Recueil d'exercices mathématiques pour la MPSI

Dan MELLER

2020-2022

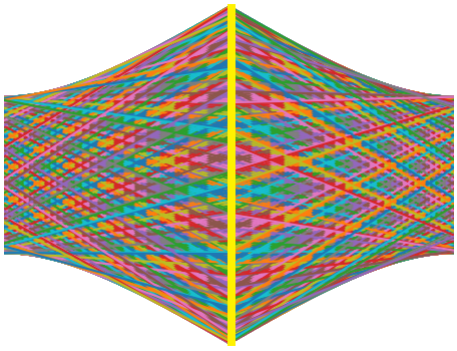

Table des matières

Remerciements

Je tiens à remercier les promotions Sigmas (MPSI Ginette) 2021, 2022, et 2023. Ces exercices ont été conçus pour eux et testés par leur soins. Merci également à Frédéric Morlot, leur professeur de mathématiques, de m'avoir laissé une liberté totale dans le choix des exercices.

1 Introduction

Ces exercices ont été choisis ou conçus pour découvrir le programme sous l'angle de problèmes assez variés, voire parfois exotiques. Les techniques utilisées dans les résolutions sont cependant relativement universelles et permettent d'appliquer des notions de cours importantes, souvent à la croisée de plusieurs chapitres. Certains exercices permettent également d'aborder des éléments importants de culture mathématique avec les outils du programme.

Les exercices marqués par Δ sont considérés comme classiques. Des éléments de correction sont systématiquement donnés quand la technique de résolution ne découle pas simplement de l'énoncé de la question.

Si vous remarquez une erreur dans les énoncés, une faute d'orthographe ou bien encore un problème de mise en page en Latex, n'hésitez pas à m'en faire part à l'adresse : *dan.meller@polytechnique.edu*

2 Nombres complexes

2.1 Δ Somme de racines de l'unité

Soit $n \in \mathbb{N}^*$. On note les racines de l'unité : $\omega_j := e^{2\pi ij/n}$ pour $j \in [|1, n|]$.

1. Pour $p \in \mathbb{N}$, que vaut $S_p := \sum_{j=1}^{n} \omega_i^p$?
2. En déduire que pour $p, q \in \mathbb{N}$, il existe $c \in \mathbb{N}$ tel que $S_p S_q = S_c$

Éléments de correction : 2. $c = pgcd(p, q)$ par exemple.

2.2 Cône complexe

Soit $\theta_1, \theta_2 \in [-\frac{\pi}{2}, \frac{\pi}{2}]$ tels que $\theta_1 < \theta_2$.
On pose

$$C := \{z \in \mathbb{C} |\ \theta_1 \leq arg(z) \leq \theta_2\}$$

1. Montrer que C est stable par addition

Éléments de correction : Il est commode de se ramener à un cas particulier. Par exemple en réalisant une rotation (multiplication par un complexe bien choisi), on se ramène au cas où $\theta_1 = -\theta_2$. On peut alors réécrire C avec une condition portant sur les parties réels et imaginaires :

$$C = \{z \in \mathbb{C} |\ |\Im(z)| \leq \tan(\theta_2)\Re(z)\}$$

3 Ensembles et applications

3.1 Pseudo-inverse

Soit A et B deux ensembles. On considère deux fonctions $f : A \longrightarrow B$ et $g : B \longrightarrow A$ tels que $f \circ g = Id_B$.

1. A-t-on nécessairement : $g \circ f = Id_A$?
2. Calculer l'itéré n-ième de $g \circ f$ (On remarquera plus tard dans l'année que si f et g sont linéaires alors on a affaire à un projecteur)
3. On suppose qu'il existe h tel que $h \circ f = Id_A$. Montrer que $g \circ f = Id_A$

3.2 Entropie discrète et lemme de Gibbs

On pose :

$$\begin{array}{rccc} H & : & {\mathbb{R}_+^*}^n & \to & \mathbb{R} \\ & & p & \mapsto & -\sum_{i=1}^n p_i \ln(p_i) \end{array}$$

ainsi que $C := \{p \in {\mathbb{R}_+^*}^n |\ \sum_{i=1}^n p_i = 1\}$.

1. Montrer que H est positive
2. Montrer que H n'admet pas de minimum sur C
3. Soit $p \in C$. Pour $t \in \mathbb{R}$, on pose :

$$q_t = \left(p_1 + t, p_2 - \frac{t}{n-1}, ..., p_n - \frac{t}{n-1}\right)$$

   Montrer que pour t dans un voisinage de 0 on a : $q_t \in C$ et $H(q_t)$ bien défini.
4. Montrer que $H(q_t)$ est dérivable en 0 et donner sa dérivée .
5. On suppose que H admet un maximum sur C. Donner une condition nécessaire sur celui-ci.
6. En déduire la seule valeur possible pour le maximum de H.

Remarque et éléments de correction : On montre ici que seule la distribution uniforme peut maximiser l'entropie discrète. Si p représente une loi de probabilité cela correspond à la situation où l'on a le plus d'incertitude sur l'issu d'une expérience aléatoire. Pour aller plus loin : ensemble microcanonique en physique statistique.

3.3 Parité et involution

1. Soit A un ensemble fini et ϕ une involution de A sans point fixe. Montrer que A est de cardinal pair.
2. Soit B un ensemble fini. Soit n un entier tel que $2 \leq n \leq |B|$. Montrer que l'ensemble des injections de $[|1, n|]$ dans B est fini et que son cardinal est pair.

Éléments de correction : 1. On pourra trouver une relation d'équivalence qui permet de partitionner A en ensembles dont le cardinal est pair 2. On peut appliquer ce qui précède en considérant l'action d'une transposition sur une involution. On pourrait aussi calculer directement le cardinal de ces involutions.

4 Groupes, anneaux et corps

4.1 Technologie RAID 5 et RAID 6

On considère l'opération XOR qui est définie sur $\{0,1\}$ par : $1+0=0+1=1$ et $0+0=1+1=0$. On remarquera qu'il s'agit simplement de l'addition dans $\mathbb{Z}/2\mathbb{Z}$ ce qui permet d'obtenir immédiatement l'associativité et la commutativité de cette opération. On étend cette opération "+" sur $B := \{0,1\}^n$ par

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$

1. Soit $X \in B$, que vaut $X + X$?
2. Soit $(Y, Z) \in B^2$, résoudre l'équation $X + Y = Z$ pour $X \in B$
3. On modélise le contenu d'un disque dur par un élément de B (n-uplet de bits). On dispose de $d+1$ disques, dont les d premiers comportent de l'information que l'on souhaite conserver, comment prévenir la perte d'un disque parmi les $d+1$?
4. On souhaite désormais prévenir 2 pertes, on se munit donc de d+2 disques. On note $(D_1, ..., D_d) \in B^d$ l'état des d premiers disques qui contiennent de l'information. On pose :

$$D_{d+1} := \bigoplus_{i=1}^{d} D_i$$

$$D_{d+2} := \bigoplus_{i=1}^{d} T^i(D_i)$$

où T est un opérateur de décalage par un bit :

$$\begin{array}{rccc} T & : & B & \to & B \\ & & (x_1, x_2, ..., x_n) & \mapsto & (x_n, x_1, x_2, ..., x_{n-1}) \end{array}$$

T^i désigne bien entendu l'itéré i-ième de T. Soit $k \in [|1, d|]$. Montrer que si l'on perd les disques $\{d+1, d+2\}$ ou $\{k, d+2\}$ alors on peut reconstituer toute l'information des d premiers disques.

5. Montrer que cela reste valable si l'on perd les disques $\{k, d+1\}$
6. Soit $Y \in B$, Montrer que l'équation $X + T(X) = Y$ admet 0 ou 2 solutions.
7. Soit désormais $j \in [|1, d||]$. On suppose que $d \leq n$ et que l'on perd les disques $\{k, j\}$. Montrer que l'on peut retrouver toute l'information perdue à conjugaison prés (le conjugué de $x \in 0, 1$ est $1 + x$).

Remarque : Le principe du RAID 6 a été ici simplifié pour pouvoir être abordable avec les notions de sup. En réalité on préfère travailler octet par octet pour le couplage entre disques (c'est à dire d=8). La technique précédente ne permettrait donc de travailler au plus qu'avec 8 disques d'informations à cause de la contrainte $d \leq n$ et on a aurait en plus une incertitude parmi deux options en cas de perte de deux des 8 premiers disques. La vrai technique mise en place dans le RAID 6 permet de contourner cette difficulté, en voici les grandes lignes : (celles-ci font appel à des notions qui seront vues plus tard dans l'année, je conseille donc d'y revenir après avoir vu le chapitre sur les polynômes)

On considère les 8-uplets de bits comme des polynômes de degré ≤ 7 à coefficient dans $\mathbb{Z}/2\mathbb{Z}$. L'addition se définit aisément sur ces objets et revient à faire l'opération XOR sur les 8-uplets de bits. On

définit également la multiplication de deux de deux de ces objets P et Q comme le reste de la division polynomiale de P*Q par un polynôme irréductible A de degré 8 (ce qui garantit bien que le résultat soit un polynôme de degré plus petit que 7). Enfin on modifie la définition du dernier disque :

$$D_{n+2} = \sum_{i=1}^{n} X^i D_i$$

On peut ici voir la proximité avec la technique précédente que cette nouvelle méthode corrige :

La multiplication par X s'apparente presque à une translation de bits, seulement le dernier coefficient devant X^7, s'il est non nul, va devenir X^8 et donc être réduit par le polynôme irréductible A ce qui va modifier les coefficients précédents légèrement. Par exemple si l'on considère $A = X^8+X^2+1$:

Le 8-uplet P := (0,0,0,1,0,0,0,1) correspond au polynôme X^7+X^3. On a donc $X*P = reste[X^8+X^4] = X^4 + reste[X^8] = X^4 - X^2 - 1 = X^4 + X^2 + 1 = (1,0,1,0,1,0,0,0)$. On retrouve ici le translaté de P : $(1,0,0,0,1,0,0,0)$ + un terme de correction qui est $(0,0,1,0,0,0,0,0)$

La démonstration du bon fonctionnement de cette méthode est alors essentiellement un exercice (difficile) d'algèbre (les 8-uplets avec + et $*$ définis ainsi forment un corps).

