{ ou } \int_I S_n \xrightarrow[n\to+\infty]{} \int_I S$$

Pour établir de telles limites, on utilisera en général le théorème de convergence dominée.

Établissement de la domination sur A pour le théorème de continuité

Une domination sur tout l'ensemble est toujours suffisante, c'est pourquoi on commencera toujours, dans la pratique, par chercher à établir une telle domination. Lorsque A est un intervalle de $\mathbb{R}$, on pourra chercher une domination sur tout segment de A ou sur toute famille d'intervalles adaptée à la situation, c'est-à-dire permettant d'obtenir une domination sur tout segment de A.

Établissement de la domination sur J pour le théorème de dérivabilité

Bien entendu, une domination sur tout J est suffisante. Dans la pratique, on commencera par essayer d'établir une domination globale et, seulement si nécessaire, on se limitera aux segments de J, voire à une famille d'intervalles adaptée à la situation, c'est-à-dire permettant d'obtenir une domination sur tout segment de J.

Classe $\mathcal{C}^\infty$

Pour montrer que g est de classe $\mathcal{C}^\infty$, il suffit de vérifier que :

- pour tout $t \in I$, la fonction $x \mapsto f(x,t)$ est de classe $\mathcal{C}^\infty$;
- pour tout $k \in \mathbb{N}$, pour tout $x \in J$, la fonction $t \mapsto \dfrac{\partial^k f}{\partial x^k}(x,t)$ est continue par morceaux sur I ;
- chacune des dérivées partielles $\dfrac{\partial^k f}{\partial x^k}$ est dominée sur tout segment.

16.2 Astuces

Une "factorisation" utile Si f est dérivable, remarquer que la fonction :

$$F : \quad (u,v) \quad \longmapsto \quad \begin{cases} \dfrac{f(u)-f(v)}{u-v} \text{ si } u \neq v \\ f'(u) \text{ si } u = v \end{cases}$$

peut se réécrire sous la forme :

$$F(u,v) = \int_0^1 f'\big((1-t)u + tv\big)\ dt$$

Cela permet de ne plus avoir à séparer les deux cas et de par exemple appliquer les théorèmes de continuité ou de dérivation.

Application. Théorème de division.

16.3 Exercices classiques

Un exemple où le théorème de dérivation ne fonctionne pas

Montrer que

$$F : x \mapsto \int_0^{+\infty} \frac{\sin(xt)}{x(1+t^2)}\ dt$$

est de classe $\mathcal{C}^2$.

Démonstration. On commence par utiliser le théorème de dérivation pour montrer qu'elle est $\mathcal{C}^1$, mais on ne parvient pas avec ce même théorème à montrer qu'elle est $\mathcal{C}^2$. On effectue alors une intégration par parties dans l'expression de $F'(x)$ (ou un changement de variable) et on parvient ensuite à montrer que F' est $\mathcal{C}^1$, donc que F est $\mathcal{C}^2$. □

Méthode de Laplace

A COMPLETER

Fonction Gamma Γ

On définit la fonction Gamma par :

$$\Gamma(z) = \int_0^{+\infty} t^{z-1} e^{-t} \, dt$$

Elle vérifie :

- $\forall n \in \mathbb{N}, \ \Gamma(n+1) = n!$;
- Γ est log-convexe ;

Démonstration. Pour le premier point, effectuer des intégrations par parties successives. □

Chapitre 17

Séries entières

17.1 Points méthode

Utilisation de la sommation par paquets

On suppose que I est réunion disjointe de $(I_\lambda)_{\lambda\in\Lambda}$. Soit $(a_i)_{i\in I}$ une famille d'éléments de E, on a lorsque la famille est sommable ou à valeurs dans $\overline{\mathbb{R}_+}$:

$$\sum_{i\in I} a_i = \sum_{\lambda\in\Lambda}\left(\sum_{i\in I_\lambda} a_i\right)$$

Comment appliquer le théorème de sommation par paquets

Pour appliquer le théorème de sommation par paquets, on appliquera en général de le théorème de sommation par paquets (cas positif) pour montrer :

$$\sum_{\lambda\in\Lambda}\left(\sum_{i\in I_\lambda}\|a_i\|\right) < +\infty$$

puis on l'appliquera sans les normes avec le même recouvrement disjointe (I_λ).

Utilisation des sommes doubles

Si $(a_{p,q})_{(p,q)\in\mathbb{N}^2}$ est une famille à valeurs dans $\overline{\mathbb{R}_+}$ ou une famille sommable, on a :

$$\sum_{(p,q)\in\mathbb{N}^2} a_{p,q} = \sum_{p=0}^{+\infty}\left(\sum_{q=0}^{+\infty} a_{p,q}\right) = \sum_{q=0}^{+\infty}\left(\sum_{p=0}^{+\infty} a_{p,q}\right) = \sum_{n=0}^{+\infty}\left(\sum_{p+q=n} a_{p,q}\right)$$

Sommabilité d'une famille double

Pour montrer la sommabilité d'une famille double, on montrera en général l'un des résultats suivants :

$$\sum_{p=0}^{+\infty}\left(\sum_{q=0}^{+\infty}\|a_{p,q}\|\right) < +\infty \quad \text{ou} \quad \sum_{q=0}^{+\infty}\left(\sum_{p=0}^{+\infty}\|a_{p,q}\|\right) < +\infty \quad \text{ou} \quad \sum_{n=0}^{+\infty}\left(\sum_{p+q=n}\|a_{p,q}\|\right) < +\infty$$

Une méthode de détermination du rayon de convergence

Soit $\sum a_n z^n$ une série entière de rayon de convergence R et $z_0 \in \mathbb{C}$.

- Si $\sum a_n x_0^n$ est une série convergente, alors $R \geqslant |z_0|$.
- Si $\sum a_n z_0^n$ est une série divergente, alors $R \leqslant |z_0|$.

En particulier, la règle de d'Alembert pour les séries permet parfois de déterminer le rayon de convergence.

Dérivation sur l'intervalle ouvert de convergence

On peut dériver terme à terme la somme d'une série entière de la variable réelle sur son intervalle **ouvert** de convergence.

Primitivation et intégration terme à terme

On peut primitiver terme à terme la somme d'une série entière sur l'intervalle ouvert de convergence. On peut intégrer terme à termer la somme d'une série entière sur tout segment inclus dans l'intervalle ouvert de convergence.

Structure des fonctions développables en série entière

On a les résultats suivants.

- Si f et g sont des fonctions développables en série entière sur $D_O(0,r)$, alors $f+g$, λf et fg sont développables en série entière sur $D_O(0,r)$.
- Si f et g sont développables en série entière, alors $f+g$, λf et fg sont développables en série entière.
- Si f est développable en série entière sur $]-r,r[$, alors toutes les dérivées et les primitives de f sont développables en série entière sur $]-r,[$.

Méthode de l'équation différentielle

Voici comment utiliser une équation différentielle.

- Si on sait que f est développable en série entière, on cherche une relation de récurrence entre les coefficients de ce développement (par unicité du développement en série entière) pour déterminer ces derniers.
- Si on cherche à montrer que f est développable en série entière, on cherche une série entière de rayon de convergence strictement positif satisfaisant à la même équation différentielle et l'on utilise un résultat d'unicité des solutions d'une telle équation différentielle.

17.2 Astuces

Détermination d'un RCV Pour déterminer le rayon de convergence de $\sum a_z^n$, on peut encadrer (a_n) par deux suites plus simples dont les séries entières correspondantes ont des rayons plus faciles à déterminer. On en déduit un encadrement du rayon de convergence de $\sum a_n z^n$.

Utilisation de la dérivation et de l'intégration pour obtenir un DSE Pour trouver le DSE d'une fonction pénible, on dérive (on essaie de se ramener à quelque chose de facile à DSE, une fraction rationnelle par exemple) et on intègre ensuite le DSE pour obtenir celui de l'expression initiale.

Formule de Cauchy (HP) Si $f(z) = \sum_{n=0}^{+\infty}$ admet pour RCV $R > 0$, alors on a la formule de Cauchy :

$$\forall n \in \mathbb{N},\ \forall r \in [0, R[,\ a_n = \frac{1}{2\pi} \int_0^{2\pi} f(re^{i\theta}) e^{-in\theta}\, d\theta$$

Cette formule est particulièrement utile lorsqu'on s'intéresse à des problèmes à rayon constant.

Démonstration. Il suffit d'écrire $f(re^{i\theta})$, de multiplier par l'exponentielle complexe, d'intégrer et de justifier l'interversion série-intégrale. □

Application. Une fonction DSE bornée sur $\mathbb{C}$ est constante.

Application. Une fonction DSE sur un disque ouvert, continue sur le disque fermé et nulle sur le cercle est nulle partout. On utilise la formule et le théorème de continuité d'une intégrale à paramètre. Prolongement : une telle fonction uniquement nulle sur un arc de cercle de longueur non nulle est nulle partout. Pour cela, on remarque que l'anneau des fonctions DSE sur le disque ouvert et continues sur le disque fermé est intègre (prendre deux fonctions non nulles, les plus petits coefficients non nuls, et le coefficient du produit de Cauchy correspondant à la somme des indices), puis on crée une fonction à partir de composées de f par des rotations (en tournant d'assez pour que notre nouvelle fonction sur le cercle passe toujours par l'arc où f est nulle). Cette fonction est nulle par le premier cas, et par intégrité, une composée de f par une rotation est nulle, donc f est nulle.

Utilisation de l'unicité du DSE Pour extraire un terme particulier d'une somme infinie, penser à utiliser l'unicité des coefficients d'une série entière.

Utilisation avec les matrices Penser aux analogies avec les séries entières, même quand on travaille avec des matrices, mais il vaut alors mieux travailler avec des matrices nilpotentes de sorte que la série soit finie.

Application. Si N est nilpotente, on pose :

$$M = \sum_{n=1}^{+\infty} \frac{(-1)^{n-1}}{n} N^n$$

et on devrait tomber sur quelque chose du style $\exp(M) = I + N$ (A VERIFIER).

Utilisation d'une relation de récurrence linéaire Si $f(x) = \sum_{n=0}^{+\infty} a_n x^n$ où (a_n) vérifie la relation de récurrence linéaire :

$$a_n = \sum_{k=1}^{p} \lambda_k a_{p-k}$$

on peut alors écrire

$$f(x) = \sum_{k=1}^{p} \lambda_k x^k f(x) + \text{premiers termes}$$

Cela permet d'isoler f et de montrer que f est une fraction rationnelle.

