Exercices de préparation aux oraux

Paul Coutant–Denord

22 novembre 2025

1 Introduction

Cette feuille contient divers exercices, fait pour des élèves de deuxième année de classe préparatoire, ainsi que leur correction et des indications. L'objectif est la préparation des oraux de concours. Une partie des exercices sont originaux, et sont inspirés par mes lectures ([5]) ou par mes cours à l'ENS Paris ([1], [4], [2], [3], etc). Ainsi, la difficulté des exercices est assez variable. Lorsqu'une année est précisé, c'est que j'ai repris un exercice déjà existant.
Si vous trouvez une faute, que ce soit sur le plan mathématique, ou sur le plan de l'orthographe, veuillez m'écrire à l'adresse suivante : paul.coutant–denord@ens.psl.eu

Table des matières

2 Algèbre

2.1 Relations binaires

2.1.1 Ensemble bien ordonné

Énoncé

Soit $(X, \leq)$ un ensemble totalement ordonné. On dit que $(X, \leq)$ a la propriété du bon ordre si et seulement si toute partie de X admet un élément minimum. Montrer que si $(X, \leq)$ et $(X, \geq)$ ont la propriété du bon ordre, alors X est fini.

Indication

On pourra montrer que, toute suite $(X, \leq)$ admet une sous suite croissante.

Correction

On va d'abord montrer l'indication. On considère l'ensemble des éléments de la suite, et on peut en extraire un minimum, qui constitue le premier terme de notre extraction $x_{\varphi(0)}$. On regarde ensuite l'ensemble des termes x_n avec $n \geq \varphi(0)$, et on extrait $x_{\varphi(1)}$ le minimum, et ainsi de suite.
Supposons par l'absurde que X soit infini. Soit alors (x_n) une suite injective. On peut en extraire une sous suite croissante (pour l'ordre $\leq$) qui est également injective. Mézalor l'ensemble que constitue les termes de cette sous suite admet un minimum pour l'ordre$\geq$, donc un maximum pour $\leq$, et donc, la suite est stationnaire. D'où l'absurdité

2.2 Polynômes

2.2.1 Autour des ensembles algébriques affines (type ENS semi-gentil)

Cet énoncé traite des fondements de la géométrie algébrique. Pour approfondir le sujet, voir [5]

Énoncé

Pour $S \subset \mathbb{R}[X_1, ..., X_n]$. On note $V(S) = \{x \in \mathbb{R}^n / \forall P \in S, P(x) = 0\}$. $V(S)$ est alors nommé "ensemble algébrique affine". On note également pour $X \subset \mathbb{R}^n, I(X) = \{P \in \mathbb{R}[X_1, ..., X_n]\} / \forall x \in X, P(x) = 0\}$
a) Montrer que, pour tout $X \subset \mathbb{R}^n$, $I(X)$ est un idéal de $\mathbb{R}[X_1, ..., X_n]$
b) Soit $S \subset \mathbb{R}[X_1, ..., X_n]$ non vide. On suppose que $V(S)$ est dense dans $\mathbb{R}^n$. Que dire de $V(S)$?
c) On note $\mathcal{F} = \{V(S), S \subset \mathbb{R}[X_1, ..., X_n]\}$. Montrer que $\mathcal{F}$ est stable par union finie et intersection quelconque.
d) L'ensemble $V = \{(t, \sin t), t \in \mathbb{R}\}$ est il un ensemble algébrique affine ?

Indications
a) Il suffit de vérifier chaque point de la définition d'un idéal
b) Que dire de $P \in S$? On rappel que les applications polynomiales sont continues pour la topologie normé de $\mathbb{R}^n$
c) On peut remarquer que $V(I(V(S))) = V(S)$. En particulier $I(V(S))$ est l'idéal engendré par S. On pourra utiliser que pour $(I_j)_{j \in J}$ une famille d'idéaux : $\sum_j I_j = \{i_{j_1} + ... + i_{j_r} / r \geq 1, j_k \in J, i_{j_k} \in I_{j_k}\}$ est un idéal. Si I, J sont deux idéaux, $IJ = \{\sum_{k=1}^r i_k j_k / i_k \in I, j_k \in J, r \geq 1\}$ est également un idéal.
d) On peut se donner explicitement un polynôme qui s'annule sur V, et essayer de montrer qu'il est nul. En particulier, on peut regarder les points d'annulations de $\sin t$.

Correction a) On a que : $0 \in I(X)$. Pour tout $P, Q \in I(X)$ et $x \in X$, $(P - Q)(x) = P(x) - Q(x) = 0$ donc $I(X)$ est un sous groupe de $\mathbb{R}[X_1, ..., X_n]$. De plus, soit $P \in I(X), Q \in \mathbb{R}[X_1, ..., X_n]$ et $x \in X$, $PQ(x) = P(x)Q(x) = 0$ donc $I(X)$ est bien un idéal.
b) Si $S = \emptyset$, $V(S) = \mathbb{R}^n$. Sinon, soit $P \in S$. Alors P est une fonction continue qui s'annule sur un ensemble dense, donc, P est nulle, ainsi, $V(S) = V(\{0\}) = \mathbb{R}^n$
c) On vérifie comme à la question a) que la somme d'idéaux et le produit d'idéaux définis dans les indications sont effectivement des idéaux. Pour l'union finie : il suffit de la montrer pour $V(S) \cup V(S')$. On a alors, $V(S) = V(I(S))$ et $V(S') = V(I(S'))$ et donc $V(S) \cup V(S') = V(I(S)I(S'))$. Pour l'intersection quelconques, on considères $(V(S_i))_{i \in I}$ et alors $\cap_{i \in I} V(S_i) = V(\sum I(S_i))$.
d) Soit $P = \sum_{k=0}^r Q_k(X) Y^r$ un polynôme à deux indéterminés, s'annulant sur V. Alors, comme sin s'annule en $n\pi$, on a que : $P(n\pi, \sin n\pi) = P(n\pi, 0) = 0$ donc $Q_0(n\pi) = 0$ pour tout $n \in \mathbb{Z}$, donc $Q_0 = 0$. On peut donc factoriser P par Y. Le polynôme obtenu en divisant par Y s'annule également sur $\{(t, \sin t), t \in \mathbb{R} \backslash \pi\mathbb{Z}\}$ et donc, par continuité de P/Y, P/Y s'annule également pour $t \in \pi\mathbb{Z}$. On a donc, comme précédemment $Q_1 = 0$, et on peut itérer ! Alors $P = 0$ et donc, V ne peut pas être un ensemble algébrique affine.

2.2.2 ENS SR 2024

Énoncé

Soit $P \in \mathbb{C}[X]$ à coefficient dans $\mathbb{T}$ les racines de l'unité non constant. Soit $z \in \mathbb{C}$ une racine de P. Montrer que $|z| < 2$

Indication

Écrire de manière explicite le polynôme, et isoler le terme en z^n.

Correction

Si $|z| \leq 1$, c'est gagné. Supposons alors $|z| > 1$. Notons $P = \sum_{k=0}^{n} a_k X^k$. Alors comme $P(z) = 0$, on a $\sum_{k=0}^{n} a_k z^k = 0$ donc $a_n z^n = -\sum_{k=0}^{n-1} a_k z^k$. Ainsi, en passant au module, et par inégalité triangulaire : $|z|^n \leq \sum_{k=0}^{n-1} |z|^k = \frac{1-|z|^n}{1-|z|} < \frac{|z|^n}{|z|-1}$ ainsi, $|z| - 1 < 1$ donc $|z| < 2$

2.2.3 Critère de Eisenstein

Énoncé

Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$, p premier tel que $p|a_0, ..., p|a_{n-1}$ mais $p \nmid a_n, p^2 \nmid a_0$.