4.2 Rubik's Cube

1. Donner plusieurs diviseurs non triviaux du nombre total de configuration d'un Rubik's cube

Éléments de correction : On pourra s'aider d'un rubik's cube physique et compter la périodicité de certaines opérations.

4.3 Δ Ordre dans un groupe commutatif fini

Soit $(G, *)$ un groupe commutatif fini dont le neutre est noté e.

1. Montrer qu'il existe un élément z d'ordre maximal
2. Soit x et y deux éléments dont les ordres sont premiers entre eux, quel est l'ordre de $x * y$?
3. Montrer que pour tout élément d'ordre d, il existe un élément d'ordre k pour tout diviseur k de d.
4. Montrer que tous les ordres des éléments de G divisent celui de z

Éléments de correction : 2. On note, a l'ordre de x, b l'ordre de y et d l'ordre de xy. On a $(x*y)^{ab} = e$ donc $d|ab$. On veut montrer que $ab|d$ pour conclure par antisymétrie. Comme a et b sont premiers entre eux, il suffit de montrer que $a|d$ (sans perte de généralité). Il suffit même de montrer que $a|db$ (on a relaxé le problème en faisant "passer" b de l'autre côté). Comme a est l'ordre de x, il suffit de montrer que $x^{db} = e$ ce qui est aisé. 3. Si x est d'ordre d, considérer $x^{d/k}$. 4. Raisonner par l'absurde en utilisant les deux questions précédentes.

Remarque : La question 2 est un peu subtile mais très classique, elle intervient dans de nombreuses démonstrations relatives aux groupes commutatifs finis. Elle intervient notamment dans la démonstration du théorème de structure de Kronecker qui stipule que tout groupe commutatif fini est isomorphe à un groupe de la forme : $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ...\mathbb{Z}/n_p\mathbb{Z}$ avec $n_1|n_2|...|n_p$ (suite croissante pour la divisibilité).

5 Arithmétique

5.1 Δ Théorème chinois

Soit $n \in \mathbb{N}^*$, on note $\mathcal{P}$ l'ensemble des nombres premiers

1. Montre que $E = 0[n] \iff \forall p \in \mathcal{P} : E = 0\ [p^{v_p(n)}]$
2. Résoudre : $x^2 + 29 = 0\ [30]$

Remarque : Le théorème chinois est fondamental pour la résolution des équations modulaires ! En effet, le résultat est particulièrement intéressant quand E est une expression algébrique. On pourrait formaliser davantage l'équivalence du premier exo en posant le morphisme chinois qui a tout élément x de $\mathbb{Z}/n\mathbb{Z}$ associe le vecteur composé des classes d'équivalence de x modulo $p^{v_p(n)}$. Ce qui a été démontré plus haut est alors l'injectivité du morphisme chinois (en passant par la caractérisation du noyau). Par égalité de cardinal cela implique alors que celui-ci est bijectif et donc qu'il s'agit bien d'un isomorphisme.

5.2 Δ Indicatrice d'Euler

On définit $\phi(n)$ comme le cardinal de $\{k \in [|1, n|[, pgcd(n, k) = 1\}$. Il s'agit de l'indicatrice d'Euler.

1. Montrer que
$$\sum_{d|n} \phi(d) = n$$
2. Montrer que pour
$$n \in \mathbb{N}^*,\ \phi(n) = n \prod_{p \in \mathcal{P},\ p|n} \left(1 - \frac{1}{p}\right)$$

Remarque : Cette fonction peut sembler un peu curieuse et arbitraire par sa définition en premier lieu. Il est peut-être plus naturel de l'introduire (et de s'en souvenir) en tant que cardinal du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$. La propriété $x^{\phi(n)} = 1\ [n]$ est alors une conséquence directe du petit théorème de Fermat. L'indicatrice d'Euler est un objet au coeur de l'arithmétique qui présente de nombreuses autres propriétés intéressantes. Pour en savoir plus sur l'exercice précédent cf la formule d'inversion de Mobius : `https://fr.wikipedia.org/wiki/Formule_d%27inversion_de_M%C3%B6bius`

En notant $*$ le produit de convolution de Dirichlet, on a montré ici que $Id = \phi * 1$. Il en découle que $\phi = \mu * Id$. Malheureusement μ est quasiment aussi long que ϕ à calculer d'un point de vue algorithmique. Cette formule présente donc surtout un intérêt théorique.

Éléments de correction : 1. La somme invite à trouver une partition de $[|1, n|]$. On peut par exemple penser à $(A_d := \{1 \leq k \leq n|\ k \wedge n = d\})_{d|n}$. On montre alors que le cardinal de A_d vaut $\phi(n/d)$ ce qui conclut la preuve en changeant d'indice. 2. Calculer l'indicatrice d'Euler directement pour les puissances d'un nombre premier puis remarquer que pour $m, n \in \mathbb{N}^*$ tels que $m \wedge n = 1$ on a : $\phi(mn) = \phi(m)\phi(n)$. Utiliser enfin la décomposition en facteurs premiers pour conclure.

5.3 Tests de primalité : Exact, Fermat, Miller-Rabin

1. Donner un algorithme exact pour tester si un nombre est premier
2. Déduire du petit théorème de Fermat un test de primalité. On demande seulement que celui n'engendre aucun faux négatif.
3. Un nombre de Carmichael : montrer que $561 = 3 * 11 * 17$ est un faux positif au test précédent *ie* : $\forall x \in [|1, 560|[,\ x^{560} = 1\ [561]$
4. Soit p un nombre premier, on pose s et d tel que d impair et $p - 1 = 2^s d$. Montrer que :
$$a^d = 1\ [p]\ OU\ \exists r \in [|0, s-1|], a^{2^r d} = -1$$
5. Miller-Rabin : En déduire un test pour décider a priori si un nombre n'est pas premier

Remarques : La complexité de ce test est logarithmique ce qui est bien mieux que la complexité usuelle en $O(\sqrt{n})$. On pourrait montrer que si p n'est pas premier alors en choisissant a au hasard parmi $[|2, p-1|]$, la probabilité d'obtenir un test de Miller Rabin positif est inférieure à $1/4$. En répétant l'opération 20 fois on a alors seulement une probabilité de $(1/4)^{20} = 10^{-12}$ d'avoir un faux positif (*ie* un faux nombre premier).

Voici un excellent résumé du principe de Miller-Rabin en pratique : `http://defeo.lu/in420/DM3%20-%20Test%20de%20Miller-Rabin`

Éléments de correction : 1. Pour savoir si n est premier, on essaye de diviser n par tous les nombres entiers ≥ 2 inférieurs à $\sqrt{n}$. Si aucun de ces nombres ne donne un quotient entier alors n est premier. 2. Par le petit théorème de Fermat, $\forall p \in \mathcal{P},\ \forall x \in (\mathbb{Z}/p\mathbb{Z})^*,\ x^{p-1} = 1[p]$. Si un nombre ne vérifie pas cette propriété, alors il n'est pas premier. 3. Utiliser le théorème chinois, pour se ramener au calcul de x^560 modulo 3,11 et 17. Puis utiliser le petit théorème de Fermat pour simplifier l'exposant. 4. On commence par remarquer que comme $\mathbb{Z}/p\mathbb{Z}$ est un anneau intègre (car c'est un corps), l'équation $x^2 = 1$ y admet exactement deux solutions 1 et -1. On procède ensuite itérativement en remarquant $a^{p-1} = 1[p]$ par le petit thèorème de Fermat.

5.4 Un lemme usuel

Soit q en entier supérieur à 2.

1. Montrer que si $q^d - 1 | q^m - 1$ alors $d|m$

Éléments de correction : Écrire la division euclidienne de m par d

5.5 Δ Théorème de Liouville (1844)

Les nombres algébriques réels sont les éléments de $\mathbb{R}$ qui sont racines d'un polynôme à coefficients rationnels.

1. Montrer que tous les nombres rationnels sont algébriques et donner un nombre algébrique qui n'est pas rationnel
2. Soit x un nombre algébrique irrationnel. On pose le degré de x ainsi :
$$d(x) := \min\{deg(P) | P \in \mathbb{Q}[X] \backslash \{0\},\ P(x) = 0\}$$
3. Montrer que $d(x)$ est bien défini et que $d(x) >= 2$
4. Montrer que $\exists A > 0, \forall p, q \in \mathbb{Z} \times \mathbb{N}^*, |x - \frac{p}{q}| \geq \frac{A}{q^{d(x)}}$

Remarque : On montre alors facilement que la somme de n=0 à l'infini des $10^{-n!}$ est un nombre transcendant. En effet, la factorielle dans la somme fournit de gros trous avec pleins de zéros dans l'écriture décimale du nombre ce qui permet de l'approcher extrêmement bien par un rationnel en tronquant la somme. Il s'agit de la première construction explicite d'un nombre dont on peut prouver la transcendance.

Éléments de correction : $q^{d(x)}(P(p/q) - P(a))$ est un entier. On pourra ensuite utiliser l'inégalité des accroissements finis.

6 Suites

6.1 Méthode de Héron

Soit $a \in \mathbb{R}$

1. En appliquant la méthode de Newton à $x \mapsto (x-a)^2$, construire une suite qui converge vers $\sqrt{a}$

Remarque : C'est une technique très ancienne et très efficace : `https://fr.wikipedia.org/wiki/M%C3%A9thode_de_H%C3%A9ron`

6.2 Δ Approximation rationnelle

Soit x un nombre réel irrationnel et $(p_n/q_n)_{n\in\mathbb{N}}$ une suite de rationnels qui tend vers x. Montrer que p_n et q_n tendent vers l'infini quand n tend vers l'infini.

6.3 Δ Suites de Cauchy

Soit (U_n) une suite réelle telle que $\forall \epsilon > 0,\ \exists N \in N,\ \forall p, q \geq N, |U_p - U_q| < \epsilon$

1. Montrer que U est bornée
2. Montrer que U converge
3. Application, Théorème du point fixe de Banach : Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$ telle que $\forall x, y \in \mathbb{R},\ |f(x) - f(y)| < k|x - y|$ et $k < 1$. Montrer que f admet un unique point fixe.
4. Est-ce encore vrai si $k = 1$?