Équivalent au bord de l'intervalle de convergence Pour (a_n) et (b_n) des suites de réels strictement positifs telles que $a_n \sim b_n$, alors si $\sum a_n z^n$ et $\sum b_n z^n$ sont de RCV égal à 1 et si $\sum a_n$ diverge, alors on a pour x réel :

$$\sum_{n=0}^{+\infty} a_n x^n \underset{x\to 1}{\sim} \sum_{n=0}^{+\infty} b_n x^n$$

Pour le démontrer, faire la différence entre les deux expressions et utiliser les ε.

Principe des zéros isolés Si f est la somme d'une série entière et $z_0 \in \mathbb{C}$ est dans le disque ouvert de convergence et vérifie $f(z_0) = 0$, alors :

$$\exists \delta > 0,\ \forall z \in D(z_0, \delta) \setminus \{z_0\},\ f(z) \neq 0$$

On commence par le prouver dans le cas où $z_0 = 0$. En notant n_0 le plus petit indice tel que a_n soit non nul, on a dans le disque ouvert de convergence :

$$f(z) = z^{n_0} \sum_{k=0}^{+\infty} a_{n_0+k} z^k$$

où le second facteur est une fonction continue (car DSE) qui tend vers a_{n_0} non nul en 0, donc ne s'annule pas dans un voisinage de 0. Ainsi, f est bien non nulle dans un voisinage épointé de 0.

Pour z_0 quelconque dans le disque ouvert de convergence, on utilise l'analycité de f, *ie* on étudie la fonction composée par une translation, $z \mapsto f(z - z_0)$ qui est aussi DSE et vérifie les hypothèses du cas précédent.

Application. Par contraposée, s'il existe une suite de complexes différents de z' et qui tend vers z_0 telle qu'on ait toujours $f(z_k) = 0$, alors si f est DSE, f est nulle. Prolongement : on peut étendre ce résultat si on travaille sur une partie connexe.

Limite au bord dans le cas des coefficients positifs Si (a_n) est une suite positive et $f(z) = \sum_{n=0}^{+\infty} a_n x^n$ est de RCV $R > 0$, alors on a :

$$f(x) \xrightarrow[x \to R]{} \sum_{n=0}^{+\infty} a_n R^n$$

En effet, si la série converge, c'est simplement le théorème d'Abel radial. Sinon, en repassant par les sommes partielles, on peut prouver que la série entière tend vers $+\infty$.

Calcul de sommes de séries Pour calculer des sommes de séries comme :

$$\sum_{n=1}^{+\infty} \frac{(-1)^n}{2n+1}$$

On interprète cette série comme une série entière au bord de son disque de convergence. On calcul la série entière associée par les théorèmes de cours et les méthodes habituelles sur les séries entières, et on conclut avec le théorème d'Abel radial.

Formules de coefficients binomiaux Voici une formule utile qui s'obtient en dérivant le DSE de $1/(1-x)$:

$$\forall x \in]-1, 1[, \ \sum_{n=0}^{+\infty} \binom{n+p}{p} x^n = \frac{1}{(1-x)^{p+1}}$$

En particulier, la formule pour $p = 2$ peut servir (le cas $p = 1$ est du cours) :

$$\sum_{n=0}^{+\infty} (n+1) x^n = \frac{1}{(1-x)^2}$$

Erreur classique Un fonction de classe $\mathcal{C}^\infty$ n'est pas nécessairement DSE. Exemple :

$$x \mapsto \begin{cases} e^{-1/x^2} \text{ si } x > 0 \\ 0 \text{ sinon} \end{cases}$$

En effet, cette fonction serait nulle si c'était le cas. En revanche, si une fonction est DSE, elle est de classe $\mathcal{C}^\infty$ sur son intervalle ouvert de converge, égale à sa série de Taylor.

Utilisation pour les intégrales Dans certains d'utilisation des séries entières, notamment le calcul d'intégrales, il faut parfois se ramener sur un intervalle où la fonction est DSE. Cela peut nécessiter l'usage de la relation de Chasles et des changements de variable.

Application. Étude de

$$\int_0^{+\infty} \frac{t^{x-1}}{1+t}\,dt$$

pour $0 < x < 1$. Couper en 1. A la fin, il faut repasser par les sommes partielles et utiliser le théorème de convergence dominée.

17.3 Exercices classiques

Théorème de Tauber

Si $\sum a_n z^n$ est une série de rayon entière de rayon de convergence 1, si sa somme S tend vers une limite finie l radialement en 1 et si $a_n = o\left(\frac{1}{n}\right)$, alors $\sum a_n$ converge et on a :

$$\sum_{n=0}^{+\infty} a_n = l$$

Démonstration. Montrer que

$$\sum_{k=1}^{n} a_n - S\left(1 - \frac{1}{n}\right)$$

tend vers 0. Pour cela, écrire :

$$\sum_{k=1}^{n} a_n - S\left(1 - \frac{1}{n}\right) = \sum_{k=1}^{n} a_k \left(1 - \left(1 - \frac{1}{n}\right)^k\right) + \sum_{k=n=1}^{+\infty} a_k \left(1 - \frac{1}{n}\right)^k$$

On montre que les deux termes tendent vers 0. Pour le premier, utiliser le fait que

$$1 - \left(1 - \frac{1}{n}\right)^k \leqslant \frac{n}{k}$$

(le démontrer avec une factorisation de Bernoulli) puis utiliser le théorème de Cesaro avec (na_n) qui tend vers 0 par hypothèse. Pour le second terme, écrire artificiellement

$$a_k = a_k \frac{k}{k}$$

Majorer tous les $1/k$ par $1/(n+1)$ puis majorer en module tous $a_k k$ par la borne supérieure de ces éléments pour $k \geqslant n+1$, borne supérieure qui tend vers 0 par hypothèse. Enfin, pour le reste, majorer brutalement par la série géométrique totale pour avoir une expression simple, et majorer $1 - 1/n$ par 1. $\square$

Théorème d'Abel non tangentiel

Si on a la convergence de la série au bord du disque de convergence, on a non seulement la continuité radiale, mais aussi la continuité dans tout secteur angulaire non tangentiel.

Démonstration. Effectuer une transformation d'Abel. Je n'ai ensuite pas trouvé mieux que de repasser par les ε. Couper en deux la série et utiliser pour le terme "reste" une majoration brutale par une suite géométrique totale. On devra utiliser la majoration :

$$\frac{1}{1-|z|} \leqslant \frac{2}{1-|z|^2}$$

(vraie car $(|z|-1)^2 \geqslant 0$) □

Théorème de Bernstein

Soit $a > 0$ et $f \in \mathcal{C}^\infty(]-a,a[,\mathbb{R})$ telle que $\forall n \in \mathbb{N},\ \forall x \in]-a,a[,\ f^{(n)}(x) \geqslant 0$. Alors, f est développable en série entière sur $[0,a[$ et sur $]-a,a[$.

Démonstration. Pour cela, montrer que la fonction $x \mapsto R_n(x)/x^{n+1}$ est une fonction croissante de x en utilisant la formule de Taylor avec reste intégral sous sa deuxième forme. On majore ensuite $R_n(x)$ par $R_n(y)x^{n+1}/y^{n+1}$ avec $x < y < a$. Or, $R_n(y)$ est bornée en écrivant la formule de Taylor, donc $R_n(x)$ tend vers 0 quand n tend vers $+\infty$ et f est DSE sur $[0,a[$. Pour symétriser le résultat :

$$|R_n(-x)| \leqslant \frac{|x|^{n+1} f^{n+1}(0)}{(n+1)!} \xrightarrow[n\to+\infty]{} 0$$

car c'est le terme général d'une série convergente par ce qui précède. On a donc le résultat sur $]-a,a[$. □

Application. En fait, il suffit qu'on suppose la positivité sur $[0,a[$ pour avoir le résultat. Cela permet de montrer que tan est DSE.

Fonctions analytiques

En utilisant une série double, on montre que si f est DSE sur $I =]-R,R[$, alors pour tout $x_0 \in I$, la fonction $t \mapsto f(x_0+t)$ est DSE sur $]-\alpha,\alpha[$ avec $\alpha = R - |x_0|$. On dit que f est analytique sur I.

Chapitre 18

Équations différentielles

18.1 Points méthode

Détermination d'une solution particulière pour une EDL d'ordre 1

Pour déterminer une solution particulière de l'équation avec second membre :

- on commence par chercher une solution particulière "évidente" (éventuellement en se guidant sur le problème, physique, géométrique ou autre, d'où est issu cette équation différentielle) ;
- si l'on n'en trouve pas, on peut utiliser la méthode de variation de la constante car une solution non nulle de l'équation homogène associée ne s'annule pas.

Résolution d'une EDL d'ordre 1

Résolution d'une équation différentielle de la forme $a(t)y' + b(t)y = c(t)$ sur un intervalle sur lequel a ne s'annule :

- On commence par résoudre l'équation sur tout intervalle sur lequel a ne s'annule pas (on sait que l'ensemble des solutions est une droite affine).
- On procède ensuite par analyse/synthèse puisque l'on n'a aucune théorème ni d'existence ni d'unicité.

Structure des solutions

Pour résoudre une équation différentielle linéaire, on ajoute une solution particulière à la solution générale de l'équation homogène associée.

Base des solutions de l'équation homogène

Si l'on dispose de n fonctions $\varphi_1, \dots, \varphi_n$ de I dans E de dimension n, alors, pour prouver que la famille $(\varphi_1, \dots, \varphi_n)$ est une base de $\mathcal{S}_0$, il suffit de démontrer au choix :

- que $\varphi_1, \dots, \varphi_n$ appartiennent à $\mathcal{S}_0$ et forment une famille libre ;
- que $\mathcal{S}_0 \subset \mathrm{Vect}(\varphi_1, \dots, \varphi_n)$. On a alors $\mathcal{S}_0 = \mathrm{Vect}(\varphi_1, \dots, \varphi_n)$ pour des raisons de dimension, et la famille $(\varphi_1, \dots, \varphi_n)$ est génératrice, donc une base de $\mathcal{S}_0$. Il n'est pas nécessaire de démontrer préalablement que les fonctions φ_k appartiennent à $\mathcal{S}_0$.