Montrer que P est irréductible. *C'est le critère d'Eisenstein*

Indication

On pourra plonger la relation dans $\mathbb{Z}/p\mathbb{Z}$

Correction

Écrivons $P = QR$ et projetons dans $\mathbb{Z}/p\mathbb{Z}[X]$. On a alors que $\overline{P} = \overline{a_n} X^n = \overline{QR}$. Or par intégrité de $\mathbb{Z}/p\mathbb{Z}$, on a que $\overline{Q} = \overline{q} X^k$ et $\overline{R} = \overline{r} X^l$ et donc, Q, R ont un coefficient constant multiple de p, donc, le coefficient constant de P est multiple de p^2. Absurde.

2.3 Anneaux

Pour en apprendre plus sur l'algèbre commutative et en particulier sur les anneaux, voir [3]

2.3.1 Sur les idéaux maximaux de $\mathcal{C}^0([0,1],\mathbb{R})$ (Exercice type ENS)

Énoncé
Soit A un anneau commutatif unitaire. On dit qu'un idéal I est maximal si et seulement si il est différent de A et maximal pour la relation d'ordre que constitue l'inclusion (il n'est pas inclus dans un idéal plus gros autre que A).
Déterminer les idéaux maximaux de $A = \mathcal{C}^0([0,1],\mathbb{R})$.
On admettra la propriété de Borel-Lebesgue : Pour un compact X et $(F_i)_{i\in I}$ une famille de fermé de X, si $\cap_{i\in I} F_i = \emptyset$ alors, il existe $J \subset I$ fini tel que $\cap_{j\in J} F_j = \emptyset$.

Indication
Il convient de considérer les points d'annulations des fonctions d'un tel idéal.

Correction On va montrer que ces idéaux sont de la forme $I_x = \{f \in \mathcal{C}^0([0,1],\mathbb{R}), f(x) = 0\}, x \in \mathbb{R}$.
Soit I un idéal propre (différent de A). Alors tout élément de I admet au moins un point d'annulation. En effet, si $f \in I$ ne s'annule pas, alors f est inversible et $I = A$. De plus, deux fonctions $f, g \in I$ ont toujours un point d'annulation commun. En effet, on aurait sinon, comme $f^2 + g^2 \in I$, $f^2 + g^2$ serait inversible et donc $I = A$. Soit $F = \cap_{f\in I} f^{-1}\{0\}$. Alors F est un fermé. On admet alors la caractérisation de Borel-Lebesgue de la compacité, on a que si F est fini, il existe $f_1, ..., f_n$ tel que $\cap_{i=1}^n f_i^{-1}(\{0\}) = \emptyset$. Et donc, comme vu précédemment $f_1^2 + ... + f_n^2$ est inversible, ce qui aboutit à $I = A$. Ainsi, $F \neq \emptyset$ et donc, il existe $x \in F$ tel que tout $f \in I$ s'annule en x. En particulier $I \subset I_x$ et donc, par maximalité, $I = I_x$.

2.3.2 Caractéristique d'un anneau unitaire (Mines +)

Énoncé
a) Soit A un anneau unitaire. Montrer qu'il existe un unique morphisme d'anneau $\varphi : \mathbb{Z} \longrightarrow A$. Décrire son noyau.
b) Le noyau du morphisme précédent s'écrivant $c\mathbb{Z}$, avec $c \geq 0$, on appelle c la caractéristique de A. Montrer que c est un nombre premier
c) On se donne K un corps fini. Quels sont les cardinaux possibles pour K ?

Indications
a) $\mathbb{Z}$ est engendré par 1.
b) Écrire $c = ab$, et regarder $a1_A \times b1_A$

c) Notons p sa caractéristique. Il convient de voir K comme un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel

---

Correction

a) φ est déterminé par l'image de 1 or comme φ est un morphisme d'anneau, $\varphi(1) = 1_A$
b) Suivre l'indication. On a $a1_A \times b1_A = 0$ donc $a1_A = 0$ ou $b1_A = 0$ et donc, par définition de la caractéristique, on en conclut que c est premier.
c) Soit p la caractéristique de A. On définit, pour $\lambda \in \mathbb{Z}/p\mathbb{Z}$ et $x \in K, \lambda \cdot x = \lambda 1_K \times x$. Alors $(K, +, \cdot)$ est un $\mathbb{Z}/p\mathbb{Z}$ espace vectoriel. Comme il est de cardinal fini, il est de dimension fini, et donc isomorphe en tant qu'espace vectoriel à $(\mathbb{Z}/p\mathbb{Z})^n$ pour un certain $n \geq 1$. Et donc, son cardinal est p^n.

2.4 Groupes

Pour approfondir l'étude des groupes, et trouver de nombreux exercices à ce sujet, voir [2]

2.4.1 Éléments d'ordres finis dans un groupe infini (difficulté Mines)

Énoncé

a) Trouver un groupe infini dont tous les éléments sont d'un même ordre fini
b) Trouver, pour p un nombre premier, un groupe qui admet un élément d'ordre p^r pour tout $r \geq 1$.
c) Trouver un groupe et deux éléments a, b tel que $a^2 = b^2 = 1$ (ici 1 représente l'élément neutre du groupe) et tel que ab soit d'ordre infini

---

Correction

a) On peut par exemple prendre les suites à valeurs dans $\mathbb{Z}/p\mathbb{Z}$ avec p premier. Plus généralement, pour X un ensemble infini, $\mathcal{F}(X, \mathbb{Z}/p\mathbb{Z})$ convient.
b) Un exemple classique est le sous groupe quasi-cyclique de Prüfer : $\cup_{n\geq 1}\mu_{p^n}$ (μ_k désigne les racines $k-$ièmes de l'unité dans $\mathbb{C}$)
c) On peut regarder dans $G = \mathcal{S}(\mathbb{R})$ l'ensemble des bijections de $\mathbb{R}$ dans $\mathbb{R}$ et poser $a : x \mapsto 1 - x$ et $b : x \mapsto -x$ alors $a^2 = b^2 = Id$ mais $ab : x \mapsto x + 1$ qui n'est pas d'ordre fini.

2.4.2 Groupe d'exposant 2 (inspiré de ENS SR 2024 mais niveau Mines)

Énoncé

a) Soit G un groupe fini dont tous les éléments sont d'ordre 2. Montrer que G est abélien.
b) Montrer qu'un tel groupe peut être vu comme un $\mathbb{Z}/2\mathbb{Z}$ espace vectoriel. Que dire de son cardinal ?
c) (ENS SR 2024) On se donne $G \subset GL_n(\mathbb{R})$ un groupe dont tous les éléments sont dans $\mathcal{S}_\backslash(\mathbb{R})$. Montrer que $Card(G)|2^n$

Indication

b) Il faut poser $0.x = 0$ et $1.x = x$. De plus, tel espace vectoriel sera de dimension finie.
c) Utiliser le théorème spectral. Que dire des valeurs propres des éléments ?

Correction

a) Soit $a, b \in G$. On a que ab est d'ordre 2 donc $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$.
b) En posant la loi de l'indication, on a bien une loi de $\mathbb{Z}/2\mathbb{Z}-$espace vectoriel, qui comme il est de dimension fini, est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ et $Card(G) = 2^k$.
c) Soit $g \in G$. D'après le théorème spectral, g est diagonalisable or les valeurs propres de g sont des racines de l'unité (car $g^{Card(G)} = I_n$) donc, ces valeurs propres ne peuvent être que 1 ou -1 et donc, tout élément de G est d'ordre 2. En particulier, G est abélien, donc G est codiagonalisable, ce qui permet de voir qu'il contient au maximum 2^n élément. Or d'après la question b), G a un nombre d'élément qui est une puissance de 2, d'où le résultat.