Éléments de correction : 3. Montrer qu'une suite définie par la relation de récurrence $U_{n+1} = f(U_n)$ est une suite de Cauchy et que celle-ci converge nécessairement vers un point fixe de f. Soit $p, q \in \mathbb{N}$, tels que $p \geq q$, on a : $|U_p - U_q| \leq k^q |f^{p-q}(U_0) - U_0|$. Il suffit donc de montrer que $(f^n(U_0))_{n\in\mathbb{N}}$ est bornée pour conclure. Cela vient essentiellement de la convergence de la série géométrique de terme k^n. Plus précisément :

$$|f^n(U_0) - U_0| \leq \sum_{j=0}^{n-1} |f^{j+1}(U_0) - f^j(U_0)| \tag{1}$$

$$\leq \sum_{j=0}^{n-1} k^j |f(U_0) - U_0| \tag{2}$$

$$\leq \frac{1}{1-k} |f(U_0) - U_0| \tag{3}$$

4. Considérer par exemple : $f : x \mapsto x + 1$

7 Espaces vectoriels

7.1 Δ Une famille libre

1. Montrer que les $x \mapsto ln(|x + a|)$ pour $a > 0$ forment une famille libre.

7.2 Δ Famille libre adaptée à une application nilpotente

Soit f une application linéaire de Edans E telle que f soit nilpotente d'ordre n. Montrer qu'il existe x dans E tel que $(x, f(x), \dots f^{n-1}(x))$ soit libre

7.3 Dimension de $\mathbb{R}$ vu comme un $\mathbb{Q}$-ev

1. Montrer que $(1, \sqrt{2}, \sqrt{3})$ est $\mathbb{Q}$-libre, que peut-on en déduire quant à $\mathbb{R}$ vu comme $\mathbb{Q}$-espace vectoriel ?
2. Soit P un polynôme à coefficients rationnels de degré 3 tel que $P(\sqrt{2}) = 0$ et $P(\sqrt{3}) = 0$. Montrer que $P = 0$
3. Montrer que $(\ln(p))_{p \in \mathcal{P}}$ est $\mathbb{Q}$-libre, que peut-on dire de la dimension de $\mathbb{R}$ comme $\mathbb{Q}$-ev ?
4. Quelle est la dimension de $\mathbb{C}$ vu comme un $\mathbb{R}$-ev ? Comme un $\mathbb{Q}$-ev ?

Éléments de correction : 1. En élevant au carré une relation de liaison après avoir fait passer $\sqrt{2}$ d'un côté, on en déduirait que $\sqrt{3}$ est rationnel ce qui est absurde. Donc $\mathbb{Q}$ a une $\mathbb{R}$ dimension supérieure ou égale à 3.
2. Utiliser la question 1. 3. Utiliser l'unicité de la décomposition en facteurs premiers. 4. $\mathbb{C}$ est un $\mathbb{R}$ espace vectoriel de dimension 2 mais un $\mathbb{Q}$ espace vectoriel de dimension infinie.

7.4 Idéaux bilatères de $L(E)$

Soit E un espace vectoriel de dimension finie. Un idéal bilatère I de $L(E)$ est un sous-groupe de $(L(E), +)$ qui de surcroît vérifie : $\forall f, g \in I \times L(E),\ f \circ g \in I$ *et* $g \circ f \in I$ Quels sont les idéaux bilatères de $L(E)$?

Éléments de correction : Supposons qu'il existe $f \in I$ tel qu'il existe $x \in E$ tel que $f(x) \neq 0$. Soit $(e_i)_{1 \leq i \leq n}$ une base de E, montrer que pour $i, j \in [|1, n|]$ l'application g telle que $g(e_i) = e_j$ et $\forall k \neq i,\ g(e_k) = 0$ appartient à I. En déduire que I contient une base de $L(E)$. Finalement les seuls idéaux bilatères sont $\{0\}$ et $L(E)$.

7.5 Δ Premier lemme de factorisation

Soit E, F, G des espaces vectoriels. Soit u une application linéaire de E vers F et v de E vers G (faire un schéma). On suppose que F admet une base finie. On cherche w tel que $v = w \circ u$.

1. Supposons qu'un tel w existe, quelle condition nécessaire doivent alors vérifier v et u ?
2. On suppose $Ker(u)$ inclus dans $Ker(v)$, montrer que l'on peut fixer w tel que $v = w \circ u$

7.6 Δ Union finie de sev stricts

Soit $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel

1. Si $\mathbb{K}$ est fini, montrer qu'il existe un $\mathbb{K}$-espace vectoriel qui peut s'écrire comme une union finie de ses sous-espaces vectoriels stricts.
2. On suppose $\mathbb{K}$ infini. Montrer que E n'est pas la réunion de d'un nombre fini de sous-espaces vectoriels stricts.

Éléments de correction : 1. Par exemple, $\mathbb{K}^2 = \bigcup_{x \in \mathbb{K}^2} \mathbb{K}x$. On en déduit qu'il va être crucial d'utiliser le caractère infini du corps dans la question suivante. 2. Soit $F_1, ..., F_n$ des sous-espaces vectoriels stricts de E tels que $F_1 \not\subset \bigcup_{i=2}^n F_i$ (on peut toujours se ramener à ce cas si l'union n'est pas triviale). Soit $y \in F_1 \backslash \bigcup_{i=2}^n F_i$ et soit $z \in E \backslash F_1$ (possible car F_1 est un sous-espace vectoriel strict). Considérons l'application : $t \in \mathbb{K} \mapsto y + tz$. Cette application ne peut prendre au plus qu'une valeur dans chaque F_i pour $i \in [|1, n|]$. En effet, supposons que l'on puisse fixer t_1 et t_2 tels que $y + t_1 z \in F_i$ et $y + t_2 z \in F_i$ alors par différence, $z \in F_i$ (absurde si $i = 1$) puis $y \in F_i$ ce qui est absurde si $i \geq 2$. Comme l'ensemble de départ ($\mathbb{K}$) est infini, cela implique que cette application possède au moins une image qui n'appartient pas à $\bigcup_{i=1}^n F_i$ et donc l'ensemble précédent ne peut pas être égal à E.

7.7 Δ Commutant d'une application nilpotente d'ordre n

Soit E un espace vectoriel de dimension n. Soit f une application de $L(E)$ nilpotente d'ordre n. On note C le commutant de f, *ie* $C := \{g \in L(E) |\ f \circ g = g \circ f\}$

1. Montrer que C est un espace vectoriel de dimension supérieure ou égale à n
2. Montrer qu'on a en fait $\dim(C) = n$.

Éléments de correction : 1. Montrer qu'il existe $x \in E$ tel que $\mathcal{B} := (x, f(x), f^2(x), ..., f^{n-1}(x))$ forme une base de E. En déduire que la famille $(Id, f, f^2, ..., f^{n-1})$ est une famille libre appartenant à C. 2. Soit $g \in C$, g est complètement caractérisée par son image de la base $\mathcal{B}$. Comme g commute avec f, on a pour $k \in [|0, n|[$, $g(f^k(x)) = f^k(g(x))$ donc g est simplement caractérisée par son image de x. Autrement dit, l'application :

$$\begin{aligned} C &\to E \\ g &\mapsto g(x) \end{aligned}$$

est un isomorphisme d'espaces vectoriels. En conséquence $\dim(C) = \dim(E) = n$.

8 Analyse et dérivabilité

8.1 Δ Théorème de Darboux et trois applications

1. Théorème de Darboux : Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ une fonction dérivable. Soit I un intervalle, montrer que $f'(I)$ est un intervalle
2. Donner toutes les fonctions f dérivables qui vérifient : $f'^2 = 1$
3. Montrer que toute fonction convexe et dérivable est nécessairement de classe $\mathcal{C}^1$. On pourra utiliser librement la caractérisation des fonctions convexes dérivables : ce sont les fonctions dont la dérivée est croissante.
4. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$ dérivable telle que $f^2 + 2f * f' + f'^2 = 1$. Que peut-on dire de f ?

Remarques : Le théorème de Darboux permet de renforcer significativement les hypothèses sur une fonction que l'on suppose simplement dérivable. Il est utile de le garder en tête !

Éléments de correction : Pourr un intervalle $[a, b]$, on pourra considérer le taux d'accroissement $g(x, y) := \frac{f(x)-f(y)}{x-y}$ comme une fonction de deux variables. Un chemin qui va de (a, a) à (b, b) sans passer par la diagonale (par exemple en passant par le point (a, b)) balaye nécessairement toutes les valeurs entre $[f'(a), f'(b)]$ par le théorème des valeurs intermédiaires. On applique ensuite le théorème des accroissements finis pour conclure.

8.2 Δ Majoration des fonctions uniformément continue

Soit F une fonction uniformément continue définie sur $\mathbb{R}_+$.

1. Montrer que F peut être majorée par une fonction affine
2. Est-ce que la réciproque est vraie ?

8.3 Pseudo-dérivation

On pose $A : \mathbb{R}[X] \longrightarrow \mathbb{R}[X]$ une application linéaire telle que $\forall P, Q \in \mathbb{R}[X], A(PQ) = PA(Q) + QA(P)$

1. Pour $n \in \mathbb{N}$ et $P, Q \in \mathbb{R}[X]$, calculer $A^n(PQ)$
2. Donner un exemple d'une telle application
3. Déterminer toutes les applications A qui vérifient la condition sus-mentionnée.

Éléments de correction : 1. Penser à la formule de Leibniz, 2. La dérivation 3. On peut trouver $P \in \mathbb{R}[X]$ tel que $A(Q) = P * Q'$

8.4 Commutant des observables impulsion et position

On pose A, B deux applications de $\mathbb{R}[X]$ dans lui-même telles que $A : P \mapsto X * P$, $B : P \mapsto P'$

1. Calculer $[A, B] := A \circ B - B \circ A$
2. Montrer qu'une telle relation de commutation n'est pas possible sur un espace de dimension finie i.e. si A et B sont définis sur un espace de dimension finie.

Remarque : Cette relation de non commutation entre A et B est essentielle en mécanique quantique, c'est la source de l'inégalité de Heisenberg. La deuxième question montre que l'on ne peut pas faire de mécanique quantique sur un espace de dimension finie si l'on veut considérer à la fois la position et l'impulsion d'une particule.