Cas où A est diagonalisable

Si la matrice A est diagonalisable, alors en notant $(V_1, \dots, V_n)$ une base de vecteurs propres et $(\lambda_1, \dots, \lambda_n)$ la liste des valeurs propres associées, on obtient une base $(\varphi_1, \dots, \varphi_n)$ de l'espace $\mathcal{S}_0$ des solutions de (E_0) en prenant, pour tout $k \in [\![1, n]\!]$:

$$\varphi_k : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{K} \\ t & \longmapsto & e^{\lambda_k t} V_k \end{array}$$

Cas où A est diagonalisable uniquement sur $\mathbb{C}$

Si $A \in \mathcal{M}_n(\mathbb{R})$ est diagonalisable dans $\mathbb{C}$ mais pas dans $\mathbb{R}$, on peut déterminer l'ensemble $\mathcal{S}_\mathbb{R}$ des solutions de (E_0) à partir de la diagonalisation de A :

1. On forme une base de vecteurs propres complexes de A telle que :
   - les vecteurs propres associées à des valeurs propres réelles appartiennent à $\mathbb{R}^n$;
   - vis-à-vis des des valeurs propres non réelles, on forme des couples de vecteurs propres conjugués (*ie* de la forme $(V, \overline{V})$).
2. Dans la base $(\varphi_1, \dots, \varphi_n)$ de $\mathcal{S}_\mathbb{C}$ évoquée dans le point méthode qui précède, on voit alors apparaître :
   - pour les valeurs propres réelles, des applications de la forme $t \mapsto e^{\lambda t} V$, qui sont à valeurs dans $\mathbb{R}^n$;
   - pour les valeurs propres non réelles, des couples de la forme $(t \mapsto e^{\lambda t} V,\ t \mapsto e^{\overline{\lambda} t} \overline{V})$, c'est-à-dire des couples de la forme $(\varphi, \overline{\varphi})$.
3. On change les couples de la forme $(\varphi, \overline{\varphi})$ en $(\mathrm{Re}(\varphi), \mathrm{Im}(\varphi))$, qui est encore une base de $\mathcal{S}_\mathbb{C}$. Or, cette base n'est formée que d'applications à valeurs dans $\mathbb{R}^n$, donc c'est une base de $\mathcal{S}_\mathbb{R}$.

Cas où A est non diagonalisable sur $\mathbb{C}$

Si A est non diagonalisable sur $\mathbb{C}$:

1. On trigonalise, c'est-à-dire qu'on écrit $A = PTP^{-1}$ avec T triangulaire supérieure.
2. En posant $Y = P^{-1}X$ et en traduisant sur Y le système différentiel, $X' = AX$, on obtient le système différentiel $Y' = TY$: ce système différentiel est triangulaire et on peut donc le résoudre ligne par ligne, du bas vers le haut.
3. On trouve les solutions recherchées à l'aide de la relation $X = PY$.

Remarquer qu'il n'est donc pas nécessaire de calculer P^{-1}. Et lorsqu'on trigonalise A, on cherchera à obtenir la matrice triangulaire la plus simple possible afin d'obtenir le système différentiel le plus simple possible.

Remarque (Utilisation calculatoire de la décomposition de Dunford). Si jamais on dispose facilement de la décomposition de Dunford de la matrice, on pourra l'utiliser pour calculer directement $\exp(tA)$ et s'éviter des tonnes de calcul. En particulier, cela peut énormément servir si la matrice n'est pas diagonalisable et ne possède qu'une seule valeur propre : en effet, la matrice diagonalisable dans la décomposition de Dunford n'est alors autre qu'une matrice scalaire associée à l'unique valeur propre, et la matrice nilpotente s'en déduit en soustrayant cette matrice scalaire à la matrice de départ.

Recherche d'une solution particulière

Pour trouver une solution particulière de $y' = a(t) \cdot t + b(t)$:

- on commencera par chercher une solution évidente ;
- dans le cas où il n'y en a pas d'évidente, on pourra utiliser la méthode de variation de la constante en cherchant y sous la forme $t \mapsto \exp(ta) \cdot \Lambda(t)$, avec $\Lambda : I \mapsto E$ dérivable ;
- pour une équation différentielle $Y' = AY + B(t)$ avec $A \in \mathcal{M}_n(\mathbb{K})$ et $B \in \mathcal{C}^1(I, \mathbb{K}^n)$, si l'on réduit A sous la forme $A = PDP^{-1}$ avec D diagonale ou triangulaire, en posant $Z = P^{-1}Y$, on est ramené à résoudre $Z' = DZ + P^{-1}B(t)$, et on récupère ensuite $Y = PZ$

Méthode de variations des constantes à l'ordre 2

Si on connaît une base (φ_1, φ_2) de l'espace des solutions de (E_0), alors on peut chercher une solution particulière de $(E) : x'' + a_1(t)x' + a_0(t)x = b(t)$ sous la forme :

$$\varphi = \lambda_1\varphi_1 + \lambda_2\varphi_2 \quad \text{avec} \quad \lambda_1 \quad \text{et} \quad \lambda_2 \quad \text{dérivables sur} \quad I$$

Une telle fonction φ est solution de (E) si :

$$\begin{cases} \lambda_1'\varphi_1 + \lambda_2\varphi_2 = 0 \\ \lambda_1'\varphi_1' + \lambda_2'\varphi_2' = b \end{cases}$$

On peut alors déterminer λ_1' et λ_2', puis λ_1 et λ_2 par calcul de primitives.

Étude d'une équation non normalisée

Pour résoudre une équation différentielle linéaire de la forme

$$a_n(t)x^{(n)} + \ldots + a_0(t)x = b(t)$$

lorsque la fonction a_n possède des points d'annulation :

- on commence par résoudre l'équation sur tout intervalle sur lequel a_n ne s'annule pas ;
- on cherche ensuite, par analyse/synthèse, les solutions sur l'intervalle entier en exploitant les conditions de dérivabilité et de continuité pour obtenir les constantes.

18.2 Astuces

Annulation du wronskien Pour une équation différentielle de degré 2 à coefficients constants, si le Wronskien est nul en un point, il est nul partout, puisqu'il est solution d'une équation

$$y' = ay$$

Le théorème de Cauchy linéaire permet de conclure.

Existence d'autres solutions Si on étudie des solutions particulières d'équations différentielles linéaires, bien penser qu'il existe probablement plein d'autres solutions (le théorème de Cauchy linéaire peut en assurer l'existence).

Utilisation pour le calcul d'intégrales à paramètres Si F est une intégrale à paramètre qu'on cherche à exprimer autrement, on peut avoir envie de trouver une équation différentielle vérifiée par F. Pour cela, on fait parfois une intégration par parties sur l'intégrale après l'avoir dérivée.

Equations d'Euler Pour les équations d'Euler :

$$x^2y''(x) + axy'(x) + by(x) = 0$$

avec $(a, b) \in \mathbb{C}^2$, le changement de variables $x = e^t$ fonctionne sur $\mathbb{R}_+^*$, et sur $\mathbb{R}_-^*$, on utilise $x = -e^t$. En d'autres termes, cela revient à chercher des solutions en $x \mapsto x^r$.

Fausses équations différentielles faisant intervenir $f(1/t)$ Si on a affaire à des équations faisant intervenir $f(1/t)$ pour $t \in \mathbb{R}_+^*$, on peut faire un changement de variable $t = e^u$, ce qui va permettre de se ramener à des équations différentielles usuelles (à mettre en regard de la méthode pour les équations d'Euler).

Application. Trouver les f dérivables sur $\mathbb{R}_+^*$ telles que

$$\forall t > 0,\ f'(t) = f\left(\frac{1}{t}\right)$$

Utilisation d'une autre équation différentielle et lemme de Gronwall Pour étudier une solution f d'une équation différentielle :

$$y''(x) + y'(x) + q(x)y(x) = 0$$

(ou quelque chose qui y ressemble), connaissant des hypothèses sur f ou q, on peut essayer de résoudre l'équation $z'' + z = g$ avec $g(x) = -q(x)f(x)$. Cela donne une nouvelle expression de f avec laquelle on peut parfois utiliser le lemme de Gronwall. Cette méthode qui consiste à obtenir une nouvelle expression d'une fonction en résolvant une autre équation différentielle est intéressante.

Principe des zéros isolés Si f est solution non nulle de l'équation homogène du second ordre

$$y''(t) + a(t)y'(t) + b(t)y(t) = 0$$

avec a et b continues, alors tout zéro de f est isolé (*ie* f est non nulle dans un voisinage épointé de x_0). En effet, soit x_0 tel que $f(x_0) = 0$. Alors $f'(x_0) \neq 0$ car sinon elle serait solution d'un problème de Cauchy dont la fonction nulle est solution, et serait alors nulle. Comme

$$\frac{f(x)}{x - x_0} \xrightarrow[x \to x_0]{} f'(x_0) \neq 0$$

f est non nulle dans un voisinage de x_0.

18.3 Exercices classiques

Méthode de Sturm-Liouville (HP)

Soit p_1 et p_2 des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$ telles que $p_1 \leqslant p_2$. On considère les équations différentielles :

$$\begin{cases} y'' + p_1 y = 0 & (E_1) \\ y'' + p_2 y = 0 & (E_2) \end{cases}$$

Soit y_1 une solution réelle non nulle de (E_1) et y_2 une solution de (E_2). Si t_1 et t_2 sont deux zéros distincts de y_1, alors il existe $t \in [t_1, t_2]$ tel que $y_2(t) = 0$.

Démonstration. Considérer $W = y_1 y_2' - y_1' y_2 = y_1 y_2 (p_1 - p_2)$. Les zéros de y_1 sont isolés, donc on peut prendre SPG t_1 et t_2 deux zéros consécutifs de y_1. SPG, on peut supposer que y_1 est strictement positive entre t_1 et t_2 : on a alors $y_1'(t_1) > 0$ et $y_2'(t_2) < 0$ en effectuant un DL. On raisonne alors par l'absurde en supposant que y_2 ne s'annule pas sur $[t_1, t_2]$. Le Wronskien est alors monotone, mais s'il est croissant par exemple, alors il est positif en t_1 et négatif en t_2. Mais par conséquent, $y_1'(t_1) = 0$. Donc y_1 est nulle car c'est une solution au problème de Cauchy :

$$\begin{cases} y'' + p_1 y = 0 \\ y(t_1) = 0 \\ y_1'(t_1) = 0 \end{cases}$$

C'est absurde, donc y_2 s'annule sur $[t_1, t_2]$. En examinant la preuve ci-dessus, on peut même montrer en réalité que y_2 s'annule dans $[t_1, t_2[$ et dans $]t_1, t_2]$. $\square$

Application. Application à l'étude des zéros d'une solution non nulle sur $\mathbb{R}_+$ de $y'' + e^t y = 0$. Montrer que ces zéros forment une suite strictement croissante, dont on déterminera un équivalent à l'infini.

Application. Permet de montrer qu'une solution de $y'' + qy = 0$ avec $q > 0$ et $q' > 0$ au voisinage de l'infini admet une infinité de zéros.