2.4.3 Lemme de Cauchy dans le cas abélien (type Mines +)

Énoncé

Soit G un groupe fini, abélien. Soit $x_1, ..., x_n$ qui engendre G et d'ordre $d_1, ..., d_n$.
a) Montrer que $Card(G)|d_1...d_n$
b) En déduire que si p est un facteur premier de $Card(G)$, alors il existe un élément d'ordre p dans G.
Il s'agit du lemme de Cauchy, qui peut être démontrer dans le cas non abélien. Mieux, le théorème de Sylow nous permet même d'affirmer l'existence d'un sous groupe d'ordre une puissance de p maximale. L'exercice ci-dessus provient du TD d'Algèbre I donné en 2025 par Louise Nataf, vous pouvez trouver d'autres exercices sur les groupes sur sa page perso

---

Indication Considérer un morphisme $\varphi : \prod_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} \longrightarrow G$

Correction

a) Soit $\varphi : \begin{array}{c} \mathbb{Z}/d_1\mathbb{Z} \times ... \times \mathbb{Z}/d_n\mathbb{Z} \longrightarrow G \\ (k_1, ..., k_n) \mapsto x_1^{k_1}...x_n^{k_n} \end{array}$. Alors φ est un morphisme de groupe surjectif. Or pour tout $x \in G$ il y a $Card(\ker\varphi)$ antécédent. Ceci montre que $Card(G) \times Card(\ker\varphi) = d_1...d_n$, et on a le résultat.

b) Soit p premier divisant $Card(G)$ alors il existe i tel que $p|d_i$ donc on peut écrire $d_i = pm$ et alors x_i^m est d'ordre p.

2.5 Arithmétique

2.5.1 Infinité de triplet pythagoricien

Énoncé

Montrer qu'il existe une infinité de triplet pythagoricien $(a, b, c) \in \mathbb{Z}^3$ ($a^2 + b^2 = c^2$) non proportionnels.

Indication

On se ramènera à des considérations géométriques

Correction

Soit (a, b, c) un triplet pythagoricien non nul.

On va se ramener à un problème de géométrie. En effet, $\frac{a^2}{c^2} + \frac{b^2}{c^2} = 1$ et donc le point $(a/c, b/c)$ est un point rationnel du cercle unité. De plus, si l'on note $\pi : (\mathbb{Z}^*)^3 \longrightarrow \mathbb{Q}^2$ tel que $\pi(a, b, c) = (a/c, b/c)$, alors deux triplets proportionnels sont envoyés par π sur le même point. Ainsi, si l'on montre qu'il y a une infinité de point à coordonnées rationnelles sur le cercle unité, c'est gagné.

Pour cela, on va considérer pour $t \in \mathbb{R}$, l'intersection de la droite passant par $(-1, 0)$ et $(0, t)$. Le point en question, de coordonnée (x, y) vérifie :

$y = t(x + 1)$ et $x^2 + y^2 = 1$. On a alors que $t^2(x^2 + 2x + 1) + x^2 - 1 = x^2(1 + t^2) + 2xt^2 + t^2 - 1 = 0$ or $4t^4 - 4(t^2 - 1)(t^2 + 1) = 4$ et donc $x = -\frac{t^2 \pm 1}{1+t^2}$.

Or on s'intéresse au point différent de $(-1, 0)$, donc on veut $x = \frac{1-t^2}{1+t^2}$ et alors $y = \frac{2t}{1+t^2}$.

Ainsi, comme on peut prendre une infinité de t rationnelle, on obtient bien une infinité de points à coordonnées rationnelles, et donc il existe bien une infinité de triplet pythagoricien non proportionnels.

2.5.2 X 2024

Énoncé

Soient $n \in \mathbb{N}, P \in \mathbb{Z}[X]$ de degré majoré par n, Δ le pgcd de $P(0), ..., P(n)$. Montrer que pour tout $k \in \mathbb{Z}$, $\Delta | P(k)$

Indication

On pourra considérer les polynômes interpolateurs de Lagrange.

Correction

Soit $L_k = \prod_{i=0, i\neq k}^{n} \frac{X-i}{k-i}$. On a alors que $P = \sum_{k=0}^{n} P(k) L_k$.
Montrons donc que pour $k \in [|0, n|]$, L_k est à valeur entière.
On a $L_k(i) = \frac{i(i-1)...(i-n)}{(k)(k-1)(1)(-1)...(k-n)}$ et alors, on peut faire apparaitre des coefficients binomiaux, ce qui montre le résultat.

2.5.3 Indicatrice d'Euler, Mines 2024

Énoncé

Montrer que pour $n \geq 1$, on a $\varphi(n) \geq \frac{n \ln 2}{\ln n + \ln 2}$

Indication

Il convient de minorer brutalement $\varphi(n)$ exprimé à l'aide de la décomposition de n en nombre premier

---

Correction

Soit $n = \prod_{k=1}^{r} p_k^{\alpha_k}$. Alors $\varphi(n) = n \prod_{k=1}^{r} (1 - \frac{1}{p_k}) \geq n \prod_{k=1}^{r} (1 - \frac{1}{k+1}) \geq n \frac{1}{r+1}$.
Or $n \geq p_1 ... p_r \geq 2^r$ donc $r \leq \frac{\ln(n)}{\ln(2)}$.
Finalement $\varphi(n) \geq \frac{n}{r+1} \geq \frac{n}{\ln(n)/\ln(2)+1} \geq \frac{n \ln(2)}{\ln(n)+\ln(2)}$

2.5.4 Intervalle contenant un nombre premier

Énoncé

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un nombre premier entre $n+1$ et $n! - 1$

Indication

On pourra considérer un diviseur premier de $n! - 1$

Correction

Soit p un diviseur premier de $n! - 1$. Alors, si $p \leq n$, $p|n!$ or $p|n! - 1$ donc $p|1$, absurde. Donc $p \geq n + 1$ et $p \leq n! - 1$, c'est ce qu'on voulait montrer

---

2.6 Matrices

2.6.1 ENS PLSR 2024

Énoncé

Soit $A, B \in \mathcal{M}_n(\mathbb{R})$ tels que $A^2 + B^2 = AB$ et $AB - BA \in GL_n(\mathbb{R})$. Montrer que $3|n$

Indication

Lorsqu'on dispose d'expression algébrique, il peut être utile de chercher à les factoriser dans $\mathbb{C}$ (puisqu'il est algébriquement clos) et regarder ensuite comment ça se passe avec nos objets. Ici, il faut factoriser $a^2 + b^2 - ab$. On obtient $(a + jb)(a + j^2 b)$

Correction

On calcul $(A + jB)(A + j^2B) = A^2 + j^2AB + jBA + B^2 = (1 + j^2)AB + jBA = j(BA - AB)$ et donc $\det(A + jB)(A + j^2B) = j^n \det(BA - AB)$ or $\det(A + jB)(A + j^2B) = |\det(A + jB)|^2$ donc j^n est réel, donc $3|n$

2.7 Réduction

2.7.1 Sous groupes de matrice (inspiré par ENS SR 2024)

Énoncé

Caractériser les groupes inclus dans $\mathcal{M}_n(\mathbb{K})$ avec comme loi la loi multiplicative usuelle.

Indication

On pourra considérer les relations multiplicatives que vérifient le neutre d'un tel groupe.

Correction

Soit G un tel groupe et e son élément neutre. On a que $e^2 = e$ donc e est la matrice d'un projecteur. Notons $E = \ker(e - Id)$ et $F = \ker e$.

Quitte à conjuguer, on se ramène donc au cas où $e = \begin{matrix} I_r & 0 \\ 0 & 0_{n-r} \end{matrix}$. Soit $g \in G$. $ge = eg = g$ donc g stabilise E et F et en particulier g est de la forme, après avoir appliqué la même conjugaison que pour e : $\begin{pmatrix} \rho(g) & 0 \\ 0 & 0_{n-r} \end{pmatrix}$. Alors, $\rho : G \longrightarrow GL_r(\mathbb{K})$ est un morphisme injectif de groupe.
Et donc, tout groupe pour la loi multiplicative de $\mathcal{M}_n(\mathbb{K})$ s'identifie à un sous groupe d'un $GL_n(\mathbb{K})$.

2.7.2 Sur les représentations irréductibles d'un groupe abélien, inspiré par X MPI 2024

Énoncé

Soit G un groupe abélien, V un $\mathbb{C}-$espace vectoriel de dimension fini et $\rho : G \longrightarrow GL(V)$ un morphisme de groupe. On suppose que $\{0\}$ et V sont les seuls espaces stables par tous les $\rho(g), g \in G$.
a) Montrer que $\dim V = 1$
b) Posons $G = \mathbb{U}$ et $f : \mathbb{R} \longrightarrow GL(V)$ définie par $f(\theta) = \rho(e^{i\theta})$. On suppose que f est dérivable en 0, déterminer ρ.