Éléments de correction : 1. $[A, B] = -Id$ 2. Penser à la trace

8.5 Des suites jumelles

Soit $u_0 \in \mathbb{R}$, on définit par récurrence :

1. $u_{n+1} = \cos(u_n)$, montrer que u_n converge et donner sa limite
2. $u_{n+1} = \sin(u_n)$, montrer que u_n converge et expliciter sa limite.

Éléments de correction : 1. Pour α tel que $\cos(\alpha) = \alpha$, majorer par récurrence $|u_n - \alpha|$ 2. Montrer que la suite est monotone et bornée.

9 Systèmes linéaires et matrices

9.1 Détermination théorique de la pente des dunes

9.1.1 Contexte

La barkhane est une dune qui se forme lorsqu'un vent dominant souffle dans une direction unique sur une étendue de sable. Cette dune prend une forme de croissant dont la corde est orthogonale à la direction vent qui l'a formé.
Cette dune est asymétrique et présente deux côtés dont les pentes sont très variés. Le premier côté exposé au vent présente une pente douce sur laquelle le sable remontre sous l'effet du vent.

Le second côté, sous le vent, présente une pente plus forte qui est due à l'avalanche du sable déposé. L'angle de la pente correspond à un angle critique au-delà duquel la pente n'est plus stable. On parle de criticalité auto-organisée (*self-organized criticality*). Le but de ce problème est de déterminer de façon théorique la valeur de l'angle limite.

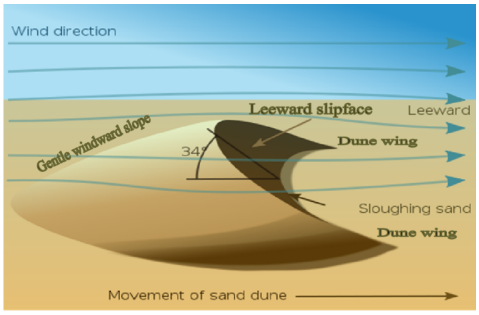

FIGURE 1 – Principe de la barkhane

FIGURE 2 – Barkhanes en Namibie

9.1.2 Modélisation

On considère un empilement compact de sphères comme les mandarines dans la figure 3. On ne s'intéresse qu'à 4 sphères dans cet exercice. Les sphères 0, 1 et 2 sont posés sur un plan de façon compacte et la sphère 3 est posée sur les 3 premières.

1. Quelle est la figure géométrique formée par les centres des 4 sphères ? Quelle est la longueur d'une arête en fonction du rayon des sphères ?
2. Hypothèse : On suppose que les sphères n'exercent entre elles que des forces de réaction normales. Cette hypothèse est relativement bien vérifiée pour le sable du Sahara dont les grains sont extrêmement lisses (Figure 4). On suppose les sphères immobiles, montrer avec le PFD qu'il existe des coefficients positifs a, b et c ainsi que des vecteurs unitaires : r_0, r_1, r_2 tels que :
   (a) r_i ait pour direction la droite passant par le centre de la sphère i et le centre de la sphère 3
   (b) $ar_0 + br_1 + cr_3 = g$ où g le vecteur unitaire négativement colinéaire à la gravité.
3. Montrer qu'il existe une base de vecteurs e_x, e_y et e_z tels que les coordonnées sphériques des vecteurs r_j soient $\begin{bmatrix} 1 \\ \theta \\ j\frac{2\pi}{3} \end{bmatrix}$ On ne cherchera pas à expliciter θ mais on expliquera seulement son origine géométrique.

FIGURE 3 – Mandarines en empilement compact

FIGURE 4 – Sable du Sahara Libyen vu au microscope

Remarque : On déduit facilement du plongement du tétraèdre dans un cube (voir Figure 5) la plupart des formules sur le tétraèdre, par exemple : $\tan(\theta) = \frac{1}{\sqrt{2}}$ On écrira les coordonnées polaires de g dans la base précédemment décrite : $\begin{bmatrix} 1 \\ \theta' \\ \phi \end{bmatrix}$

4. Donner la matrice $R := \begin{bmatrix} r_0 & r_1 & r_2 \end{bmatrix}$ des coordonnées en base cartésienne des vecteurs r_j.
5. Exprimer les coordonnées de g dans la base cartésienne. On notera ce vecteur contenant les coordonnées : $G(\theta', \phi)$.
6. La réciproque de la question 2 étant relativement évidente d'un point de vue physique, on déduit que : les sphères sont en équilibres si et seulement si : $\exists \begin{bmatrix} a \\ b \\ c \end{bmatrix} \in \mathbb{R}^{+3},\ R \begin{bmatrix} a \\ b \\ c \end{bmatrix} = G(\theta', \phi)$ Avec ce formalisme, l'angle d'avalanche est alors donné par :

$$A(\phi) = max \left\{ \theta' \in [0, \pi] \mid \exists \begin{bmatrix} a \\ b \\ c \end{bmatrix} \in \mathbb{R}^{+3},\ R \begin{bmatrix} a \\ b \\ c \end{bmatrix} = G(\theta', \phi) \right\}$$

7. Pourquoi A est-elle périodique ? Quelle est sa période ?
8. On prend $\phi \in [0, \frac{2\pi}{3}]$ et on se place à l'angle d'avalanche : $\theta' = A(\phi)$, que peut-on déduire sur le paramètre c ? *Il s'agit de la condition limite*
9. Écrire le système d'équation reliant alors a, b et $A(\phi)$. Ce système d'équations est-il linéaire ?
10. Exprimer $cos(A(\phi))$ en fonction de $a + b$ et de $cos(\theta)$
11. En résolvant le système d'équations, montrez que :

$$A(\phi) = \arctan(\frac{1}{\sqrt{2}(\cos(\phi) + \sqrt{3}sin(\phi))})$$

12. On trace alors A en fonction de ϕ (figure 6), commentez (on pourra faire le lien avec la valeur de 34 donnée à la Figure 1) :

Éléments de correction : 7. Période : $2\pi/3$. 8. $c = 0$ cela correspond à la perte de contact de la sphère 2 avec la sphère 3. 10. $\cos(A(\phi)) = (a+b)\cos(\theta)$ 11. Trouver une combinaison linéaire des deux autres équations pour exprimer à nouveau $a+b$. On utilise également : $\tan(\theta) = 1/\sqrt{2}$

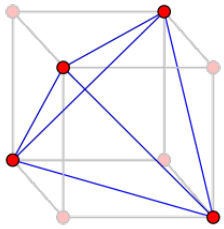

FIGURE 5 – Plongement du tétraèdre dans un cube Source : MathsPoetry https ://commons.wikimedia.org/w/index.php ?curid=25875760

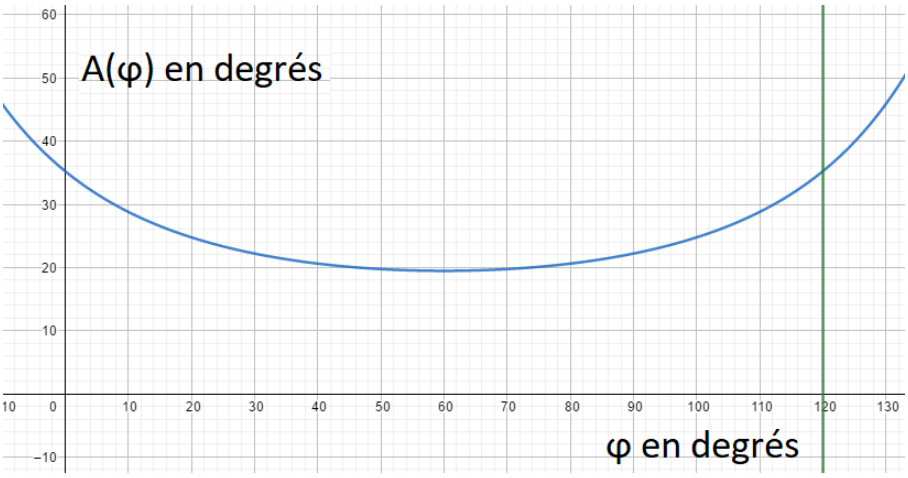

FIGURE 6 – A en fonction de ϕ

9.2 Majoration de la dimension du commutant

Soit E un espace vectoriel de dimension finie $n \geq 2$. Pour f dans $L(E)$, On pose $C(f)$ le commutant de f. C'est à dire : $C(f) := \{g \in L(E) \| \ g \circ f = f \circ g\}$

1. Montrer que $C(f)$ est un sev de $L(E)$
2. On cherche désormais à majorer sa dimension. Quelles applications $f \in L(E)$ vérifient $\dim(C(f)) = n^2$?
3. On suppose que f n'est pas une homothétie. Montrer qu'il existe une base dans laquelle la matrice A représentant f a une première colonne dont seul le deuxième coefficient est non nul et vaut 1
4. On pose M la matrice ayant les coefficients $(l_1, \ldots, l_n)$ sur sa première ligne et $(c_1, .., c_n)$ sur sa deuxième colonne (On a donc $l_2 = c_1$). On la prend nulle partout ailleurs. Donner la première colonne et la deuxième ligne de AM ainsi que celle de MA
5. En notant V les matrices partout nulles en dehors de la première ligne et de la deuxième colonne, déterminer $C(f) \cap V$
6. En déduire que $\dim(C(f)) \leq n^2 - 2n + 2$

Remarque : Cette borne est atteinte pour une matrice dont seul le coefficient en haut à gauche est non nul. On peut montrer qu'un commutant est au moins de dimension n et que cette borne est atteinte pour les applications nilpotentes d'ordre n.

Source : Cette méthode est issue d'une pâle d'algèbre de MP* (2019 Ginette).

9.3 Promenade autour de la légère nuance entre algèbre et sous-algèbre

1. Montrer que tout anneau intègre fini est un corps
2. Soit A une sous-algèbre de $M_n(\mathbb{K})$ et M un élément de A. Montrer avec la même technique que si M est inversible alors son inverse appartient à A.
3. En déduire que toutes les matrices triangulaires supérieures dont la diagonale ne s'annule pas sont inversibles et que leur inverse est une matrice triangulaire supérieure dont la diagonale de s'annule pas.
4. Désormais on suppose seulement que A est une partie de $M_n(\mathbb{K})$ et que $(A, +, x, .)$ est une algèbre. Quelle est la différence avec la situation précédente, est ce que la démonstration de la question 2 est toujours valable ?
5. Que peut-on dire de l'unité de A ? Quelle équation doit-elle vérifier ?
6. Montrer que l'unité de A est de rang maximal dans A
7. Montrer que le résultat de la question 2 reste valable si l'on suppose seulement que A est une algèbre contenue dans $M_n(\mathbb{K})$ avec les mêmes lois.