Une application de la méthode de Sturm-Liouville

Montrer que les zéros d'une solution y sur $\mathbb{R}_+$ non nulle de $y'' + e^t y = 0$ forment une suite strictement croissante (t_n). Déterminer un équivalent de la suite (t_n).

Démonstration. Pour le fait qu'il y en a une infinité, utiliser la méthode de Sturm-Liouville avec $t \mapsto \sin(t)$ solution de $y''+y = 0$ car $\forall t \in \mathbb{R}_+,\ e^t \geqslant 1$. Ensuite, pour les ordonner, on peut remarquer qu'il ne peut y avoir une infinité de zéros sur le compact $[0, A]$ grâce au principe des zéros isolés. On peut alors les ordonner. Pour l'équivalent, on utilise le fait que

$$\forall t \in [t_n, t_{n+1}],\ e^{t_n} \leqslant e^t \leqslant e^{t_{n+1}}$$

On applique la méthode de Sturm-Liouville à $t \mapsto \sin(e^{t_n/2}(t - t_n))$, y et $t \mapsto \sin(e^{t_{n+1}/2}(t - t_n))$ pour obtenir l'encadrement :

$$\frac{\pi}{e^{t_{n+1/2}}} \leqslant t_{n+1} - t_n \leqslant \frac{\pi}{e^{t_n/2}}$$

Or, $t_n \to +\infty$ puisque par construction on a des zéros aussi grand que l'on veut (ou alors, par l'absurde, t_n convergerait vers un zéro de y par continuité, mais cela est impossible par stricte croissance de (t_n)). Par conséquent, $t_{n+1} - t_n \to 0$. On en déduit que

$$t_{n+1} - t_n \sim \frac{\pi}{e^{t_n/2}}$$

car les exponentielles sont équivalentes car la différence des arguments tend vers 0. On étudie ensuite la suite annexe $e^{t_n/2}$. En faisant la différence de deux termes, on trouve une limite non nulle avec les résultats précédents $(\pi/2)$ donc on peut sommer les relations de comparaison. On en déduit que

$$e^{t_n} \sim \frac{n^2\pi^2}{4}$$

et comme tout tend vers $+\infty$, on sait qu'on peut prouver rapidement qu'on peut passer les équivalents au ln, ce que l'on fait et qui fournit finalement :

$$t_n \sim 2\ln(n)$$

□

Lemme de Gronwall (HP)

Soit I un intervalle de $\mathbb{R}$, $t_0 \in I$, ainsi que que $a : I \to \mathbb{R}_+$ et $b : I \to \mathbb{R}_+$ deux fonctions continues. On note A la primitive de a s'annulant en t_0. Si y de classe $\mathcal{C}^1$ vérifie :

$$\forall t \geqslant t_0,\ \|y'(t)\| \leqslant b(t) + a(t)\|y(t)\|$$

alors y vérifie :

$$\forall t \geqslant t_0,\ \|y(t)\| \leqslant \|y(t_0)\|e^{A(t)} + e^{A(t)} \int_{t_0}^{t} b(s)e^{-A(s)}\ ds$$

Le résultat est facile à retrouver : on majore $\|y\|$ par la solution du problème de Cauchy :

$$\begin{cases} z' = b(t) + a(t)z \\ z(t_0) = \|y(t_0)\| \end{cases}$$

Démonstration. La concept est simple : on fait des choses sans comprendre pourquoi, mais ça marche et tout va se simplifier par miracle. □

Application. Étude du comportement asymptotique des solutions de l'équation :

$$y'' + \frac{1}{x^2}y' + y = 0$$

$f' + f$ de limite nulle

Soif $f \in \mathcal{C}^1(\mathbb{R}_+, \mathbb{R})$ telle que $f' + f \xrightarrow[+\infty]{} 0$. Alors :

$$\begin{cases} f \xrightarrow[+\infty]{} 0 \\ f' \xrightarrow[+\infty]{} 0 \end{cases}$$

Démonstration. En effet, on pose $g = f' + f$ et on résout $y' + y = g$. Les fonctions y solutions sont celles telles qu'il existe $C \in \mathbb{R}$ tel que

$$\forall x \in \mathbb{R}_+,\ y(x) = e^{-x}\left(\int_0^x e^t g(t)\ dt + C\right)$$

Or, f vérifie cette équation différentielle, donc il existe une telle constante C. De plus, puisque $e^t g(t) = o(e^t)$, on a par intégration des relations de comparaion :

$$\int_0^x e^t g(t)\ dt = o(e^x)$$

On en déduit que $f(x) = o(1)$, c'est-à-dire que

$$f \xrightarrow[+\infty]{} 0$$

Par différence avec $f' + f$, on obtient le résultat sur f'. □

Application. Si f est de classe $\mathcal{C}^2$ et vérifie $f'' + 3f' + 2f \xrightarrow[+\infty]{} 0$, alors f, f' et f'' tendent vers 0 quand x tend vers $+\infty$. Il suffit d'appliquer deux fois ce qui précède à $g = f' + 2f$. Cela se généralise sans peine.

Équation différentielle vérifiée par le wronskien

On considère n solutions de $y' = ay$ avec $a \in \mathcal{C}(I, \mathcal{L}(F))$ où F est dimension finie, dont on prend $\mathcal{B}$ une base. On considère $y_1, \ldots, y_n$ des solutions de cette équation et w leur wronskien. Soit $t_0 \in I$. Alors :

$$\forall t \in I,\ w(t) = w(t_0) \exp\left(\int_{t_0}^{t} \mathrm{Tr}(a(u))\ du\right)$$

Démonstration. En effet, d'après un exercice classique de formes n-linéaires alternées, on a pour tout u et pour tout t :

$$\mathrm{Tr}(a(u)) \det_{\mathcal{B}}(y_1(t), \ldots, y_n(t)) = \sum_{j=1}^{n} \det_{\mathcal{B}}(y_1(t), \ldots, a(u)(y_j(t)), \ldots, y_n(t))$$

Soit, puisqu'on a des solutions de l'équation, $a(u)(y_j(t)) = y_j'(t)$. On en déduit que

$$\mathrm{Tr}(a(u)) w(t) = \sum_{j=1}^{n} \det_{\mathcal{B}}(y_1(t), \ldots, y_j'(t), \ldots, y_n(t)) = w'(t)$$

On en déduit la formule annoncée en résolvant l'équation différentielle. □

Équation $y'' + q(x)y$ avec q positive croissante asymptotiquement

On considère $q \in \mathcal{C}^1(\mathbb{R}_+, \mathbb{R})$ et l'équation $y'' + q(x)y = 0$. Alors :

- toute solution admet une infinité de zéros ;
- toute solution est bornée

Démonstration. Pour le premier point, appliquer la méthode de Sturm-Liouville sur un voisinage de $+\infty$ car on a alors $q(x) \geqslant k > 0$ par croissance et positivité asymptotiques de q. On se ramène alors aux zéros de sin (à peu de choses près) que l'on contrôle bien, et la méthode de Sturm-Liouville prouver que toute solution de la première équation admet un zéro entre deux zéros de ce sin.

Pour le deuxième point, considérer $z(x) = (y(x))^2 + \dfrac{(y'(x))^2}{q(x)}$. Cette fonction est dérivable au voisinage de $+\infty$, et sa dérivée est négative (on a une simplification car y est solution). Ainsi, z est décroissante à partir d'un certain seuil, puis par positivité, y^2 est bornée dans ce voisinage de $+\infty$, donc y y est bornée. Par continuité, y est donc bornée sur $\mathbb{R}_+$ tout entier. □

Existence de solutions non bornées

Considérons l'équation différentielle $y'' + q(x)y = 0$ avec q continue et intégrable. Alors :

- La dérivée de toute solution bornée de cette équation tend vers 0 en $+\infty$;
- En déduire qu'il existe des solutions à cette équation non bornées.

Démonstration. Soit y une solution de cette équation. Prouvons les deux points dans l'ordre.

- En intégrant y'' entre 0 et t et en remarquant que qy est intégrable car c'est un $O(q)$, on trouve que y' admet une limite finie en $+\infty$. Cette limite ne peut être non nulle, car en intégrant y' au voisinage de $+\infty$ là où y' serait de signe constant est de module minorée par un réel strictement positif, on trouverait que y est non bornée.
- S'il existe une solution non nulle bornée y_1, on considère une deuxième solution y_2 telle que (y_1, y_2) soit un système fondamental. Alors, le wronskien de y_1 et y_2 est constant car l'équation différentielle ne possède pas de terme en y', et il est donc égal à une constante non nulle car (y_1, y_2) est un système fondamental. De plus, si y_2 est bornée, alors d'après le premier point, le wronskien doit tendre vers 0 en l'infini, donc être nul. Or, il est non nul, donc y_2 et non bornée. Dans tous les cas, il existe une solution non bornée.

□

Pas trop d'annulations dans un voisinage d'un point

On se donne une EDL d'ordre n :

$$x^{(n)} + \sum_{k=0}^{n-1} a_k(t)x^{(k)} = 0$$

où les a_k sont continues sur un intervalle I d'intérieur non vide (sinon le résultat n'a pas d'intérêt), ainsi que $t_0 \in I$. Alors, il existe un voisinage J de t_0 dans I tel que toute solution non nulle de l'équation s'annule au plus $n-1$ fois sur J.

Démonstration. On raisonne par l'absurde, et on prend, pour tout $p \in \mathbb{N}$, une fonction φ_p solution non nulle qui s'annule au moins n fois sur

$$J_p = \left[t_0 - \frac{1}{2^p}, t_0 + \frac{1}{2^p}\right]$$

Quitte à renormaliser φ_p, on peut la supposer de norme 1 (nous verrons pour quelle norle apèrs). En effet, cet intervalle est un voisinage de t_0 APCR. Alors, avec le théorème de Rolle, pour tout $k \in [\![0, n-1]\!]$, $\varphi_p^{(k)}$ s'annule en $x_p^{(k)}$. On extrait de (φ_p) une sous-suite qui converge vers φ par compacité de la sphère unité en dimension finie. Alors, on choisit maintenant d'avoir travaillé avec la norme

$$N(f) = \|f\|_\infty + \ldots + \|f^{(n-1)}\|_\infty$$

On a alors :

$$|\underbrace{\varphi_p^{(k)}(t_0)}_{=0} - \varphi^{(k)}(t_0)| \leqslant \|\varphi_p^{(k)} - \varphi^{(k)}\|_\infty \leqslant N(\varphi_p - \varphi) \xrightarrow[p\to+\infty]{} 0$$

donc, par continuité et unicité de la limite $\varphi^{(k)}(t_0) = 0$. Par unicité de la solution au problème de Cauchy avec de telles conditions initiales, $\varphi = 0$, ce qui est absurde car elle est de norme 1 donc non nulle. □

Solutions stables par dérivation $\implies$ coefficients constants

Soient $a_0, \ldots, a_{n-1}$ continue. On suppose que l'ensemble E_0 des solutions de

$$x^{(n)} + \sum_{k=0}^{n-1} a_k(t) x^{(k)} = 0$$

est stable par dérivation. Alors les a_k sont constantes.