Indication

a) Utiliser le fait que $\mathbb{C}$ est algébriquement clos
b) Le fait que l'on travaille avec un morphisme de groupe permet de généraliser la dérivabilité.

Correction

a) Comme G est abélien, tous les $\varphi(g)$ pour $g \in G$ commutent. Or $\varphi(g_0)$ admet un vecteur propre u car V est un $\mathbb{C}-$espace vectoriel. Alors, $Vect(u)$ est un espace stable par tout $\varphi(g), g \in G$, et donc, $Vect(u) = V$. D'où le résultat.
b) Comme V est de dimension 1, on peut prendre $V = \mathbb{C}$ et ainsi, ρ est un morphisme de $\mathbb{U}$ dans $\mathbb{C}^*$.
On a que $(f(h) - 1)/h \longrightarrow_{h\to 0} f'(0)$. Or $\frac{f(x+h)-f(x)}{h} = \frac{\rho(e^{ix+ih})-\rho(e^{ix})}{h} = \frac{\rho(e^{ix})(\rho(e^{ih})-1)}{h}$ car ρ est un morphisme. Ainsi f est dérivable sur $\mathbb{R}$ tout entier, et $f'(x) = f(x)f'(0)$. Donc $f(x) = f(0)e^{f'(0)x} = e^{f'(0)x} = \rho(e^{ix})$
Posons $f'(0) = a + ib$. Alors $e^{2\pi a + 2i\pi b} = 1$ donc $a = 0$ et b est entier. Donc $\rho(z) = z^n$ avec $n \in \mathbb{Z}^*$

2.7.3 Sur les racines de matrices symétriques positives, Mines 2024

Énoncé

Soient $A, B \in \mathcal{S}_n^+(\mathbb{R})$ telles que A^2 et B^2 commutent. Montrer que A et B commutent.

On pourra utiliser qu'une matrice symétrique positive admet une unique racine symétrie positive.

Correction

Comme A^2 et B^2 commutent, il existe $P \in O_n(\mathbb{R})$ tel que :
$D_{A^2} = PA^2P^\top$ et $D_{B^2} = PB^2P^\top$ soient diagonales. Et alors, comme les coefficients de D_{A^2} et D_{B^2} sont positifs, on peut en extraire une racine D_A et D_B à coefficient positif. Et ainsi, $P^\top D_A P = A$ et $P^\top D_B P = B$ par unicité de la racine symétrique positif. Et alors A, B commutent.

---

3 Analyse

3.1 Topologie

Le programme de classe préparatoire se concentre avant tout sur les espaces vectoriels normés. Certaines caractéristiques essentielles comme la complétude ne sont pas abordés. Pour approfondir la topologie de manière générale et de voir divers théorèmes qui peuvent parfois tomber comme exercice, voir [1]

3.1.1 Condition de transitivité d'une rotation sur le tore (Type ENS)

Énoncé

Soit $\mathbb{T}$ l'ensemble des nombres complexes de module 1. Pour $\alpha \in \mathbb{R}$, on pose $T_\alpha : \begin{array}{c} \mathbb{T} \longrightarrow \mathbb{T} \\ z \mapsto e^{2i\pi\alpha}z \end{array}$. Trouver une condition nécessaire et suffisante sur α pour qu'il existe $x \in \mathbb{T}$ tel que $O_\alpha^+(x) = \{T_\alpha^n(x), n \geq 0\}$ soit dense dans $\mathbb{T}$ (ici, la notation puissance réfère à la composition).

On dit alors que T_α est un système dynamique topologique transitif. Pour mieux comprendre, voir [4]

Indication

Il convient de traiter le cas α rationnel, et α irrationnel.
Pour α irrationnel, on pourra montrer pour $N-$itération de la rotation que deux points sont à une distance plus petite que $2\pi/N$.

Correction

Si α est rationnel, alors, il existe $q \in \mathbb{N}^*$ tel que $T_\alpha^q(x) = x$ pour tout $x \in \mathbb{T}$. Donc $O_\alpha^+(x)$ n'est pas dense car fini.
Si α est irrationnel : soit $x \in \mathbb{T}$. Alors pour $n \neq m$ deux entiers, on a $T_\alpha^n(x) \neq T_\alpha^m(x)$. En particulier, pour $N \geq 1$, par le principe des tiroirs, il existe $0 \leq n < m \leq N$ tel que $|T_\alpha^n(x) - T_\alpha^m(x)| \leq \frac{2\pi}{N}$. Ainsi, la rotation $T_\alpha^{m-n} = T_{\alpha^{m-n}}$ est d'angle plus petit que $\frac{2\pi}{N}$, ce qui permet d'approcher tout point comme on le veut.

3.1.2 Un autre exemple de densité dans le cercle unité (Mines 2024)

Énoncé

Soit $f : \mathbb{R}^+ \longrightarrow \mathbb{R}$ une fonction de classe $\mathcal{C}^1$ telle que $f(x) \longrightarrow +\infty$ et $f'(x) \longrightarrow 0$ quand $x \longrightarrow +\infty$. Montrer que $\{e^{if(n)}, n \in \mathbb{N}\}$ est dense dans le cercle unité

Indication

Il faut utiliser l'hypothèse sur la dérivé pour contrôler les "pas" que l'on fait sur le cercle.

Correction

Soit $N \geq 1$. Il existe A tel que, pour $x \geq A$, $|f'(x)| \leq \frac{2\pi}{N}$. Alors, pour $n \geq A$, $|f(n+l) - f(n+k)| \leq \frac{2\pi|k-l|}{N}$ par inégalité des accroissements finis. Alors, soit z sur le cercle unité. Il existe alors k tel que $|z - e^{if(n+k)}| \leq \frac{2\pi}{N}$, ce qui montre la densité.

3.1.3 Sur la connexité (X-MPI-2024)

Énoncé

Soit E un espace vectoriel normé. Soit U, V deux ouverts disjoints tels que $U \cap V = \emptyset$ et $U \cup V = E$. Que dire de U et V ?

Indication

On va montrer que $U = E$ (ou $V = E$). Pour ça, on va utiliser la connexité par arc de E.
Faire un dessin !

Correction

Supposons par l'absurde U, V non vides. Remarquons tout d'abord que U, V

sont également fermés. Soit alors $u \in U$ et $v \in V$ et $\gamma(t) = tu + (1-t)v$. Alors $\gamma : [0,1] \longrightarrow E$ est continue.
Soit $\tau = \inf\{t \in [0,1], \gamma(t) \in V\}$ (on vérifie aisément l'existence de τ). Tout d'abord, comme U est ouvert, on peut se donner une petite boule ouverte autour de u incluse dans U et il existe alors $t' > 0$ tel que $\gamma(t) \in U$ pour $t < t'$. Cela garantit que $\tau > 0$. On va regarder ce qui se passe en τ. Pour $t < \tau$, $\gamma(t) \in U$ et comme U est fermé, $\gamma(\tau) \in U$. Or si $\gamma(\tau) \in U$, on peut trouver une petite boule autour de $\gamma(\tau)$ qui est dans U. Et alors, il existe $\tau' > \tau$ tel que $\gamma(t) \in U$ pour $t < \tau'$. Absurde.
Dans un espace topologique quelconque, cette propriété s'appelle la connexité. Tout espace métrique n'est pas forcément connexe. Si l'on prend X un ensemble et qu'on l'on pose la distance $d(x,y) = 1$ si $x \neq y$ et $d(x,y) = 0$ sinon la distance discrète, X n'est pas connexe (toute partie de X est un ouvert).