Remarque : Il s'agit donc d'une généralisation (un peu artificielle) du résultat vu en cours pour les sous-algèbres. A retenir : Il faut faire attention à l'unité d'une algèbre qui n'est pas forcément celle que l'on croit ! Certains cas sont cependant trompeurs : on montre aisément que toute $\mathbb{R}$-algèbre contenue dans $\mathbb{C}$ et pour les mêmes lois a forcément 1 pour unité (un bon exercice apéritif). Une règle générale à garder en tête est que ces algèbres sont souvent un peu dégénérées (au sens du rang pour l'exo

précédent par exemple). Cela vient du fait que seul 1 peut jouer le rôle de l'unité vis-à-vis de tous les autres éléments (unicité du neutre). En supposant que l'unité de l'algèbre est différente de 1 on force structurellement une inclusion stricte dans l'algèbre contenante ce qui peut s'avérer très contraignant en fonctions des cas.

Éléments de correction : 1. On pourra poser pour $y \in A$ non nul : $x \mapsto xy$ et remarquer que cette application est injective. 5. C'est un projecteur 6. $rg(u \circ v) \leq rg(u)$

9.4 Δ Caractérisation de l'antisymétrie

Soit A dans $M_n(R)$. Montrer que : A antisymétrique $\iff \forall X \in \mathbb{R}^n,\ X^T AX = 0$

Éléments de correction : Pour le sens direct, remarquer qu'un élément de $\mathbb{R}$ est égal à sa transposée. Pour le sens réciproque, on peut commencer par montrer : $\forall X, Y \in \mathbb{R}^n,\ X^T AY = -X^T A^T Y$. Pour cela, on peut appliquer la formule à X,Y et $X + Y$.

9.5 Un regard matriciel sur le produit vectoriel

1. Soit E un espace vectoriel de dimension finie et on se donne $B = (e_i)_{1 \leq i \leq n}$ une base. Soit $u : E \times E \longrightarrow F$ une application bilinéaire, c'est-à-dire telle que pour tout $x \in E$,, $u(., x)$ et $u(x, .)$ sont linéaires. Montrer que u est caractérisée par son image de la base couplée : $B \times B$. (C'est-à-dire tous les éléments de la forme (e_i, e_j))
2. On cherche une représentation des vecteurs de $\mathbb{R}^3$ dans $M_3(\mathbb{R})$ qui soit compatible avec le produit vectoriel que l'on note $\times$ et qui est défini comme en physique. C'est-à-dire on cherche une application linéaire $f : \mathbb{R}^3 \longrightarrow M_3(\mathbb{R})$ qui vérifie : $\forall X, Y \in \mathbb{R}^3, X \times Y = f(X)Y$. Montrer que ce problème admet une unique solution et donner une expression explicite de ladite solution que l'on notera f.
3. Quelle est l'image de f ? Quelle est sa dimension ?

Remarque : Ce lien entre les matrices antisymétriques et le produit vectoriel est assez profond. Il pourra être mieux compris en fin de spé avec la notion d'espace tangent des rotations de $\mathbb{R}^3$ en l'identité.

10 Polynômes

10.1 Contenu d'un polynôme et Lemme de Gauss sur les coefficients polynomiaux (*Disquisitiones arithmeticae* 1801)

Pour P un élément de $\mathbb{Z}[X]$ on note $c(P)$ le contenu de ce polynôme c'est-à-dire le pgcd de tous ses coefficients

1. Étant donné P, Q dans $\mathbb{Z}[X]$, montrer que $c(PQ) = c(P) * c(Q)$
2. Lemme de Gauss : Soit P un élément de $\mathbb{Z}[X]$ unitaire et A un diviseur unitaire de P dans $\mathbb{Q}[X]$ Montrer que P est dans $\mathbb{Z}[X]$
3. Application : Soit $P = \sum_{k=0}^{p-1} X^k$ avec p premier. Montrer que P est irréductible dans $\mathbb{Q}[X]$.

Remarque : Ce résultat est énoncé dans les « Recherches arithmétiques » de Gauss qui énonce ce résultat sous sa forme contraposée (proposition 42) et le démontre d'une autre façon bien que « les gens instruits qui voudront comparer [les démonstrations] s'assureront aisément qu'elles partent du même principe ». Il est intéressant de noter le style relativement récent des notations (notamment les notations modulaires). On perçoit aussi l'introduction de notations bien moins explicites qu'aujourd'hui (avec beaucoup de "... "et de "etc"). Peut-être que l'influence relativement récente de l'informatique sur les mathématiques a pu populariser l'utilisation d'indices « dummy » pour les énumérations, ceux-ci étant omniprésents dans les boucles for.

Source : `http://mpstar.lamartin.free.fr/fichiers/matieres-61-1379754810.pdf`

10.2 Δ Interpolation optimale et Polynômes de Tchebychev

Soit f une fonction de $\mathbb{R}$ dans $\mathbb{R}$ de classe $\mathcal{C}^{n+1}$, soit $x_1, .., x_n$ des éléments de $[-1, 1]$ deux à deux distincts. Soit P l'interpolée de Lagrange de f en les $(x_i)_{1\leq i\leq n}$.

1. Soit x dans $[-1, 1]$, montrer qu'il existe y dans $[-1, 1]$ tel que :

$$f(x) - P(x) = \frac{f^{(n)}(y)}{n!} \prod_{1\leq i\leq n} (x - x_i)$$

   Indication : On pourra essayer de construire une fonction auxiliaire afin de trouver y en appliquant le théorème de Rolle.

2. On cherche alors les (x_i) qui minimisent le maximum sur $[-1, 1]$ de $\prod_{1\leq i\leq n}(x - x_i)$. Reformuler cette question avec le vocabulaire polynomial et la norme infinie.
3. Montrer que cet optimum est atteint pour les racines des polynômes de Tchebychev et donner alors une majoration de l'écart avec f.

Remarque : Un résultat assez invraisemblable qui montre que pour obtenir la meilleure interpolation au sens de la norme infinie, il ne faut pas choisir des points régulièrement espacés mais plutôt les choisir selon les racines des polynômes de Tchebychev (ce qui revient à augmenter la densité de points sur les bords).

Éléments de correction : 1. On commence par $x \notin \{x_1, ..x_n\}$. On peut par exemple poser la fonction auxiliaire :

$$A : y \mapsto (f(y) - P(y)) \prod_{1\leq i\leq n} (x - x_i) - (f(x) - P(x)) \prod_{1\leq i\leq n} (y - x_i)$$

On obtient cela par tâtonnements en cherchant une fonction qui s'annule $n + 1$ fois (pour appliquer le théorème de Rolle n fois) et dont l'égalisation de la dérivée n-ième avec 0 donne l'égalité demandée. 2. On cherche un polynôme unitaire à n racines dans $[-1, 1]$ dont la norme infinie est minimale. 3. On pourra commencer par se rappeler deux propriétés des polynômes de Tchebychev $(T_n)_{n\in\mathbb{N}}$ en démontrant l'une à partir de l'autre :

$$\begin{cases} T_n(\cos(x)) = \cos(nx) \\ T_{n+2} = 2XT_{n+1} - T_n,\ T_0 = 1,\ T_1 = X \end{cases}$$

On en déduit que pour $n \in \mathbb{N}^*$ $P_n := \frac{1}{2^n} T_n$ est un polynôme unitaire possédant n racines dans $[-1, 1]$ et de norme infinie $1/2^n$. Soit Q un polynôme unitaire de norme infinie strictement inférieure à $1/2^n$. Considérer $P_n - Q$ et remarquer qu'il s'agit d'un polynôme de degré $n-1$ dont le signe sur les élément de $\{\frac{k\pi}{n} |\ k \in [|0, 2n|[\}$ est connu. Conclure que $P_n = Q$: absurde.

10.3 Δ Stabilisation du cercle unité

Trouver tous les polynômes $P \in \mathbb{C}[X]$ tel que $P(\mathbb{U}) \subset \mathbb{U}$

Éléments de correction : On pourra trouver un polynôme $Q \in \mathbb{C}[X]$ tel que $PQ = X^{\deg(P)}$ en remarquant que $\forall z \in \mathbb{U},\ z\bar{z} = 1$.

10.4 Δ Sommes de Newton nulles

1. Soit $x_1, ..., x_n \in \mathbb{R}$ distincts tels que $\forall k \in \mathbb{N}^*,\ \sum_{i=1}^n x_i^k = 0$. Montrer que $\forall n \in [|1, n|], x_i = 0$
2. Soit $x_1, ..., x_n \in \mathbb{C}$ distincts tels que $\forall k \in \mathbb{N}^*,\ \sum_{i=1}^n x_i^k = 0$. Montrer que $\forall n \in [|1, n|], x_i = 0$

Éléments de correction : 1. Utiliser la relation avec $k = 2$ 2. Montrer que $\forall P \in X\mathbb{C}[X], \sum_{i=1}^n P(x_i) = 0$, puis utiliser les polynômes interpolateurs de Lagrange.

10.5 Polynôme irréductible sur $\mathbb{Z}[X]$

Soit $a_1, ..., a_n \in \mathbb{Z}$ distincts, on pose $P = (X - a_1)...(X - a_n) - 1$. Montrer que P est irréductible dans $\mathbb{Z}[X]$.

Éléments de correction : On écrit $P = AB$ avec $deg(A) \leq n/2$. En évaluant sur les a_i et puisque $A(a_i)$ est entier on obtient $\forall i \in [|1, n|],\ A^2(a_i) = 1$. Si $deg(A^2) < n$ on obtient le résultat, sinon $deg(A^2) = n$ puis $A^2 - 1 = \prod_{i=1}^n (X - a_i) = P + 1 = AB + 1$. Donc $A(A - B) = 2$ et donc A est constant : absurde car $deg(A^2) = n$.