Démonstration. On note D l'endomorphisme induit par la dérivation sur E_0. E_0 est de dimension n, on note

$$\chi_D = X^n + \sum_{k=0}^{n-1} b_k X^k$$

le polynôme caractéristique de D. D'après le théorème de Cayley-Hamilton, tout élément de E_0 vérifie donc aussi l'équation différentielle :

$$x^{(n)} + \sum_{k=0}^{n-1} b_k x^{(k)} = 0$$

En considérant les solutions dont les conditions initiales sont

$$\forall k \in [\![0, n-1]\!],\ x^{(k)}(t_0) = \delta_{k,l}$$

on on obtient que

$$\forall k \in [\![0, n-1]\!],\ \forall t \in \mathbb{R},\ a_k(t) = b_k$$

□

Remarque. Réciproquement, avec la même méthode, tout sous-espace vectoriel de dimension finie n de $\mathcal{C}^\infty(I, \mathbb{K})$ stable par dérivation est l'ensemble des solutions d'une équation différentielle linéaire d'ordre n à coefficients constants.

Paramètre à valeurs antisymétriques

On considère l'équation $X' = A(t)X$ d'inconnue matricielle avec $\forall t \in \mathbb{R},\ A(t) \in \mathcal{A}_n(\mathbb{R})$. Soit X une solution de cette équation différentielle. Montrer que si $X(0) \in \mathcal{O}_n(\mathbb{R})$, alors

$$\forall t \in \mathbb{R},\ X(t) \in \mathcal{O}_n(\mathbb{R})$$

Démonstration. Supposons $X(0) \in \mathcal{O}_n(\mathbb{R})$ et considérons $f : t \mapsto X(t)^T X(t)$. Il est clair que f est dérivable et :

$$\forall t \in \mathbb{R}, f'(t) = X(t)^T A(t) X(t) + X(t)^T A(t)^T X(t) = X(t)^T A(t) X(t) - X(t)^T A(t) X(t) = 0$$

si bien que f est constante. Or, $f(0) = I_n$ puisque $X(0) \in \mathcal{O}_n(\mathbb{R})$. Par conséquent :

$$\forall t \in \mathbb{R},\ f(t) = I_n$$

Autrement dit, on a bien :

$$\forall t \in \mathbb{R},\ X(t) \in \mathcal{O}_n(\mathbb{R})$$

$\square$

Une identité remarquable

On considère A et B deux matrices de $\mathcal{M}_n(\mathbb{C})$ et on pose $C = AB - BA$. On suppose que A et B commutent avec C. On définit :

$$\forall t \in \mathbb{R},\ M(t) = e^{-t(A+B)}e^{tA}e^{tB}$$

Exprimer $M(t)$ en fonction de C et t.

Démonstration. On utilise l'astuce de dérivation : en mettant la dérivée de la première fonction à sa droite, et celles des deux suivantes à leur gauche, on obtient :

$$\forall t \in \mathbb{R},\ M'(t) = e^{-t(A+B)}\left(-Be^{tA} + e^{tA}B\right)e^{tB}$$

On écrit alors :

$$\forall t \in \mathbb{R},\ -Be^{tA} + e^{tA}B = \sum_{n=0}^{+\infty} \frac{t^n}{n!}(A^nB - BA^n)$$

Or, il est classique, par récurrence, que

$$\forall n \in \mathbb{N}^*,\ A^nB - BA^n = nAc^{n-1}$$

Par conséquent, après réindexation et utilisation de la définition de l'exponentielle, on en déduit :

$$\forall t \in \mathbb{R}, M'(t) = e^{-t(A+B)}tCe^{tA}e^{tB}$$

Or, comme C commute avec A, C commute avec e^{tA} (par continuité du produit), si bien qu'on a finalement :

$$\forall t \in \mathbb{R},\ M'(t) = tCM(t)$$

Comme de plus $M(0) = I_n$, on en déduit finalement l'identité :

$$\forall t \in \mathbb{R},\ M(t) = \exp\left(\frac{t^2}{2}C\right)$$

$\square$

Inégalité de Liapounov

Soit $a < b$ et $f : [a, b] \to \mathbb{R}$. Soit u une fonction non nulle de classe $\mathcal{C}^2$ solution de $y'' + fy = 0$ sur $[a, b]$ vérifiant $u(a) = u(b) = 0$. Montrer l'inégalité de Liapounov :

$$\int_a^b |f| \geqslant \frac{4}{b-a}$$

Démonstration. Puisque les zéros sont isolés, on peut sans perte de généralité supposer que a et b sont des zéros consécutifs de u, ce qui revient à prouver une inégalité encore plus forte que celle demandée. Ensuite, on utilise la méthode de variations des constantes pour montrer que :

$$\forall t \in [a,b],\ (b-a)u(t) = (t-a)\int_t^b u(s)f(s)(b-s)\ ds + (b-t)\int_a^t u(s)f(s)(s-a)\ ds$$

Ensuite, on considère t_0 en lequel la norme infinie de u sur $[a,b]$ est atteinte (qui est strictement positive car u est non nulle). L'inégalité triangulaire permet d'obtenir :

$$(b-a)\|u\|_\infty \leqslant (t_0-a)\int_{t_0}^b \|u\|_\infty |f(s)|(b-t_0)\ ds + (b-t_0)\int_a^{t_0} \|u\|_\infty |f(s)|(t_0-a)\ ds$$

On en déduit en regroupant les termes et en simplifiant par la norme infinie non nulle :

$$b-1 \leqslant (b-t_0)(t_0-a)\int_a^b |f|$$

Or, $x \mapsto (b-x)(x-a)$ atteint son maximum en $\dfrac{a+b}{2}$ (fonction polynomiale de degré 2), où elle vaut alors $\dfrac{(b-a)^2}{4}$. En majorant puis divisant par cette dernière quantité, on obtient bien :

$$\int_a^b |f| \geqslant \frac{4}{b-a}$$

□

Théorème de stabilité de Liapounov

On considère $T >$ et q une fonction continue sur $\mathbb{R}$ T-périodique. On note S l'ensemble des solutions de l'équation (E) :

$$y'' + qy = 0$$

On note y_1 (resp. y_2) l'élément de S vérifiant $y_1(0) = 1$ et $y_1'(0) = 0$ (resp. $y_2(0) = 0$ et $y_2'(0) = 1$).

1. Montrer que si $f \in S$, alors $f_T : x \mapsto f(x+T)$ appartient aussi à S. On note alors Φ l'endomorphisme de S qui à f associe f_T ainsi que A sa matrice dans la base (y_1, y_2).
2. Calculer le déterminant de A.
3. On suppose que $|\mathrm{Tr}(A)| < 2$. Montrer que tout élément de S est borné.
4. On suppose q positive non identiquement nulle. Montrer que tout élément de S possède possède au moins deux zéros.
5. On suppose q positive non identiquement nulle et $T\displaystyle\int_0^T q < 4$. En utilisant l'inégalité de Liapounov, montrer que les solutions de (E) sont toutes bornées.

Démonstration. Remarquons qu'on a pour tout $f \in S$, $f = f(0)y_1 + f'(0)y_2$.

1. Immédiat en utilisant la T-périodicité de q.

2. D'après notre remarque préliminaire, $\Phi(y_1) = y_1(T)y_1 + y_1'(T)y_2$ et symétriquement pour $\Phi(y_2)$. Alors :

$$A = \begin{pmatrix} y_1(T) & y_2(T) \\ y_1'(T) & y_2'(T) \end{pmatrix}$$

Pour le déterminant de A, on reconnaît le Wronskien évalué en T. Or, le Wronskien est constant puisqu'il n'y a pas de terme en y' dans (E). Par conséquent, il est égal au Wronskien en 0, soit :

$$\det(A) = 1$$

3. Matrice 2×2, on nous a demandé de calculer le déterminant à la question d'avant et on nous donne une information sur la trace, il faut penser polynôme caractéristique ! L'hypothèse nous assure que χ_A possède deux valeurs propres complexes non réelles conjuguées λ et $\overline{\lambda}$. De plus, elle sont de module 1 car leur produit vaut $\det(A) = 1$. On considère (u_1, u_2) une base de vecteurs propres des solutions complexes associée aux valeurs propres $(\lambda, \overline{\lambda})$. Alors, $|u_1|$ et $|u_2|$ sont T-périodiques. Elles sont donc bornées. Donc toute solution complexe est bornée. *A fortiori*, toute solution réelle est bornée.

4. En raisonnant un première fois par l'absurde en supposant qu'une solution y ne s'annule pas, il est classique, en utilisant la convexité ou la concavité, que y doit être constante, puis constante nulle. En raisonnant par l'absurde une seconde fois en supposant que y possède uniquement un point d'annulation x_0, on peut sans perte de généralité supposer y négative avant x_0 puis positive après. Alors, y est concavec après x_0, donc y' admet une limite dans $\mathbb{R} \cup \{-\infty\}$. Cette limite ne peut être strictement sinon positive sans quoi y tendrait vers $-\infty$ en $+\infty$, ce qui contredirait sa positivité. Donc cette limite est positive et y' est positive après x_0 donc y croît après x_0. Elle admet donc une limite l strictement positive en $+\infty$. Mais, à partir d'un certain $y'' \leqslant -\dfrac{1}{2}lq$, et puisque q n'est pas identiquement nulle et est périodique, l'intégrale de y'' diverge vers $-\infty$, donc y' tend vers $-\infty$, ce qui est là encore absurde.

5. On essaye de se ramener à la question 3. En raisonnant par l'absurde, on suppose que $|\mathrm{Tr}(A)| \geqslant 2$. Alors A admet une valeur propre réelle λ, et on peut considérer u un vecteur propre de l'endomorphisme Φ associé à la valeur propre λ. D'après la question 4, u admet un zéro a. Puisque c'est un vecteur propre, $a+T$ est aussi un zéro de u. L'inégalité de Liapounov fournit alors :

$$T \int_a^{a+T} q \geqslant 4$$

ce qui est absurde par hypothèse (la valeur de l'intégrale de q sur une période est une constante par périodicité). On en déduit que $|\mathrm{Tr}(A)| < 2$, puis la question 3 conclut.