3.1.4 Partition du plan à l'aide de cercle (ENS 2019)

Énoncé
Montrer qu'on ne peut pas partitionner le plan $\mathbb{R}^2$ avec des cercles de rayon non nul

---

Indication
Faire un dessin ! On considère un cercle, puis le cercle passant par le centre du cercle précédent, etc

---

Correction
Pour $x \in \mathbb{R}^2, r > 0$, notons $S(x,r)$ le cercle de centre x et de rayon r.
Supposons par l'absurde qu'une telle partition existe et soit alors $x_0 \in \mathbb{R}^2$ et $r_0 > 0$ tel que $S(x_0, r_0)$ soit dans la partition. Alors, par hypothèse, il existe un unique x_1 et r_1 tel que $x_0 \in S(x_1, r_1)$. Or les deux cercles considérés ne s'intersectent pas, donc $r_1 < \frac{r_0}{2}$. En effet, x_0 et x_1 sont à distance r_1 et l'autre extrémité du diamètre passant par x_0 doit être toujours comprise dans le cercle initial (sinon, les deux cercles se couperaient, ce qui contredirait l'hypothèse). Ainsi, $2r_1 < r_0$. On peut alors recommencer en appliquant le même raisonnement à x_1 pour obtenir x_2 etc.
On a alors construit une suite (x_n) de $\mathbb{R}^2$ et une suite (r_n) telle que $r_0 > 0$ et $r_n \leq \frac{r_0}{2^n}$. Alors, en appliquant le théorème des compacts emboîtés, on obtient que l'intersection des $B(x_n, r_n)$ est non vide, et contient en particulier un point x. Or, un cercle de rayon non nul doit passer par ce point, ce qui est absurde car un tel cercle s'intersecterait avec un $S(x_n, r_n)$ pour n assez grand.

3.1.5 Condition nécessaire et suffisante pour être une boule (inspiré de ENS PLSR 2024)

Énoncé

Soit $B \subset \mathbb{R}^n$. Donner des conditions nécessaires et suffisantes pour que B soit la boule unité fermé associé à une norme.

Indication

Il convient de regarder tout d'abord la liste des propriétés d'une boule unité fermé, puis faire un dessin pour construire la norme associé.

Correction

Une boule unité est symétrique, convexe, 0 est intérieur, et comme on est en dimension finie, est compacte (la compacité ne dépend pas du choix de la norme comme elles sont toutes équivalentes). On va montrer que c'est suffisant.

Supposons donc que B est symétrique, compact et que 0 est intérieur.

On pose $N(0) = 0$. Soit $x \in \mathbb{R}^n$, $x \neq 0$. Alors il existe $\lambda > 0$ tel que $\lambda x \in B$. Soit alors $N(x) = \frac{1}{\sup\{\lambda>0, \lambda x \in B\}}$. Cette quantité est bien définie car B est bornée, et comme B est compact, pour $x \neq 0, N(x) \neq 0$ et $\frac{x}{N(x)} \in B$. On va maintenant montrer que N est une norme. On a bien la positivité et le caractère défini.

Soit $\lambda \in \mathbb{R}^*, x \in \mathbb{R}^n, x \neq 0$. On a que $N(\lambda x) = N(|\lambda| x)$ par symétrie de B, et $N(|\lambda| x) = \frac{1}{\sup\{\mu>0 / \mu|\lambda| x \in B\}} = \frac{|\lambda|}{\sup\{\mu>0 / \mu x \in B\}} = |\lambda| N(x)$. On a bien l'homogénéité.

Soient $x, y \in \mathbb{R}^n, x \neq 0, y \neq 0$, alors $\frac{x}{N(x)}, \frac{y}{N(y)} \in B$ et donc $\frac{N(x)}{N(x)+N(y)} \frac{x}{N(x)} + \frac{N(y)}{N(x)+N(y)} \frac{y}{N(y)} = \frac{x+y}{N(x)+N(y)} \in B$. Et donc $\frac{N(x+y)}{N(x)+N(y)} \leq 1$. Et donc, on a également l'inégalité triangulaire

---

3.1.6 Une norme bien choisie sur les polynômes (Mines 2024)

Énoncé

Soit $Q \in \mathbb{R}[X]$. Construire une norme N sur $\mathbb{R}[X]$ telle que $N(X^n - Q) \longrightarrow_{n\to+\infty} 0$

Indication

On pourra chercher à construire un produit scalaire adapté aux $X^n - Q$

Correction

On a que $((n+1)(X^n - Q))_{n\geq 0}$ forme une base de $\mathbb{R}[X]$. On va alors définir une produit scalaire sur $\mathbb{R}[X]$ telle que cette base soit une base orthonormée. On pose $b((n+1)(X^n - Q), (k+1)(X^k - Q)) = \delta_{n,k}$ et on prolonge par bilinéarité. Alors, b est bien un produit scalaire, et pour la norme associé on a le résultat voulu.

3.2 Suites et séries

3.2.1 Convergence d'une série, Mines 2024

Énoncé

Nature de $\sum_{n\geq 0} \sin(\pi e n!)$

Indication

On pourra utiliser l'écriture de e en série

Correction

On a que $\sin(\pi e n!) = \sin(\pi n! \sum_{k=0}^{+\infty} \frac{1}{k!}) = \sin((n+1)\pi + \pi \sum_{k=n+1}^{+\infty} \frac{1}{k}) = \frac{(-1)^{n+1}\pi}{n+1} + O\left(\frac{1}{n^2}\right)$ d'où la convergence de la série.

3.2.2 Convergence d'une série II, Mines 2024

Énoncé

Soit (u_n) une suite réelle telle que $\sum n \ln(n)^2 u_n^2$ converge. Montrer que $\sum u_n$ converge.

Indication

On pourra appliquer l'inégalité de Cauchy-Schwarz

Correction

Soit $N \geq 2$ un entier. On a, en utilisant Cauchy-Schwarz, que $\sum_{n=2}^{N} |u_n| = \sum_{n=2}^{N} \sqrt{n} \ln(n) |u_n| \frac{1}{\sqrt{n}\ln(n)} \leq \sqrt{\sum_{n=2}^{N} n \ln(n)^2 u_n^2} \sqrt{\sum_{n=2}^{N} \frac{1}{n \ln^2(n)}}$ or on reconnait dans la première racine une somme partielle de série convergente (par hypothèse), et à droite une série de Bertrand convergente (on peut faire une comparaison série intégrale pour vérifier la convergence). Donc $\sum u_n$ converge absolument

---

3.2.3 Somme d'une série (Mines 2024)

Énoncé

Soit $x \in \mathbb{R}\backslash(-\mathbb{N})$. Montrer que $\sum_{n=0}^{+\infty} \frac{1}{x(x+1)...(x+n)} = e\sum_{n=0}^{+\infty} \frac{(-1)^n}{n!(x+n)}$

Correction

On vérifie aisément que les deux sommes en jeux convergent.
On va réaliser la décomposition en élément simple de $\frac{1}{X(X+1)...(X+n)}$.
On a : $\frac{1}{X(X+1)...(X+n)} = \sum_{k=0}^{n} \frac{a_k}{X+k}$ et, en multipliant par $X+k$ et en évaluant en $-k$, on a que : $a_k = \frac{1}{-k(-k+1)(-k+2)...(-1)(1)...(n-k)} = \frac{(-1)^k}{k!(n-k)!}$.
Ainsi : $\sum_{n=0}^{+\infty} \frac{1}{x(x+1)...(x+n)} = \sum_{n=0}^{+\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!(n-k)!(x-k)}$.
On reconnait ici un produit de Cauchy, et alors :
$\sum_{n=0}^{+\infty} \frac{1}{x(x+1)...(x+n)} = \sum_{n=0}^{+\infty} \frac{1}{n!} \sum_{n=0}^{+\infty} \frac{(-1)^n}{n!(x+n)} = e\sum_{n=0}^{+\infty} \frac{(-1)^n}{n!(x+n)}$

3.3 Suites et séries de fonctions

3.3.1 Études de régularité, Mines 2024

Énoncé

Soit $f : x \mapsto \sum_{n=0}^{+\infty} \frac{\sin(2^n x)}{2^n}$.
a) Montrer que f est définie sur $\mathbb{R}$. Montrer qu'elle y est continue.
b) Montrer que f n'est pas dérivable en 0.