10.6 Inverse d'une matrice de Vandermonde et théorème d'inversion de Fourier discret

1. Soit $x_0, \ldots, x_{n-1}$ des réels deux à deux distincts, montrer que la matrice $A := ((x_i)^j) 0 \leq i, j < n$ est inversible et donner son inverse.
2. Comment se simplifie l'inverse si les $x_0, \ldots, x_{n-1}$ sont les racines n-ième de l'unité ?

Remarques :

1. Le déterminant des matrices de Vandermonde sera vu plus tard dans l'année ce qui donnera un autre argument pour justifier son inversibilité. Cependant il ne faut pas oublier que celle-ci est fondamentalement liée à l'interpolation de Lagrange.
2. La première ligne de l'inverse est facile à évaluer.
3. Dans le cas de la question 2, on retrouve la formule d'inversion de Fourier discrète. Celle-ci stipule que la transformée de Fourier est sa propre inverse (à quelques détails près).

Éléments de correction : 1. Faire le lien avec l'évaluation polynomiale puis utiliser l'interpolation de Lagrange.

Correction :

1. Si l'on note A le vecteur colonne formé des coefficients $[a_0, ..., a_{n-1}]$ alors : $XA = Y$ avec Y le vecteur colonne des $[P(x_0), ..., P(x_{n-1})]$. Avec P le polynôme : $\sum_{i=0}^{n-1} a_i X^i$. On cherche donc pour inverser la matrice à exprimer les coefficients de P à partir de n évaluations de celui-ci que l'on notera y_i. On commence par écrire P dans la base de Lagrange en les x_i afin d'avoir $P(x_i) = y_i$:

$$P = \sum_{i=0}^{n-1} y_i L_i$$

Puis :

$$P = \sum_{i=0}^{n-1} \frac{y_i}{\prod_{j\neq i}(x_i - x_j))} \prod_{j\neq i}(X - x_j)$$

On obtient alors facilement a_0 en évaluant P en 0.

$$a_0 = \sum_{i=0}^{n-1} \frac{y_i}{\prod_{j\neq i}(x_i - x_j))} \prod_{j\neq i}(-x_j)$$

On peut donc en déduire la première ligne de l'inverse de X :
$(\frac{\prod_{j\neq i}(-x_j)}{\prod_{j\neq i}(x_i - x_j))})_{0\leq i<n}$ où i représente ici l'indice de la colonne.
Pour obtenir a_1 (et donc la seconde ligne), il suffit de dériver P puis d'évaluer en 0.
Plus généralement $a_k = P^{(k)}(0)/k!$
Faisons le calcul de P' :

$$P' = \sum_{i=0}^{n-1} \frac{y_i}{\prod_{j\neq i}(x_i - x_j))} \sum_{k\neq i} \prod_{j\neq i,k} (X - x_j)$$

Ce qui peut se réécrire joliment :

$$P' = \sum_{i=0}^{n-1} \sum_{k\neq i} \frac{y_i}{\prod_{j\neq i}(x_i - x_j))} \prod_{j\neq i,k} (X - x_j)$$

On obtient ainsi une idée claire de la forme qu'aura $P^{(k)}$: $k+1$ sommes successives dont la plage décroît de 1 à chaque fois puis un terme de degré $n-1-k$. Avec la formule de P' on déduit tout de suite la seconde ligne de l'inverse :

$$(\sum_{k\neq i} \frac{\prod_{j\neq i,k}(-x_j)}{\prod_{j\neq i}(x_i - x_j))})_{0\leq i<n}$$

où i représente l'indice de la colonne.

2. Plaçons nous dans le cas où les x_i sont les racines n-ièmes de l'unité. Remarquons alors que le produit de tous les x_i vaut -1 si n est pair et 1 sinon (on groupe les termes avec leur inverse). Ainsi : $\prod_{j\neq i}(-x_j) = \frac{1}{x_i}$. De plus :

$$X^n - 1 = \prod_{0\leq j<n} (X - x_j)$$

Donc :

$$\frac{X^n - 1}{X - x_i} = \prod_{j\neq i}(X - x_j)$$

. Pour obtenir l'évaluation du terme de droite en x_i, on cherche la limite de celui de gauche en x_i par continuité, en appliquant la règle de L'Hôpital on obtient : $nx_i^{n-1} = \prod_{j\neq i}(x_i - x_j)$. Finalement, après tous ces efforts et en remarquant que $x_i^n = 1$, on remarque que la première ligne de l'inverse de X est constituée du terme constant égal à $1/n$. Cependant on peut calculer facilement la deuxième ligne avec tous ces calculs préliminaires, on obtient immédiatement pour une colonne i donnée le coefficient

$$(X^{-1})_{2,i} = \sum_{k\neq i} \frac{1}{x_i x_k n x_i^{n-1}} = \frac{1}{n}\sum_{k\neq i}(x_k)^{-1}$$

Or pour les racines n-ièmes de l'unité, l'inversion c'est comme la conjugaison, puis comme la somme de tous les x_i vaut 0 on obtient finalement :

$$(X^{-1})_{2,i} = \frac{1}{n}(x_i)^{-1}$$

On retrouve progressivement la formule d'inversion de Fourier discrète qui établit que l'on obtient l'inverse de X à partir de X en changeant x_i en son inverse (ou son conjugué) puis en multipliant par un facteur 1/n et en transposant (éventuellement inutile si l'on prend les racines dans l'ordre canonique car X devient symétrique).

Pour en savoir plus sur la transformée de Fourier discrète et une utilisation intéressante de celle-ci : `https://www.youtube.com/watch?v=h7apO7q16V0`

10.7 FFT - Fast Fourier Transform

1. Si l'on représente en mémoire les polynômes par la liste de leurs coefficients, avec quelle complexité peut-on donner le résultat du produit de deux polynômes de degré n ?
2. Proposer une autre implémentation des polynômes en mémoire pour que la complexité devienne linéaire.
3. Nous cherchons désormais à trouver une méthode pour passer de la représentation par coefficients à la représentation par valeurs d'un polynôme P. Comment peut-on réaliser cela avec une multiplication matricielle ? Quelle est la complexité temporelle de ce calcul ?
4. On cherche désormais un algorithme récursif qui choisit les points astucieusement pour faire mieux en complexité. Montrer que l'on peut écrire $P = A \circ X^2 + X * B \circ X^2$ avec A et B deux polynômes dont on donnera le degré.
5. Soit $x \in \mathbb{C}$, que valent $P(x)$ et $P(-x)$ en fonction de A et de B ?

6. Afin d'améliorer la complexité, quelles relations peut-on imposer sur les points d'évaluation $x_1, .., x_n$? Comme cela doit être vrai à toutes étapes de la récursion, en déduire un ensemble de (x_i) qui permet d'implémenter un algorithme récursif. Indication : On pourra dessiner l'arbre de récursion dans le cas $n = 4$ pour avoir l'idée.
7. L'algorithme précédent se nomme : FFT, en revenant au formalisme matriciel, expliquer son nom.
8. Quelle est la complexité de la FFT ? En déduire un algorithme en $O(n \log(n))$ pour multiplier deux polynômes représentés par leurs coefficients. *Indication : On remarquera que l'inverse de la matrice dans la question 7 a une forme très simple. C'est l'analogue de la formule d'inversion de Fourier dans le cas discret.*

Remarque : Cet exercice a été inspiré par la vidéo : `https://www.youtube.com/watch?v=h7apO7q16V0` C'est une très belle (et très utile) application du cours sur les matrices et sur les polynômes.

10.8 Matrices circulantes et Transformée de Fourier Discrète

On note $\mathcal{C}$ l'ensemble des matrices circulantes, c'est à dire des éléments de $M_n(\mathbb{C})$ de la forme :

$$\begin{pmatrix} c_1 & c_2 & c_3 & ... & c_n \\ c_n & c_1 & c_2 & ... & c_{n-1} \\ c_{n-1} & c_n & c_1 & ... & c_{n-2} \\ ... & & & & ... \\ ... & & & & ... \\ ... & & & & ... \\ c_2 & c_3 & c_4 & ... & c_1 \end{pmatrix}$$

1. Montrer que $\mathcal{C}$ est un espace vectoriel et en donner une base.
2. Montrer que le produit de deux matrices circulantes est encore une matrice circulante
3. Montrer que deux matrices circulantes commutent toujours entre elles.
4. Montrer que la transformée de Fourier discrète diagonalise les matrices circulantes. *Par transformée de Fourier discrète, on désigne la matrice de Vandermonde des racines n-ièmes de l'unité. Si on note cette matrice F, on demande de montrer que $\forall A \in \mathcal{C},\ F^{-1}AF$ diagonale*

Éléments de correction : 1. On pose J la matrice circulante qui correspond à $c_n = 1$ et $\forall i \in [|0, n|[, c_i = 0$. $(J^0, J, J^2, ..., J^{n-1})$ est une base de $\mathcal{C}$. 2. Une matrice est circulante ssi c'est un polynôme en J. 4. Montrer que $AF = FD$

Remarque : 1) L'article wikipédia `https://fr.wikipedia.org/wiki/Matrice_circulante` est très bien fait pour retracer toute la démarche précédente. 2) On remarque ici que la transformée discrète permet de diagonaliser la matrice de « Shift » des vecteurs la base canonique. Comme cette matrice engendre l'algèbre des matrices circulantes, la transformée de Fourier discrète diagonalise tout élément de cette algèbre. On peut alors se demander quel est l'analogue continu de cette diagonalisation. Il s'agit tout simplement du fait que la transformée de Fourier « diagonalise » la dérivation. En effet, dans l'espace de Fourier, la dérivation est remplacée par une simple multiplication par iw, c'est tout à fait similaire à ce que vous voyez en SI pour la transformée de Laplace.

10.9 Fractions rationnelles et simplifications de somme

Soit $P \in \mathbb{R}_n[X]$ avec n racines distinctes notées : $x_1, \ldots, x_n$

1. Soit $Q \in \mathbb{R}_{n-1}[X]$, simplifier : $\sum_{k=1}^{n} \frac{Q(x_k)}{P'(x_k)}$. *Indication : Polynôme interpolateur de Lagrange*
2. Simplifier $\sum_{k=1}^{n} \frac{1}{(P'(x_k)*x_k)}$
3. Comment calculer $\sum_{k=1}^{n} \frac{1}{P'(x_k)*x_k^p}$?