$\square$

Pas de sous-espace de dimension finie impaire stable

On considère l'application T définie sur $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$ par :

$$\forall x \in \mathbb{R},\ T(f)(x) = f(x) + \int_0^x f(t)\ dt$$

Montrer que f est un automorphisme de $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$. Existe-t-il un sous-espace vectoriel de $\mathcal{C}^\infty(\mathbb{R},\mathbb{R})$ de dimension finie impaire stable par T ?

Démonstration. La caractère linéaire est immédiat. Pour l'injectivité et la surjectivité, utiliser le théorème de Cauchy linéaire. Pour la dernière question, on raisonne par l'absurde en supposant que c'est la cas. Alors, l'induit de T sur cet espace admet une valeur propre et un vecteur propre associé. On distingue deux cas : si la valeur propre vaut 1 ou non. Dans tous les cas, on montre que le vecteur propre est nul, ce qui est absurde. On en déduit qu'il n'existe pas de sous-espace de dimension finie impaire stable par T. □

Paramètre symétrique constant

Soit $A \in \mathcal{S}_n(\mathbb{R})$. On considère l'équation différentielle $X' = AX$.

1. Soit X une solution non nulle. Montrer que $t \mapsto \ln(\|X(t)\|_2)$ est convexe sur $\mathbb{R}$.
2. On suppose de plus $A \in \mathcal{S}_n^{++}(\mathbb{R})$. Soit X une solution non nulle. Montrer que $t \mapsto \|X(t)\|_2$ établit une bijection de $\mathbb{R}$ sur $\mathbb{R}_+^*$.

Démonstration. On réalise tout d'abord un travail préliminaire utile pour les deux question. En effet, en notant λ_i les éléments du spectre de A, on peut, après orthodiagonalisation, écrire

$$\forall t \in \mathbb{R}, X(t) = P\mathrm{Diag}(e^{\lambda_i t})P^{-1}X_0$$

Si X est non nulle, X_0 est non nul et on pose $Y_0 = P^{-1}X_0$ qui est donc tout aussi non nul. De plus, puisque P est orthogonale, on sait que

$$\forall t \in \mathbb{R},\ \|X(t)\| = \|\mathrm{Diag}(e^{\lambda_i t})Y_0\|$$

Par conséquent, après produit et expression de la norme 2, on trouve :

$$\forall t \in \mathbb{R},\ \|X(t)\| = \sqrt{\sum_{i=1}^n e^{2\lambda_i t} y_i^2}$$

Puis :

1. Passer au logarithme et montrer que la fonction obtenue (sans le 1/2) est convexe. Pour cela, la dériver deux fois et utiliser l'inégalité de Cauchy-Schwarz pour montrer que le numérateur est positif.
2. Remarquer que les valeurs propres sont alors strictement positives. La fonction $t \mapsto \|X(t)\|$ est alors strictement croissante et ses limites sont 0 en $-\infty$ et $+\infty$ en $+\infty$ puisque la solution est non nulle. Le théorème des valeurs intermédiaires et la stricte croissance permettent de conclure.

□

CNS de périodicité d'une solution d'une "équation périodique"

On considère l'équation différentielle d'ordre n suivante :

$$y^{(n)} + \sum_{k=0}^{n-1} a_k(t) y^{(k)} = b(t)$$

où les a_k et b sont des fonctions continues toutes périodiques de même période T. Soit y une solution de cette équation. Montrer que y est T-périodique si, et seulement si,

$$\forall k \in [\![0, n-1]\!],\ y^{(k)}(T) = y^{(k)}(0)$$

Démonstration. Considérer $z : t \mapsto y(t+T)$. z est aussi solution de l'équation puisque les a_k et b sont T-périodiques. Ensuite, y est périodique si, et seulement si, $y = z$, ce qui équivaut, puisqu'elles sont solutions d'une même équation différentielle, à l'égalité des dérivées k-èmes en 0, et correspond bien à la CNS recherchée. □

Ordre 2 et fausse périodicité

Soit $T > 0$ ainsi que $(a, b) \in \mathbb{R}^2$. On considère y une solution de l'équation différentielle

$$y'' + ay = b$$

telle que $y(T) = y(0) = 0$. Montrer que $\forall n \in \mathbb{Z},\ y(nT) = 0$.

Démonstration. Considérer $z : t \mapsto y(t+T)$ la translation. Elle est aussi solution de l'équation. On considère alors le wronskien de y et z. Celui-ci est constant car il n'y a pas de terme en y' dans l'équation. Et, en évaluant en 0, il vaut 0 donc est constamment nul. Si y est la fonction nulle, le résultat est évident. On suppose désormais que y n'est pas la fonction nulle. Il s'agit alors simplement d'une récurrence en utilisant que la dérivée de y ne peut pas s'annuler en un point où y s'annule, et en évaluant le wronskien en nT pour obtenir l'annulation de z en nT donc de y en $(n+1)T$. On "propage" en quelque sorte les annulations grâce au wronskien. □

Chapitre 19

Calcul différentiel

19.1 Points méthode

Montrer une différentiabilité

Pour montrer que f est différentiable en a, on peut chercher une application linéaire u telle que

$$f(a+h) - f(a) - u(h) = o(h)$$

Montrer une non-différentiabilité

Une application $f : \Omega \to F$ n'est **pas différentiable** en a :

- si elle n'admet pas de dérivée selon tout vecteur en a ;
- si elle en admet, mais que l'application $u : h \mapsto D_h f(a)$ n'est pas linéaire ou ne vérifie pas $f(a+h) - f(a) - u(h) = o(h)$.

Étudier une différentiabilité

Pour étudier si une fonction $f : \Omega \to F$ est différentiable en a, on peut vérifier l'existence de toutes ses dérivées partielles en a, puis voir si l'application linéaire :

$$u : h \mapsto \sum_{j=1}^{p} h_j \partial_j f(a)$$

vérifie $f(a+h) - f(a) - u(h) = o(h)$.

Montrer une classe $\mathcal{C}^1$

Pour démontrer qu'une fonction $f : \Omega \to F$ est de classe $\mathcal{C}^1$:

- on cherche d'abord à utiliser les théorèmes généraux de manipulation des fonctions de classe $\mathcal{C}^1$;
- si ceux-ci ne s'appliquent pas, on peut chercher à montrer que dans une base donnée, toutes les dérivées partielles de f sont définies et continues sur Ω.

Montrer une classe $\mathcal{C}^k$

Pour montrer qu'une fonction est de classe $\mathcal{C}^k$, on essaie tout d'abord d'utiliser les théorème généraux ou de s'y ramener.

Montre une classe $\mathcal{C}^\infty$ dans des cas compliqués

Dans les cas plus compliqués, pour montrer que f est de classe $\mathcal{C}^\infty$, on trouve une classe $\mathcal{S}$ de fonctions telle que :

- $f \in \mathcal{S}$;
- tout élément de $\mathcal{S}$ est élément continu ;
- $\mathcal{S}$ est stable par dérivation partielle.

Recherche d'*extrema*

Pour démontrer qu'une fonction $f : A \to \mathbb{R}$ admet un extremum en a, on peut étudier le signe de $g : h \mapsto f(a+h) - f(a)$.

- Si g est de signe fixe au voisinage de 0, alors f admet un *extremum* local en a.
- Si g est de signe fixe sur tout son domaine de définition, alors f admet un *extremum* global en a.

Montrer qu'un point n'est pas un extremum local

En reprenant les notations du point méthode précédent, si l'on montre que, sur tout voisinage de 0, la fonction g prend des valeurs strictement positives et des valeurs strictement négatives, alors f n'admet pas d'*extremum* local en a. En pratique, cela pourra se faire en étudiant le signe de $t \mapsto g(th)$ pour des vecteurs h bien choisis.

Lieux de recherche des *extrema* locaux

Les *extrema* locaux de $f :\to \mathbb{R}$ sont à chercher parmi :

- les points critiques de f ;
- les points de $\mathring{A}$ où f n'est pas différentiable ;
- les points de $A \setminus \mathring{A}$.

Nature des *extrema* dans le cas $\mathcal{C}^2$ euclidien

Soit $f : \Omega \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$, où Ω est un ouvert de $\mathbb{R}^2$ et a un point critique de f, ainsi que $H_f(a)$ sa matrice hessienne en a.

- Si $\det(H_f(a)) > 0$ et $\mathrm{Tr}(H_f(a)) > 0$, alors f admet un minimum local strict en a.
- Si $\det(H_f(a)) > 0$ et $\mathrm{Tr}(H_f(a)) >< 0$, alors f admet un maximum local strict en a.
- Si $\det(H_f(a)) < 0$, alors f n'admet pas d'*extremum* local strict en a.

Attention : dans le cas où $\det(H_f(a)) = 0$, on ne peut rien conclure sans une étude approfondie.

19.2 Astuces

Différentielle du déterminant

Théorème d'inversion locale

Théorème d'inversion globale

19.3 Exercices classiques

Matrices cycliques

On considère :

$$\varphi : \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) & \longrightarrow & \mathbb{R}^n \\ M & \longmapsto & (\mathrm{Tr}(M), \dots, \mathrm{Tr}(M^n)) \end{array}$$

1. Montrer que φ est de classe $\mathcal{C}^1$ et calculer sa différentielle en tout point.
2. Montrer que pour tout $M \in \mathcal{M}_n(\mathbb{R})$, on a $\mathrm{rg}(d\varphi(M)) = \deg(\pi_M)$.
3. En déduire que l'ensemble : $\{M \in \mathcal{M}_n(\mathbb{R}) \ : \ \chi_M = \pi_M\}$ est un ouvert de $\mathcal{M}_n(\mathbb{R})$.

Démonstration. Le nom de l'exercice vient du fait que le dernier ensemble est aussi l'ensemble des matrices M telles qu'il existe un vecteur X tel que $(X, \dots, M^{n-1}X)$ soit une base de $\mathbb{R}^n$, qu'on appelle ensemble des matrices cycliques.

1. Pour montrer la classe $\mathcal{C}^1$, utiliser les théorèmes généraux.

2. Utiliser le gradient.
3. Caractériser la liberté d'une famille par l'inversibilité d'un matrice.

□

Espaces tangents à $\mathcal{O}_n(\mathbb{R})$ et $\mathcal{U}_n(\mathbb{C})$ en I_n

L'ensemble des vecteurs tangents à $\mathcal{O}_n(\mathbb{R})$ (resp. $\mathcal{U}_n(\mathbb{C})$) en I_n est $\mathcal{A}_n(\mathbb{R})$ (resp. l'ensemble des matrices anti-hermitiennes, *ie* égales à l'opposé de leur transconjuguée).