Indications

a) Il faut s'intéresser à la convergence normale de la série de fonction.
b) On pourra utiliser la concavité de la fonction sin sur $[0, \pi/2]$

Correction

a) On a que, pour tout $x \in \mathbb{R}$, $|\frac{\sin(2^n x)}{2^n}| \leq \frac{1}{2^n}$. Ainsi, la série converge absolument en tout x donc f est bien définie. La majoration précédente montrer que la convergence est normale, or $f_n : x \mapsto \frac{\sin(2^n x)}{2^n}$ est continue, donc f est bien continue sur $\mathbb{R}$.
b) On considère le taux d'accroissement de f en 0. On a que, pour $x \neq 0$: $\frac{f(x)}{x} = \sum_{n=0}^{+\infty} \frac{\sin(2^n x)}{2^n x}$. Or, pour $t \in [0, \pi/2], \sin(t) \geq \frac{2}{\pi}t$ (c'est la corde qui va de $(0,0)$ à $(\pi/2, \sin(\pi/2))$). Et donc :
$\sum_{n=0}^{+\infty} \frac{\sin(2^n x)}{2^n x} = \sum_{n=0}^{N} \frac{\sin(2^n x)}{2^n x} + \sum_{n=N+1}^{+\infty} \frac{\sin(2^n x)}{2^n x}$ avec N choisi de telle sorte que pour $n \leq N$, $2^n x \in [0, \pi/2]$. Alors $f(x)/x \geq \frac{2}{\pi}(N+1) + \sum_{n=N+1}^{+\infty} \frac{\sin(2^n x)}{2^n x} \geq \frac{2}{\pi}(N+1) - \sum_{n=N+1}^{+\infty} \frac{1}{2^n x} = \frac{2}{\pi}(N+1) - \frac{1}{2^N x} \geq \frac{2}{\pi}(N+1) - \frac{4}{\pi}$. Or quand $x \to 0$, $N \to +\infty$, ce qui permet de conclure.

3.4 Séries entières

3.4.1 Le principe du maximum (Mines +)

Énoncé

Soit $f(z) = \sum_{n=0}^{+\infty} a_n z^n$ une fonction analytique définie sur $\Omega = B(0, R)$. On suppose f non constante, montrer que $|f|$ n'admet pas de maximum sur Ω.
C'est ce qu'on appelle le principe du maximum

Indication

Travailler par l'absurde et regarder ce qui se passe au voisinage du maximum

Correction

Supposons par l'absurde que $|f|$ admette un maximum sur Ω en z_0. Quitte à considérer $z \mapsto f(z-z_0)$, on peut considérer que ce maximum est atteint en z_0 et comme f est non constante, elle est non nulle, donc on peut, quitte à multiplier par un rationnel supposer que $f(0) = 1$. Alors $f(z) = 1 + a_r z^r + o(z^r)$ au voisinage de 0 et r est le plus petit entier strictement positif tel que $a_r \neq 0$. Alors, en écrivant $a_r = \rho_r e^{i\theta_r}$ et $z = \rho e^{i\theta}$, on a que $f(z) = 1 + \rho_r \rho^r e^{i(\theta_r + r\theta)} + o(z^r)$. Et alors, en prenant $\theta = -\theta_r/r$ et ρ assez petit, on a $|f(z)| > 1$. Absurde.

3.4.2 ENS U 2024 grâce à X 2024

Énoncé

a) Montrer que pour tous $r \in]0,1[$ et $\theta \in \mathbb{R}$, $\ln|1 - re^{i\theta}| = -\sum_{n=1}^{+\infty} \frac{r^n}{n} \cos(n\theta)$ (X 2024)
b) Soient $P \in \mathbb{C}[X]$ non constant tel que $P(0) \neq 0$ et $r \in \mathbb{R}_+^*, z_1, ..., z_p$ les racines de module strictement inférieur à r de P comptées avec multiplicité. Montrer que $\frac{1}{2\pi} \int_{-\pi}^{\pi} \ln|P(re^{it})|dt = \ln(|P(0)) + \sum_{k=1}^{p} \ln\left(\frac{r}{|z_k|}\right)$ (ENS U 2024)

Indication

On pourra dériver la fonction de telle sorte à se ramener à exprimer une fraction rationnelle sous forme de série entière.

Correction

a) Tout d'abord le logarithme est bien défini.De même pour la série. De plus, le résultat est évident si $\theta \in \pi\mathbb{Z}$, on suppose donc que ce n'est pas le cas.

On a que : $f(r) = 2\ln(|1 - re^{i\theta}|) = \ln(1 - 2r\cos\theta + r^2)$.
Puis, $f'(r) = \frac{2r-2\cos\theta}{1-2r\cos\theta+r^2} = \frac{2r-2\cos\theta}{(r-\cos\theta-i\sin\theta)(r-\cos\theta+\ \sin\theta)} = \frac{2r-2\cos\theta}{(r-e^{i\theta})(r-e^{-i\theta})} = \frac{1}{r-e^{i\theta}}\frac{1}{r-e^{-i\theta}} = -e^{-i\theta}\frac{1}{1-re^{-i\theta}} - e^{i\theta}\frac{1}{1-re^{i\theta}}$.
On peut alors développer l'expression en série entière, puis en intégrant, on trouve exactement le résultat voulu.
b) On a ensuite que $P = \frac{P(0)}{\prod_{k=1}^{n} -z_k}\prod_{k=1}^{n}(X - z_k)$ avec $z_{p+1}, ..., z_n$ les racines de P de module plus grand que r. Alors :
$\ln|P(re^{it})| = \ln|P(0)| + \sum_{k=1}^{n}\ln\left|\frac{re^{it}-z_k}{|z_k|}\right|$.
On est donc réduit à traiter le problème des polynômes de la forme $X - z = X - \rho e^{i\theta}$.
Si $|z| < r$, alors $\ln|re^{it} - z| = \ln|r| + \ln|1 - ze^{-it}| = \ln|r| + \ln|1 - \rho e^{i(\theta-t)}|$ et alors, on peut intégrer la série entière de la question a), et on obtient $\ln r$.
Si $|z| \geq r$, alors : $\ln|re^{it} - z| = \ln|z| + \ln|1 - \frac{r}{z}e^{it}|$ et on obtient en intégrant $\ln|z|$.
En combinant ces deux résultats, on obtient le résultat souhaité.

3.5 Calcul différentiel

3.5.1 Une équation harmonique (Mines 2024)

Énoncé

Soient $f \in \mathcal{C}^2(\mathbb{R}_+^*, \mathbb{R})$ et g définie sur $(\mathbb{R}^{+*})^2$ définie par $g(x, y) = f\left(\frac{x^2+y^2}{2}\right)$.
Déterminer les fonctions f qui vérifient $\Delta g = \frac{\partial^2 g}{\partial x^2} + \frac{\partial^2 g}{\partial y^2} = 0$

Indication

Il convient de raisonner par analyse synthèse, et de calculer.

Correction

Soit f solution. On a alors que $\Delta g = \frac{\partial}{\partial x}(xf'(\frac{x^2+y^2}{2})) + \frac{\partial}{\partial y}(yf'(\frac{x^2+y^2}{2})) = 2f'(\frac{x^2+y^2}{2}) + (x^2 + y^2)f''(\frac{x^2+y^2}{2})$. Posons $t = \frac{x^2+y^2}{2}$. On a alors que f est solution de l'équation différentielle $f'(t) + tf''(t) = 0$. Alors $f'(t) = -\frac{A}{t}$ et donc $f(t) = -A\ln(t) + B$.
On vérifie réciproquement que ces fonctions sont bien solutions.