11 Développements limités

11.1 Δ Racine carrée matricielle via un DL

1. Montrer qu'il existe un polynôme P, que l'on explicitera, tel que $\sqrt{1+x} = P(x) + o(x^{n-1})$ quand x tend vers 0.
2. Montrer que $P^2 - 1 - X$ est divisible par X^n
3. Soit N une matrice nilpotente de $M_n(\mathbb{K})$ En déduire que $I_n + N$ admet une racine carrée (matricielle bien sûr)
4. Montrer que $I_n + N$ est inversible avec la même technique

11.2 Équations différentielles discrètes

1. Soit (U_n) une suite vérifiant $U_{n+1} = U_n + \frac{1}{U_n^2}$, donner un équivalent asymptotique de U_n
2. *Équation logistique* : Soit (U_n) une suite vérifiant $U_{n+1} = U_n - U_n^2$, avec $U_0 \in]0,1[$ donner un équivalent asymptotique de U_n
3. *Équation sub-logistique* : Soit (U_n) une suite vérifiant $U_{n+1} = aU_n(1-U_n)$ avec $0 < a < 1$, expliquer pourquoi un équivalent asymptotique de U_n n'est pas pertinent. Donner un équivalent asymptotique de $log(U_n)$

Remarques : L'équation de la question 2 est un cas limite de la question 3 (on a $U_{n+1} = U_n(1-U_n)$). Ce genre de dynamique peut par exemple modéliser la croissance d'une population : le facteur U_n correspond à une croissance exponentielle auto-induite et le terme $(1-U_n)$ peut s'interpréter comme une limitation matlthusienne liée par exemple aux ressources. On observe ici un phénomène très courant en physique : un comportement exponentiel pour le cas général ($\log(U_n) \sim \log(a^n)$) et un comportement en puissance pour le cas critique ($U_n \sim n^{-1}$).

Éléments de correction : 1. On réécrit $U_{n+1} - U_n = 1/U_n^2$, c'est l'analogue discret de l'équation différentielle $y^2y' = 1$. Celle-ci se résout en $y^3 = 3t$. En conséquence on calcule la quantité $U_{n+1}^3 - U_n^3$ et on montre que celle-ci tend vers une constante. On applique ensuite le théorème de Cesàro pour conclure. 2. De même 3. Un équivalent dans ce cas dépendra du terme initial. On obtient un comportement géométrique.

11.3 Δ Loi de Poisson

Soit $k \in \mathbb{N}$, quelle est la limite de $\binom{n}{k} p^k (1-p)^{n-k}$ lorsque $n \longrightarrow +\infty$ et $np \longrightarrow \lambda \in \mathbb{R}_+^*$?

Remarque : On montre ici que la loi binomiale tend vers la loi de Poisson sous certaines hypothèses. Pour un nombre de tirage n grand, la probabilité d'observer k succès indépendants de probabilité p est bien approchée par la loi de Poisson de paramètre np évaluée en k.

Éléments de correction : On obtient $\frac{\lambda^k}{k!}e^{-\lambda}$

11.4 Complexité minimale du tri

Un algorithme de tri prend en entrée une liste de taille n et fournit en sortie une permutation qui permet de trier la liste. On représente son exécution par un arbre binaire dont les nœuds internes sont des comparaisons (deux issues possibles à chaque fois donc c'est bien un arbre binaire) et dont les feuilles sont des permutations.

1. Donner une minoration du nombre de feuilles que doit avoir l'arbre d'exécution pour que l'algorithme soit correct
2. Donner alors le nombre de comparaisons minimal C_n que doit effectuer l'algorithme
3. Donner un développement asymptotique de C_n quand n tend vers l'infini
4. En déduire qu'un algorithme de tri a au mieux une complexité en $O(n\log(n))$

Éléments de correction : 1. Le nombre de feuilles doit être supérieur au nombre de permutations possibles pour que l'algorithme puisse trier tous les cas. Donc $f \geq n!$. Comme $f \leq 2^{C_n}$, on déduit $C_n \geq \log_2(n!)$. 3. On pourra utiliser la formule de Stirling pour obtenir un développement asymptotique.

12 Intégration

12.1 Δ Norme p et norme infinie

Soit f une fonction continue sur $[0,1]$ à valeur dans $\mathbb{R}$.
Étudier la limite quand $p \to \infty$ de

$$\left(\int_0^1 |f|^p\right)^{\frac{1}{p}}$$

Remarque : On montre ici que la norme p de f ($||f||_p$) tend vers la norme infinie de f ($||f||_\infty$) quand p tend vers l'infini. Cela justifie ce choix de notation qui peut sembler un peu étonnant au premier abord.

12.2 Principe de moindre action et approximation polynomiale

Soit

$$A : f \mapsto \int_0^1 f'^2 - f$$

1. Minimiser $A(P)$ dans $\mathbb{R}[X]$ sous la contrainte $P(0) = 0$ et $P(1) = 0$. *Chercher d'abord un point critique puis examiner les excursions autour de celui-ci pour montrer que c'est un minimum, on pourra remarquer que si P réalise un minimum de A alors la fonction $t \mapsto A(P + tQ)$ est minimale en 0 pour tout polynôme Q nul en 0 et en 1.*
2. Donner une interprétation physique du résultat précédent

3. On s'intéresse à la fonctionnelle $B : \int_0^c P'^2 - P^2$. Quel est le système physique associé ? Quelle est la forme des solutions du problème physique ?
4. Minimiser la fonctionnelle B sur l'espace $\mathbb{R}_2[X]$ avec les conditions $P(0) = P(c) = 1$. Quel polynôme limite retrouve-t-on quand c tend vers 0 ? Est-ce surprenant ?
5. Conditions initiales : Minimiser la fonctionnelle B sur l'espace $\mathbb{R}_2[X]$ avec en sus les conditions : $P(0) = 1$ et $P'(0) = 0$ quand cela est possible.
6. Montrer que sous les hypothèses $f(0) = 1$ et $f'(0) = 0$ la fonctionnelle B n'admet jamais de minimum sur les fonctions deux fois dérivables. On pourra distinguer le cas $c = n\pi$ (utiliser la question précédente) des autres cas.

Remarques : On retrouve dans le cadre de la question 1 le principe de moindre action : Pour une trajectoire P donnée, l'action est définie comme l'intégrale de l'énergie cinétique moins l'énergie potentielle sur toute la trajectoire P. La trajectoire physiquement réalisée correspond à celle qui minimise l'action (aussi appelée Lagrangien) sous contraintes. Attention cette minimisation est a priori un problème très compliqué puisque qu'il faut minimiser sur toutes les trajectoires possibles (ce qui correspond à un espace vectoriel de dimension infinie). En pratique on se restreint souvent à la recherche de solutions approchées sur un espace de dimension finie ($\mathbb{R}_n[X]$ par exemple), c'est le principe de la méthode des éléments finis. Dans le cadre de la question 1, on obtient cependant une solution exacte sur $\mathbb{R}_n[X]$. Pour une interprétation physique de ce résultat un peu surprenant (Comment la particule peut savoir quelle trajectoire « choisir » pour minimiser l'action ?), je conseille de lire le court passage des « Feynman lectures » sur ce sujet, c'est remarquablement bien expliqué : `https://www.feynmanlectures.caltech.edu/II_19.html` Les dernières questions montrent sur un exemple simple qu'il est crucial de poser le problème physique en terme de conditions aux bords et non de conditions initiales pour obtenir des résultats cohérents.

13 Déterminant et Espaces Euclidiens

13.1 Optique Matricielle

On décrit un rayon lumineux à une abscisse x par sa distance à l'axe optique en ce point et également par sa pente. On remarquera que cette formulation ne dit rien du sens de propagation du rayon lumineux. Formellement, un rayon est donc décrit en une abscisse x donnée de sa trajectoire par un vecteur $R_x \in \mathbb{R}^2$

1. On place une lentille de focale f' en x, expliciter une relation linéaire entre le rayon entrant R_x et le rayon sortant R'_x.
2. De même pour la propagation sur un espace libre d'une distance d (en abscisse).
3. On enchaîne sur un banc optique des lentilles et du vide, Comment calculer la matrice correspondant au système total M ? Quel est son déterminant ?
4. On pose $m := Tr(M)/2$, exprimer le polynôme caractéristique $P := \det(M - XI_2)$ en fonction de m.
5. Si l'on répète le système n fois sur le banc optique, est ce que la distance à l'axe optique des rayons sortant du système diverge avec n ? On pourra distinguer les cas selon la valeur de m
6. Application : On agence n lentilles de focale f' séparée par une distance L à chaque fois, est ce que les rayons en sortie divergent avec n ?

7. Commenter les cas limites de la question précédente.
8. Comment réaliser expérimentalement ce dispositif sans avoir n lentilles ?
9. Dans ce formalisme, que peut-on dire de deux rayons dont les représentations sont colinéaires ?
10. Retrouver le théorème des vergences avec ce formalisme
11. Avec l'expérience de la question 6 et le dispositif expérimental de la question 8, dans quels cas les trajectoires des rayons sont-elles fermées ?
12. On prend $L/f' = 3$ puis $L/f' = \pi$, commenter le dessin des trajectoires du rayon qui suit :

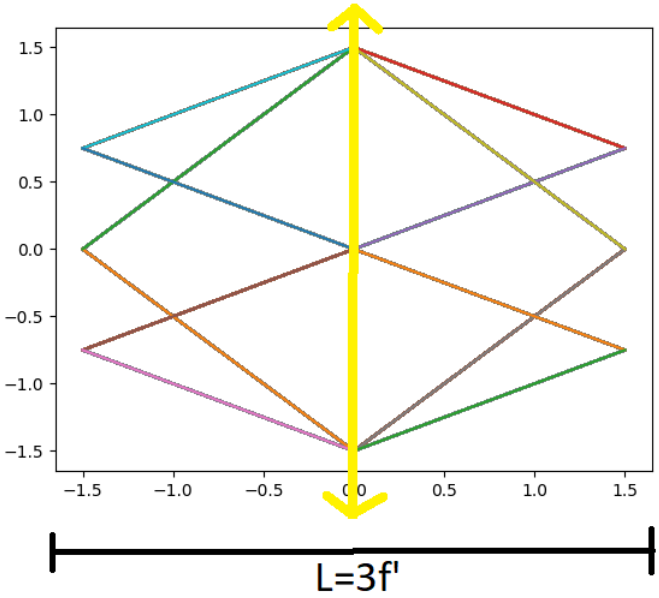

FIGURE 7 – Tracé du trajet d'un rayon quand $L = 3f'$

Éléments de correction : 1. $\begin{pmatrix} 1 & 0 \\ -\frac{1}{f'} & 1 \end{pmatrix}$ 2. $\begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix}$ 5. On distinguera les cas : $|m| < 1$, $|m| > 1$ et $m = 1$ ou $m = -1$ et on s'intéressera au caractère réel ou pas des racines du polynôme caractéristique. 6. Pour que les rayons ne divergent pas, il faut $L/f' < 4$ 7. $|m| = 1$ Il existe un seul rayon stable dans ce cas. 8. Cf la Castafiore pour avoir une indication. 9. Ces rayons se croisent sur l'axe optique.