Démonstration. On prouve le résultat pour $\mathcal{O}_n(\mathbb{R})$, la preuve est entièrement symétrique pour $\mathcal{U}_n(\mathbb{C})$. Soit A un vecteur tangents à $\mathcal{O}_n(\mathbb{R})$ en I_n. On fixe $\varepsilon > 0$ et

$$\gamma : \quad]-\varepsilon, \varepsilon[\quad \longrightarrow \mathcal{O}_n(\mathbb{R})$$

dérivable en 0 telle que $\gamma(0) = I_n$ et $\gamma'(0) = A$. Alors, en considérant $\varphi : t \mapsto \gamma(t)^T$, qui est alors tout autant définie et dérivable en 0 que γ, de dérivée $\varphi'(0) = I_n^T = I_n$. Or :

$$\forall t \in]-\varepsilon, \varepsilon[, \ \gamma(t)\varphi(t) = I_n$$

Donc, en dérivant en 0 :

$$0 = (\gamma\varphi)'(0) = \gamma'(0)\varphi(0) + \gamma(0)\varphi'(0) = A + A^T$$

si bien que $A \in \mathcal{A}_n(\mathbb{R})$. Réciproquement, soit $A \in \mathcal{A}_n(\mathbb{R})$. On considère alors :

$$\begin{array}{rccc} \gamma : &]-\varepsilon, \varepsilon[& \longrightarrow & \mathcal{O}_n(\mathbb{R}) \\ & t & \longmapsto & \exp(tA) \end{array}$$

En effet, cette application est déjà bien définie puisque la transposée de l'exponentielle est l'exponentielle de la transposée et alors, puisque A est antisymétrique, $\exp(tA)$ est bien dans $\mathcal{O}_n(\mathbb{R})$ (en fait dans $\mathcal{SO}_n(\mathbb{R})$ même avec la formule $\det(\exp) = \exp(\mathrm{Tr})$). Ensuite, γ est dérivable de dérivée $t \mapsto A\gamma(t)$ (*cf* chapitre d'équations différentielles). Ainsi, γ est en particulier dérivable en 0 et :

$$\begin{cases} \gamma(0) = I_n \\ \gamma'(0) = A \end{cases}$$

si bien que A est effectivement un vecteur tangent à $\mathcal{O}_n(\mathbb{R})$ en I_n, ce qui conclut la preuve. □

Espaces tangent à $\mathcal{SL}_n(\mathbb{K})$ en I_n

L'ensemble des vecteurs tangents à $\mathcal{SL}_n(\mathbb{K})$ en I_n est l'ensemble des matrices de trace nulle.

Démonstration. On utilise le théorème du cours avec l'application $g : A \mapsto \det(A) - 1$ qui est de classe $\mathcal{C}^1$ et dont l'annulation correspond à $\mathcal{SL}_n(\mathbb{K})$. Sa différentielle en I_n est celle du déterminant et est bien non nulle :

$$dg(I) : H \mapsto \mathrm{Tr}(H\mathrm{Com}(I)^T) = \mathrm{Tr}(H)$$

Par résultat de cours, l'espace tangent à $\mathcal{SL}_n(\mathbb{K})$ en I_n est donc le noyau de cette différentielle, *ie* l'ensemble des matrices de trace nulle. □

Remarque. L'ensemble des matrices de trace nulle est de dimension $n^2 - 1$ si on travaille dans $\mathcal{M}_n(\mathbb{R})$ et $2n^2 - 2$ si on travaille dans $\mathcal{M}_n(\mathbb{C})$ (toujours en tant que $\mathbb{R}$-espaces vectoriels dans ce chapitre). Pour le montrer, appliquer le théorème du rang.

Une autre démonstration de l'inégalité arithmético-géométrique

Démontrer l'inégalité arithmético-géométrique en utilisant du calcul différentiel.

Démonstration. □

Lemme pour l'inversion locale

Démonstration. □

Théorème d'inversion locale

En utilisant l'exercice précédent, prouver le théorème d'inversion locale :

Démonstration. □

Chapitre 20

Dénombrabilité

20.1 Points méthode

Montrer qu'un ensemble infini est indénombrable

Pour montrer qu'un ensemble infini est dénombrable, on peut :

- exhiber une bijection de $\mathbb{N}$ sur A, ce qui revient à numéroter les éléments de A en suite (a_n) ;
- exhiber une injection de A dans $\mathbb{N}$ (ou dans un ensemble dénombrable) ;
- exhiber une surjection de $\mathbb{N}$ (ou d'un ensemble dénombrable) dans A

20.2 Astuces

Vocabulaire Lorsqu'un ensemble est dénombrable, c'est qu'il est au plus dénombrable et infini. Sinon, on dit seulement au plus dénombrable pour un ensemble en bijection avec une partie de $\mathbb{N}$.

20.3 Exercices classiques

Disques ouverts

On appelle disque ouvert de $\mathbb{C}$ tout ensemble de la forme $\{z \in \mathbb{C} : |z - p| < \rho\}$ pour $p \in \mathbb{C}$ et $\rho \in \mathbb{R}_+^*$ fixés. Soit $(D_i)_{i\in I}$ une famille de disques ouverts deux à deux disjoints. Montrer que I est au plus dénombrable.

Démonstration. Utiliser la densité de $\mathbb{Q}$ dans $\mathbb{R}$ pour les parties réelles et imaginaires pour montrer qu'un point de coordonnées rationnelles appartient à chacun des disques fermés. Ensuite, utiliser la dénombrabilité de $\mathbb{Q}^2$ pour conclure. $\square$

Chapitre 21

Probabilités

21.1 Points méthode

Loi conjointe et lois marginales

Soit (X, Y) un couple de variables aléatoires discrètes.

- Pour tout $x \in X(\Omega)$, on a :

$$\mathbb{P}(X = x) = \sum_{y \in Y(\Omega)} \mathbb{P}(X = x, Y = y)$$

- Pour calculer $\mathbb{P}(X = x, Y = y)$, il suffit de se limiter au cas où $\mathbb{P}(Y = y) \neq 0$ et alors :

$$\mathbb{P}(X = x, Y = y) = \mathbb{P}(Y = y)\mathbb{P}(X = x \mid Y = y)$$

Loi d'une fonction de deux variables aléatoires discrètes indépendantes

Connaissant la loi de deux variables aléatoires indépendantes X et Y, on peut en déduire la loi de tout variable aléatoire Z fonction de X et Y. Pour tout $z \in Z(\Omega)$, on écrit $\{Z = z\}$ comme réunion d'événements de la forme $\{X = x\} \cap \{Y = y\}$.

Détermination d'une espérance sans connaître la loi

Pour déterminer la loi d'une variable aléatoire discrète dont on ne connaît pas la loi, on peut chercher à la décomposer en somme de variables aléatoires discrètes d'espérance connue. Par exemple, on pourra décomposer la variable aléatoire sous forme de somme d'indicatrices, et utiliser le fait que l'espérance de l'indicatrice d'un événement est la probabilité de cet événement.

21.2 Astuces

Possibilités à toujours envisager Toujours envisager : la combinatoire, l'utilisation d'indicatrices ou les fonctions génératrices.

Formule du crible de Poincaré Elle s'énonce :

$$\mathbb{P}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n}(-1)^k \sum_{1\leqslant i_1<\ldots<i_k\leqslant n} \mathbb{P}\left(\bigcap_{j=1}^{k} A_{i_j}\right)$$

On peut la démontrer en développant $1 - \mathbf{1}_{\cup A_i}$ avec les complémentaires, de la distributivité généralisée et les produits d'indicatrices. On conclut en passant par linéarité de l'espérance avec la formule :

$$\mathbb{E}(\mathbf{1}_A) = \mathbb{P}(A)$$

Application. Cela peut permettre de calculer la probabilité d'avoir un dérangement en tirant au hasard un élément de S_n

Variables aléatoires ne prenant que deux valeurs Quand on a des variables aléatoires ne prenant que deux valeurs, se ramener 'a des variables suivant une loi de Bernoulli via une transformation affine (peut servir à faire apparaître des lois binomiales cachées !) C'est notamment le cas quand on somme des variables de Rademacher (exemple d'une marche aléatoire...)

Fonction caractéristique Pour X une variable aléatoire à valeurs dans $\mathbb{Z}$, sa fonction caractéristique $F_X : t \mapsto \mathbb{E}(e^{itX})$ caractérise sa loi et on a :

$$\forall n \in \mathbb{Z},\ \mathbb{P}(X = n) = \frac{1}{2\pi}\int_0^{2\pi} F_X(t)e^{-int}\,dt$$

Le transfert d'indépendance permet de montrer que pour des variables aléatoires mutuellement indépendantes $X_1, \ldots, X_n$, on a, comme pour les fonctions génératrices :

$$F_{X_1+\ldots+X_n} = \prod_{i=1}^{n} F_{X_i}$$

(pas besoin que les variables aléatoires soient à valeurs dans $\mathbb{Z}$ pour cela).

Application. Permet de retrouver les stabilités de la loi de Poisson et de la loi binomiale

Fonction génératrice Pour montrer qu'une fonction f est la série génératrice d'une variable aléatoire, il faut montrer :

1. qu'elle est DSE, de RCV$\geqslant 1$;
2. que les coefficients du développement sont positifs ;
3. que la somme des coefficients vaut 1, ou encore que $f(1) = 1$ (existera si f est effectivement une série génératrice).