3.5.2 Espace tangent aux projecteurs

Énoncé

Soient $n \in \mathbb{N}^*$ et $r \in [|0, p|]$. On note $\mathcal{P}$ l'ensemble des projecteurs orthogonaux de $\mathbb{R}^n$ sur un sous espace de dimension r et $p \in \mathcal{P}$. Déterminer l'espace tangent en p à $\mathcal{P}$

Correction

On travaille dans $\mathcal{L}(\mathbb{R}^n)$ muni de la norme d'opérateur.
Soit $f :]-\eta, \eta[\longrightarrow \mathcal{P}$, $\mathcal{C}^1$ tel que $f(0) = p$. On a que, pour tout $t \in]-\eta, \eta[$, $f(t)^2 = f(t)$.
En dérivant cette expression, on a que $f'(t)f(t) + f(t)f'(t) = f'(t)$ donc en prenant en 0 : $f'(0)p + pf'(0) = f'(0)$. Si $x \in \ker p$, alors $p(f'(0)(x)) = f'(0)(x)$ donc $f'(0)(x) \in Im(p)$. Si $x \in Imp$, alors $f'(0)(x) + p(f'(0)(x)) = f'(0)(x)$ donc $p(f'(0)(x)) = 0$ donc $f'(0)(x) \in \ker p$. On en déduit donc que tout vecteur tangent à $\mathcal{P}$ en p échange les espaces propres de p.
Soit maintenant v qui échange les espaces propres de p.
Soit $f(t) = e^{-vt}pe^{vt}$, $f'(t) = -ve^{-vt}pe^{vt} + e^{-vt}pve^{vt} = e^{-vt}(pv - vp)e^{vt}$. On a alors que $f(0) = p$ et que $f'(0) = v$. De plus : $f^2(t) = e^{-vt}p^2e^{vt} = f(t)$ donc l'image est bien un projecteur, de rang plus petit que r. Il reste alors à vérifier qu'il est orthogonal, et donc que $e^{vt^*} = e^{-vt}$. Cela vient du fait que, comme p est orthogonal, $Im(p) \oplus^{\perp} \ker p = \mathbb{R}^n$

---

4 Probabilités

4.1 Calcul de loi

4.1.1 Loi de Poisson modulo p, Mines 2024

Énoncé

Soit X qui suit une loi de Poisson de paramètre $\lambda > 0$. Soit alors $p \in \mathbb{N}^*$ et $Y = \pi(X)$ où π est la projection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/p\mathbb{Z}$. Déterminer la loi de Y.

Correction

Soit $n \in [|0, p-1|]$. On va déterminer $\mathbb{P}(Y = \overline{n})$. Or :
$\mathbb{P}(Y = \overline{n}) = \mathbb{P}(\cup_{k=0}^{+\infty} X = kp + n) = \sum_{k=0}^{+\infty} \frac{\lambda^{kp+n}}{(kp+n)!} e^{-\lambda}$
On a que $\frac{1}{p} \sum_{l=0}^{p-1} e^{2i\pi(k-n)l/p}$ vaut 1 si et seulement si $k = n[p]$ et 0 sinon.
Donc, $\mathbb{P}(Y = \overline{n}) = \sum_{k=0}^{+\infty} \sum_{l=0}^{p-1} \frac{\lambda^k}{k!} e^{-\lambda} e^{2i\pi(k-n)/p}/p$.
$= \frac{1}{p} \sum_{l=0}^{p-1} \sum_{k=0}^{+\infty} e^{-\lambda} \frac{(\lambda e^{2il\pi/p})^k}{k!} e^{-2i\pi nl/p} = \frac{1}{p} \sum_{l=0}^{p-1} e^{\lambda(e^{2i\pi l/p}-1)-2i\pi ln/p}$

4.1.2 Probabilité d'être diagonalisable

Énoncé

Soient A, B, C, D quatre variables aléatoires, indépendantes suivant toutes une loi de Poisson de paramètre $\lambda > 0$.

Quelle est la probabilité que $M = \begin{pmatrix} A & C \\ B & D \end{pmatrix}$ soit $\mathbb{R} - diagonalisable$?

Indication

On pourra, à l'aide du polynôme caractéristique, dresser l'inventaire des cas où M n'est pas diagonalisable.

Correction

Pour que M soit diagonalisable, il est nécessaire et suffisant que son polynôme minimal soit scindé à racine simple. On va tout d'abord calculer le polynôme caractéristique de M.

$\chi_M = X^2 - (A + D)X + (AD - BC)$. On va ensuite regarder ses racines. En effet, ou bien M a deux valeurs propres distinctes, et est donc diagonalisable, ou bien M n'a qu'une unique valeur propre et alors M est diagonalisable si et seulement si elle est diagonale, enfin, si M n'a pas de valeur propre elle n'est pas diagonalisable.

Ceci étant dit, regardons le discriminant du polynôme caractéristique : $(A + D)^2 - 4(AD - BC) = A^2 + 2AD + D^2 - 4AD + 4BC = (A - D)^2 + 4BC$. Or les variables aléatoires B, C sont à valeurs positives, ainsi, le discriminant est toujours positif. Et M est n'est pas diagonalisable si et seulement si $A = D$ et $B = 0, C \neq 0$ ou $B \neq 0, C = 0$.

Notons p la probabilité recherché, on a que $1 - p = \mathbb{P}(A = D \cap (B = 0 \cap C \neq 0 \cup B \neq 0 \cap C = 0)) = (\sum_{n=0}^{+\infty} \mathbb{P}(A = n)\mathbb{P}(D = n)) \times 2\mathbb{P}(B = 0) \times (1 - \mathbb{P}(C = 0)) = 2e^{-3\lambda}(1 - e^{-\lambda}) \sum_{n=0}^{+\infty} \frac{\lambda^{2n}}{n!^2}$ et donc $p = 1 - 2e^{-3\lambda}(1 - e^{-\lambda}) \sum_{n=0}^{+\infty} \frac{\lambda^{2n}}{n!^2}$

4.2 Calcul d'espérance

4.2.1 Loi de Poisson, Mines 2024

Énoncé

Soit X une variable aléatoire suivant la loi de Poisson de paramètre λ. Calculer $\mathbb{E}\left(\frac{1}{X+1}\right)$ et $\mathbb{E}\left(\frac{1}{(X+1)(X+2)}\right)$

Indication

Il convient d'appliquer le théorème de transfert

Correction On commence par $\frac{1}{X+1}$. D'après le théorème de transfert : $\mathbb{E}(\frac{1}{X+1}) = \sum_{n=0}^{+\infty} \frac{1}{n+1} \times \frac{\lambda^n}{n!} e^{-\lambda} = \frac{e^{-\lambda}}{\lambda} \sum_{n=0}^{+\infty} \frac{\lambda^{n+1}}{(n+1)!} = \frac{e^{-\lambda}}{\lambda}(e^{\lambda} - 1)$.
On a ensuite, de même : $\mathbb{E}(\frac{1}{(X+1)(X+2)}) = \frac{e^{-\lambda}}{\lambda^2}(\sum_{n=0}^{+\infty} \frac{\lambda^{n+2}}{(n+2)!}) = \frac{e^{-\lambda}}{\lambda^2}(e^{\lambda} - 1 - \lambda)$.

4.2.2 Inégalité de Jensen

Énoncé
Soit $\varphi : \mathbb{R} \longrightarrow \mathbb{R}$ convexe, et X une variable aléatoire à valeur réelle ayant un moment d'ordre 1.
Montrer que $\varphi(\mathbb{E}(\mathbb{X})) \leq \mathbb{E}(\varphi(X))$.

Indication
Comme φ est convexe, si on pose $E = \{(a,b) \in \mathbb{R}^2 / \forall x \in \mathbb{R}, ax + b \leq \varphi(x)\}$, on a que $\varphi(x) = \sup_{(a,b) \in E} ax + b$

Correction
On va suivre l'indication : $\mathbb{E}(\varphi(X)) = \mathbb{E}(\sup_{a,b \in E} aX + b) \geq \sup_{a,b \in E} \mathbb{E}(aX + b) \geq \varphi(\mathbb{E}(X))$ par croissance et linéarité de l'espérance.