Limite supérieure et limite inférieure ; lemmes de Borel-Cantelli Pour une suite (A_n) d'événements, on définit la limite supérieure par :

$$\overline{\lim} A_n = \bigcap_{n\in\mathbb{N}} \bigcup_{p\geqslant n} A_p$$

et la limite inférieure par :

$$\underline{\lim} A_n = \bigcup_{n\in\mathbb{N}} \bigcap_{p\geqslant n} A_p$$

On dispose alors du premier lemme de Borel-Cantelli :

$$\text{si } \sum_{n=0}^{+\infty} \mathbb{P}(A_n) < +\infty \text{ alors } \mathbb{P}(\overline{\lim} A_n) = 0$$

On dispose aussi du second lemme de Borel-Cantelli : lorsque les A_n sont mutuellement indépendants, on a :

$$\text{si } \sum_{n=0}^{+\infty} \mathbb{P}(A_n) = +\infty \text{ alors } \mathbb{P}(\overline{\lim} A_n) = 1$$

Minimum de deux lois géométriques indépendantes On se donne $X \sim \mathcal{G}(p_1)$ et $Y \sim \mathcal{G}(p_2)$ indépendantes. On pose $q_1 = 1 - p_1$, $q_2 = 1 - p_2$ ainsi que $p = 1 - q_1q_2$. Alors $\min(X,Y) \sim \mathcal{G}(p)$. En effet, on a :

$$\{\min(X,Y) \geqslant k\} = \{X \geqslant k\} \cap \{Y \geqslant k\}$$

donc par indépendance, on a :

$$\mathbb{P}(\min(X,Y) \geqslant k) = q_1^{k-1}q_2^{k-1}$$

On obtient donc, puisque $\{\min(X,Y) = k\} = \{\min(X,Y) \geqslant k\} \cap \overline{\{\min(X,Y) \geqslant k+1\}}$, la relation :

$$\mathbb{P}(\min(X,Y) = k) = (1 - q_1q_2)(q_1q_2)^{k-1}$$

Cela traduit bien le fait que $\min(X,Y) \sim \mathcal{G}(p)$.

Maximum et minimum de variables aléatoires Quand voit un maximum ou un minimum de variables aléatoires, s'intéresser aux événements $\max(\ldots) \geqslant \varepsilon$ ou $\min(\ldots) \leqslant \varepsilon$ car on peut les écrire comme des intersections ou des unions d'événements de la forme $\{X \geqslant \varepsilon\}$ ou $\{X \leqslant \varepsilon\}$.

Découpage par les indicatrices On pourra penser à "conditionner" avec des indicatrices, notamment en découpant des variables aléatoires comme

$$X = \mathbf{1}_{\{X\leqslant a\}}X + \mathbf{1}_{\{X>a\}}X$$

Cela peut permettre d'utiliser le fait que $\mathbb{E}(1_A) = \mathbb{P}(A)$, de faire jouer des inégalités sur l'espérance, et d'utiliser d'autres sortes d'outils.

Découpage adapté à des fonctions convexes On pourra penser à écrire, si X est à valeurs dans $[a, b]$, que

$$X = \frac{b-X}{b-a}a + \frac{X-a}{b-a}b$$

Cela permet d'obtenir une inégalité en appliquant une fonction convexe ou concave. En particulier, cela est très utile si la variable aléatoire est centrée. En général, des exercices sur des inégalités de concentration peuvent commencer comme cela.

Numérotation et ordonnement dans le cas fini Quand on travaille sur des espaces probabilisés finis, pour se simplifier la vie, ne pas hésiter à numéroter, voire à ordonner, les éléments de l'univers.

Résultat de convergence en probabilité Soit (X_n) une suite de variables aléatoires admettant des moments d'ordre 2 telle que

$$\mathbb{E}(X_n) \xrightarrow[n\to+\infty]{} m \text{ et } \mathbb{V}(X_n) \xrightarrow[n\to+\infty]{} 0$$

Alors, on a :

$$\forall \varepsilon > 0,\ \mathbb{P}(|X_n - m| \geqslant \varepsilon) \xrightarrow[n\to+\infty]{} 0$$

Démonstration : soit $\varepsilon > 0$. Si $|X_n - m| \geqslant \varepsilon$, alors $|X_n - \mathbb{E}(X_n)| + |\mathbb{E}(X_n) - m| \geqslant \varepsilon$. On obtient donc à partir d'un certain rang, par croissance de la probabilité :

$$\mathbb{P}(|X_n - m| \geqslant \varepsilon) \leqslant \mathbb{P}(|X_n - \mathbb{E}(X_n) \geqslant \varepsilon - |\mathbb{E}(X_n) - m|)$$

L'inégalité de Bienaymé-Tchebychev permet de conclure avec l'hypothèse $\mathbb{V}(X_n) \xrightarrow[n\to+\infty]{} 0$.
Remarque : Cette méthode fonctionne la plupart du temps pour établir une convergence en probabilité.

Loi forte des grands nombres dans L^4 Soit (X_n) une suite de variables aléatoires iid toutes L^4 et centrées. Alors

$$\forall \varepsilon > 0,\ \sum_{n\geqslant 0} \mathbb{P}\left(\frac{X_1 + \ldots + X_n}{n} \geqslant \varepsilon\right) \text{ converge}$$

Il faut utiliser l'inclusion

$$\left\{\frac{X_1 + \ldots + X_n}{n} \geqslant \varepsilon\right\} \subset \left\{\frac{(X_1 + \ldots + X_n)^4}{n^4} \geqslant \varepsilon^4\right\}$$

On distribue ensuite pour montrer que

$$\mathbb{E}\left((X_1 + \ldots + X_n)^4\right) = O(n^2)$$

En effet, seul les termes où les 4 indices sont distincts, ou bien ou les termes où on a deux indices i et deux indices j avec $i \neq j$ ne sont pas nuls après passage à l'espérance et par indépendance, donc on obtient bien le $O(n^2)$. L'inégalité de Markov fournit alors un $O\left(\frac{1}{n^2}\right)$, ce qui permet de conclure.

21.3 Exercices classiques

Taux de panne

Avec $(x_n)_{n\in\mathbb{N}^*}$, on obtient par récurrence :

$$\mathbb{P}(X \geqslant n) = \prod_{k=1}^{n-1}(1-x_k)$$

et par conséquent $\mathbb{P}(X = n) = x_n \prod_{k=1}^{n-1}(1-x_k)$. Ensuite, il s'agit simplement d'utiliser ces formules dans tous les sens, de remarquer que

$$\mathbb{P}(X \geqslant n) \to 0$$

et de passer au ln les produits pour montrer qu'ils tendent vers $-\infty$.

Urnes de Polya

On tire commence avec b boules blanches et r boules rouges. Lorsqu'on tire une boule, on rajoute c boules de la couleur de la boule qu'on vient de tirer et on recommence. Probabilité de tirer une boule blanche au n-ème tirage ?

Démonstration. On note $\mathbb{P}_n(b,r)$ cette probabilité. Il faut **conditionner par rapport au premier événement** (en effet, on ne peut pas le faire par rapport au dernier, puisque celui-ci dépend de tout ce qu'il s'est passé avant). On obtient la relation de récurrence :

$$\mathbb{P}_n(b,r) = \frac{b}{b+r}\mathbb{P}_{n-1}(b+c,r) + \frac{r}{b+r}\mathbb{P}_{n-1}(b,r+c)$$

Par récurrence, cela permet de montrer que pour tous n, b et r, on a :

$$\mathbb{P}_n(b,r) = \frac{b}{b+r}$$

□

Urne d'Erhenfest

Démonstration. Procéder par récurrence pour le calcul de l'espérance. Conditionner. Se représenter matriciellement le problème peut aider : on a une matrice dont tous les coefficients sont nuls sauf ceux sur la sous-diagonale et la sur-diagonale. Ensuite, on peut faire le calcul à la main en regroupant bien les termes pour obtenir une relation arithmético-géométrique sur l'espérance. □

Nombre de points fixes Pour calculer l'espérance et la variance, écrire le nombre de points fixes comme une somme d'indicatrice et déterminer les probabilités des événements associés. On peut notamment calculer l'espérance et la variance du nombre de points fixes d'une permutation $\sigma \in S_n$ de cette façon.

Espérance et Cauchy-Schwarz On peut montrer que

$$\mathbb{E}(X)\mathbb{E}\left(\frac{1}{X}\right) \geqslant 1$$

en appliquant l'inégalité de Cauchy-Schwarz à $\sqrt{X}$ et $\dfrac{1}{\sqrt{X}}$ et déterminer ainsi les cas d'égalité. On a une variante si $X \sim Y$ et X et Y sont indépendantes pour montrer

$$\mathbb{E}\left(\frac{X}{Y}\right) \geqslant 1$$

On peut alors appliquer le résultat précédent avec un transfert d'indépendance et de loi, ou bien on peut simplement remarquer que par transfert d'indépendance et de loi

$$\mathbb{E}\left(\frac{X}{Y}\right) = \mathbb{E}\left(\frac{Y}{X}\right)$$

sommer les deux, puis utiliser le fait que la fonction

$$x \mapsto x + \frac{1}{x}$$

est minorée par 2 sur $\mathbb{R}_+^*$

Chapitre 22

Astuces en vrac

Montrer une égalité Quand on doit montrer une égalité entre deux expressions, bien choisir celle de laquelle on part.

Degré de liberté Parfois, il faut essayer de se créer un degré de liberté.

Une identité à connaître

$$(a^2 + b^2) \times (c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

Pour le démontrer et y penser, utiliser :

$$|a + ib|^2 \times |c + id|^2 = |(ac - bd) + i(ad + bc)|^2$$

Application. Permet de prouver que le produit de deux sommes de deux carrés est une somme de deux carrés.

Application. On dispose également d'une identité semblable pour des sommes de quatre carrés (le produit de deux sommes de quatre carrés est une somme de quatre carrés) : elle se prouve avec les quaternions. Cette dernière permet de montrer que tout entier est la somme de quatre carrés.

Entier le plus proche L'entier le plus proche d'un réel x est

$$n = \left\lfloor x + \frac{1}{2} \right\rfloor$$

Si x est exactement entre deux entiers, ceci donne le plus petit des deux.

Dérivées successives des cosinus et sinus On a :

$$\forall n \in \mathbb{N}, \forall x \in \mathbb{R}, \begin{cases} \cos^{(n)}(x) = \cos\left(x + \frac{n\pi}{2}\right) \\ \sin^{(n)}(x) = \sin\left(x + \frac{n\pi}{2}\right) \end{cases}$$

Théorème d'Al-Kashi

Loi des sinus

Fonctions homographiques L'application $x \mapsto \dfrac{ax+b}{cx+d}$ avec $c \neq 0$ est constante si, et seulement si, $ad - bc = 0$. En effet, on a :

$$\frac{ax+b}{cx+d} = \frac{a}{c} + \frac{bc-ad}{cx+d}$$

Une fonction homographique est strictement monotone sur ses intervalles où elle est continue.

Montrer une bijectivité Parfois, pour montrer une bijectivité, on peut exhiber la fonction réciproque.

Application. Pour les fonctions qui modélisent un processus qui va dans un sens, prendre la fonction qui modélise le processus inverse.

Une identité factorielle Si $i \in [\![0, n]\!]$, alors :

$$\prod_{\substack{j=0 \\ j \neq i}}^{n} (i-j) = (-1)^i (n-i) i!$$