4.2.3 Différence symétrique, ENS PLSR 2024 (abordable)

Énoncé
Soit $E = [|1,n|]$ et $p \in]0,1[$. Soit X une variable aléatoire à valeur dans $\mathcal{P}(E)$ telle que pour tout $i \in E$, $P(i \in X) = p$ et pour $i \neq j$, $i \in X$ et $j \in X$ sont indépendants. Soit Y de même loi que X, X et Y indépendant. Calculer $\mathbb{E}(|X \Delta Y|)$.

Indication
Il convient de poser les variables aléatoires X_i, Y_i qui valent 1 si $i \in X$ (resp. $i \in Y$) et 0 sinon.

Correction
Posons $X_1, ..., X_n, Y_1, ..., Y_n$ comme dans l'indication. On a alors que $|X \Delta Y| = \sum_{i=1}^{n} (X_i + Y_i - 2X_iY_i)$ et alors, par linéarité de l'espérance, et par indépendance des X_i, Y_i : $\mathbb{E}(|X \Delta Y|) = \sum_{i=1}^{n} p + p - 2p^2 = 2np(1-p)$

4.3 Probabilité asymptotique

4.3.1 ENS U 2024 (la moitié, difficile)

Énoncé

Soit G un groupe fini de cardinal N et A une partie de G aléatoire où l'on prend chaque élément de G indépendamment avec probabilité $p > 0$. On note $AA = \{xy, (x, y) \in A^2\}$.
Montrer que $\mathbb{P}(1 \in AA) \longrightarrow_{N \to +\infty} 1$

Indication

Considérer la probabilité du complémentaire. Partitionner G convenablement à l'aide des inverses.

Correction

On va plutôt regarder $\mathbb{P}(1 \notin AA)$.
Si $1 \notin AA$, alors A ne contient aucun élément d'ordre ≤ 2, et A si $x \in A$, $x^{-1} \notin A$.
On va écrire $G = \cup_{x \in R}\{x, x^{-1}\} \cup \cup_{x' \in R'}\{x'\}$ où on a regroupé les éléments par couples d'inverses et où R' est l'ensemble des éléments d'ordres plus petit que 2.
On a alors, que $\mathbb{P}(1 \notin AA) = \mathbb{P}(\cap_{x \in R}\overline{x \in A \cap x^{-1} \in A} \cap \cap_{x' \in R'} x' \notin A) = \prod_{x \in R}(1 - \mathbb{P}(x \in A \cap x^{-1} \in A)) \prod_{x' \in R'}(1 - \mathbb{P}(x' \in A))$ par indépendance.
Finalement, on a que $\mathbb{P}(1 \notin AA) \leq (1-p^2)^{Card(R)}(1-p)^{Card(R')} \leq (1-p^2)^{Card(R)+Card(R')}$ or $N = 2Card(R) + Card(R')$ donc, en passant à la limite, on obtient que $\mathbb{P}(1 \notin AA) \longrightarrow 0$ ce qui est le résultat voulu.

4.3.2 Probabilité d'une racine pour un polynôme aléatoire (inspiré par X 2022)

Énoncé

Soient $a_1, ..., a_{2n}$ des variables aléatoires de Bernoulli de paramètre $1/2$ indépendantes.
On pose $P = X^{2n+1} + \sum_{k=1}^{2n} a_k X^k + 1$. Déterminer un équivalent en $+\infty$ de p_n la probabilité que -1 soit une racine de P.

Indication

C'est un problème de dénombrement. On pourra de plus appliquer la formule de Vandermonde : $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Correction

On découpe les coefficients (a_k) de P en deux catégories : ceux d'indice pair, et ceux d'indice impair.
Pour que -1 soit racine, il est nécessaire et suffisant qu'il y ait le même nombre de coefficient pair que de coefficient impair qui valent 1.
On peut procéder par dénombrement : on a un total de 2^{2n} configuration possible pour p. De plus, pour k fixé, il y a $\binom{k}{n}^2$ configuration où k coefficient pairs valent 1 et k coefficients impairs valent 1. Alors, $p_n = \frac{\sum_{k=0}^{n}\binom{n}{k}^2}{2^{2n}} = \frac{\binom{2n}{n}}{2^{2n}} = \frac{\frac{(2n)!}{(n)!^2}}{2^{2n}} \sim \frac{(2n/e)^{2n}\sqrt{4\pi n}}{2^{2n}(n/e)^{2n}\times 2\pi n} \sim \frac{1}{\sqrt{\pi n}}$

4.3.3 Intervertir espérance et série

Énoncé

Soit (X_n) une suite de variable de Bernoulli de paramètre $p \in]0,1[$.
Déterminer l'espérance de $S = \sum_{k=0}^{+\infty} X_k p^k$.

Indication

Le résultat est intuitif. Il convient de montrer que c'est effectivement le résultat qu'on obtient.

Correction

Cela découle immédiatement du théorème de convergence monotone ! Cependant, il n'est pas au programme de classe préparatoire
On a que : $|\mathbb{E}(S) - \mathbb{E}(\sum_{k=0}^{n} X_k p^k)| = |\mathbb{E}(\sum_{k=n+1}^{+\infty} X_k p^k)| \leq \frac{p^{n+1}}{1-p}$ par linéarité puis croissance de l'espérance.
Ainsi, en passant à la limite, on a que $\mathbb{E}(S) = \frac{p}{1-p}$

4.4 Fonction génératrice

4.4.1 Mines 2024

Énoncé

a) Montrer qu'il existe une variable aléatoire telle que $\forall t \in [0,1], G_X(t) = \frac{e^{t-1}}{\sqrt{2-t}}$
b) Calculer $\mathbb{E}(X)$ et $V(X)$

Indication

C'est avant tout du calcul.

Correction
a) On voit tout d'abord que $G_X(1) = 1$. Il reste juste à montrer que l'on peut développer G_X en série entière et que ses termes sont tous positifs.
On a que $\frac{e^{t-1}}{\sqrt{2-t}} = \frac{1}{e\sqrt{2}}(\sum_{k=0}^{+\infty} \frac{t^k}{k!})(1 - \frac{t}{2})^{-1/2}$. Or la deuxième expression est développable en série entière, et l'on voit bien, en dérivant et en prenant en 0 que les termes sont positifs. Ainsi, tous les termes sont bien positif, et donc on peut bien définir une variable aléatoire de fonction génératrice G_X.
b) On a que $\mathbb{E}(X) = G'_X(1)$ et $V(X) = G''_X(1) + \mathbb{E}(X) - \mathbb{E}(X)^2$.
Or $G'_X(t) = \frac{e^{t-1}(\sqrt{2-t}+\frac{1}{2\sqrt{2-t}})}{2-t} = \frac{e^{t-1}}{\sqrt{2-t}} + \frac{e^{t-1}}{2(2-t)^{3/2}}$ et donc $G''_X(t) = \frac{e^{t-1}}{\sqrt{2-t}} + \frac{e^{t-1}}{2(2-t)^{3/2}} + \frac{e^{t-1}((2-t)^{3/2}+\frac{3}{2}\sqrt{2-t})}{2(2-t)^3}$.
On en déduit que $\mathbb{E}(X) = 1 + \frac{1}{2} = \frac{3}{2}$ et $V(X) = \frac{3}{2} + \frac{5}{4} + \frac{3}{2} - \frac{9}{4} = \frac{12+5-9}{4} = 2$

Références

[1] Djalil Chafaï. Topologie et calcul différentiel. https ://djalil.chafai.net/docs/L3/cours-tcd.pdf.

[2] Gaëtan Chenevier. Algèbre i. http ://gaetan.chenevier.perso.math.cnrs.fr/AlgebreI.html.

[3] Jean-François Dat. Algèbre ii : Anneaux, modules, théorie de galois. https ://www.math.ens.psl.eu/shared-files/9518/ ?ENS1718.pdf.

[4] Cyril Houdayer. Dynamical system. https ://cyrilhoudayer.com/wp-content/uploads/2025/09/dynamical-systems-ens-2023-2026-2.pdf.

[5] Daniel Perrin. *Géométrie Algébrique : Une introduction*. Savoirs actuels : EDP Sciences/CNRS Editions, 2001.