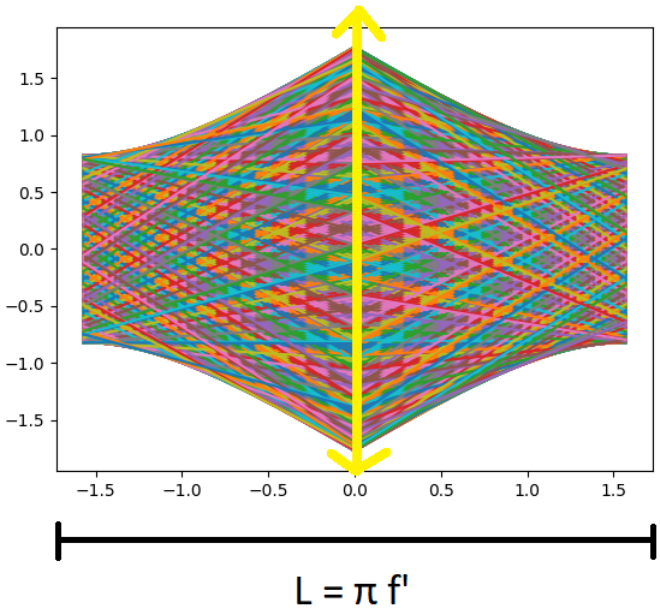

FIGURE 8 – Tracé du trajet d'un rayon quand $L = \pi f'$

13.2 Factorisation de $SL_2(\mathbb{R})$

On rappelle la définition du groupe $SL_2(\mathbb{R})$:

$$SL_2(\mathbb{R}) := \{M \in M_2(\mathbb{R}) |\ \det(M) = 1\}$$

On admet pour le moment la proposition $(P) \iff \forall A \in SL_n(\mathbb{R}), \exists X \in \mathbb{R}^n, ||AX|| = ||X||$.

1. En déduire que toute matrice A de $SL_2(R)$ peut s'écrire sous la forme :

$$A = R_1 \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} R_2$$

où R_1, R_2 sont deux rotations du plan. On appellera la matrice centrale : "matrice de cisaillement".

2. On va maintenant démontrer la proposition (P) en passant par un lemme intermédiaire. Soit A dans $GL_n(\mathbb{R})$, montrer que si pour tout X dans $\mathbb{R}^n$, $||AX|| < ||X||$ alors $det(A) < 1$. *Indication : Gram-Schmidt/Lemme de Hadamard*
3. Démontrer (P). *Indication : Considérer A^{-1} pour obtenir Y tel que $||AY|| > ||Y||$ puis appliquer le théorème des valeurs intermédiaires*
4. Comment peut-on calculer efficacement x ?
5. Quelles sont les factorisations possibles de l'identité avec cette méthode ?
6. On se place en l'identité, si l'on joue sur le paramètre des deux rotations on explore un espace de « dimension » ... ? Il s'agit d'un phénomène de "blocage de cardan".

Remarque : On montre ici que les éléments de $SL_2(\mathbb{R})$ sont issues essentiellement de 2 matrices de rotation et d'une matrice de cisaillement. Cette description est relativement « sobre » puisque les degrés de libertés coïncident bien : $SL_2(\mathbb{R})$ contient 3 degrés de libertés, 4 coefficient choisis librement moins une relation de liaison ($\det = 1$). Réciproquement, les choix des 2 matrices de rotation apportent 2 degrés de liberté (angles des rotations) et le cisaillement apporte un degré de liberté supplémentaire. Ces notions de « degrés de libertés » pourraient être formalisées en parlant plutôt de la dimension de l'algèbre de Lie de $SL_2(\mathbb{R})$, moins pompeusement, il s'agit simplement de la dimension de l'espace tangent en l'identité. On retrouve d'ailleurs ici un phénomène de "gimbal locking" (blocage de Cardan) en effet, si la matrice de cisaillement est égale à l'identité, alors le fait de jouer sur les paramètres des deux rotations ne permet que d'explorer un espace à un degré de liberté ! Le "gimbal locking" est surtout connu pour les angles d'Euler (utilisés pour paramétrer $SO_3(\mathbb{R})$) qui admettent exactement le même type de blocage. Les quaternions unitaires permettent de représenter $SO_3(\mathbb{R})$ sans ce phénomène de « Gimbal Locking », `https://fr.wikipedia.org/wiki/Quaternions_et_rotation_dans_l%27espace`

Éléments de correction : Pour obtenir x, on remarque : $Tr(A^T A) = x^2 + 2$

13.3 Quaternions

On définit :

$$SU_2(\mathbb{R}) := \{M \in M_2(\mathbb{C}) |\ \det(M) = 1,\ M^* M = I_2\}$$

où l'étoile désigne la transconjuguée (transposée de la matrice que l'on conjugue coefficient par coefficient).

1. Montrer que $\mathbb{R}^+ \cdot SO_2(\mathbb{R})$ est un corps
2. Montrer que $\mathbb{R}^+ \cdot SU_2(\mathbb{C})$ est un corps. Quelle est sa dimension en tant que $\mathbb{R}$-algèbre ?

Remarque : On voit que le corps des quaternions peut s'obtenir (Q2) de façon analogue au corps des complexes (Q1). On pourrait même généraliser encore pour obtenir les octonions par un procédé similaire. Les quaternions ne sont pas qu'une curiosité mathématique et ont une importance énorme en physique de part leur lien très fort avec les rotations de $\mathbb{R}^3$: `https://fr.wikipedia.org/wiki/Quaternions_et_rotation_dans_l%27espace`. Cela est notamment utilisé dans les centrales inertielles pour palier au phénomène de « blocage de cardan ». Les quaternions sont également très utiles en physique quantique pour comprendre des phénomènes subtiles liés au spin.

13.4 Δ Degré et rang

Soit $M \in M_n(\mathbb{R})$ et $A \in M_n(\mathbb{R})$ une matrice de rang r. Montrer que $deg(det(M + XA)) \leq r$

13.5 Plongement du groupe symétrique dans $M_n(\mathbb{R})$

On considère l'application :

$$F : \sigma \in S_n \mapsto M_\sigma := (\delta_{i,\sigma(j)})_{i,j} \in M_n(\mathbb{R})$$

qui réalise un plongement de l'ensemble des permutations des entiers entre 1 et n dans l'espace des matrices de taille $n \times n$. Le but de cet exercice est d'exhiber certains liens entre le formalisme matriciel usuel et les permutations par le biais de ce plongement.

1. Montrer que pour $\sigma, \tau \in S_n$, $M_{\sigma\circ\tau} = M_\sigma M_\tau$
2. Montrer que $det(M_\sigma) = \epsilon(\sigma)$
3. Calculer $Com(M_\sigma)$
4. Montrer que $det(M_\sigma - I_n) = 0$
5. En déduire que $det(M_\sigma + I_n)$ est pair
6. Que vaut $Tr(M_\sigma)$?
7. A quelle condition M_σ est-elle symétrique ?
8. Montrer que l'application canoniquement associée à M_σ est une isométrie
9. En déduire une restriction sur les valeurs propres de M_σ
10. Comment peut-on réduire M_σ en une matrice par bloc ?
11. Quel est le polynôme caractéristique de M_σ ? En déduire une meilleure restriction sur les valeurs propres possibles.

14 Dénombrements

14.1 Groupe de Heisenberg discret

On pose $H_3(\mathbb{Z}) = \left\{ \begin{pmatrix} 1 & y & z \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \mid (x,y,z) \in \mathbb{Z}^3 \right\}$

1. Montrer que $H_3(\mathbb{Z})$ muni du produit matriciel $*$ est un groupe
2. Est-ce que $(H_3(\mathbb{Z}), *)$ est isomorphe à $(\mathbb{Z}^3, +)$?
3. Montrer que pour tout $A, B, C \in H_3(\mathbb{Z})$, $[A,B]C = C[A,B]$ où $[A,B] := ABA^{-1}B^{-1}$ désigne le commutateur
4. On pose $X := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, Y := \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, Z := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ que vaut $[X,Y]$?
5. Soit $n \geq 2$, on pose $B_n := \left\{ \prod_{k=1}^n A_k \mid (A_k)_{k\in[|1,n|]} \in \{X, Y, Z, I_3\}^n \right\}$, montrer que $|B_n| \leq 4^n$
6. Montrer que pour tout $A \in B_n$, on peut trouver des entiers $x, y, z, j \in \mathbb{N}$ tels que $A = X^x Y^y Z^{z+j}$ avec $x + y + z \leq n$ et $j \leq xy$
7. En déduire que $|B_n| \leq n^4$
8. Montrer que pour $x, y, z \in \mathbb{N}^3$, si $z \leq xy$ et $x + y \leq n$ alors $X^x Y^y Z^z \in B_n$
9. Montrer que l'application $(x,y,z) \in \mathbb{Z}^3 \mapsto X^x Y^y Z^z \in H_3(\mathbb{Z})$ est injective
10. En déduire que $|B_n|$ est asymptotiquement minoré par $n^4/24$
11. On compare avec la situation dans $(\mathbb{Z}^3, +)$, on remplace donc X, Y, Z par $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$ respectivement et on utilise désormais la somme comme loi de groupe. Comment croît B_n avec n ? Intuitivement, que dire de la "dimension" du groupe de Heisenberg ?

Remarque : On montre ici que la "boule de rayon n" du groupe de Heisenberg discret croît comme n^4 ce qui est surprenant puisque celui n'est indexé que par 3 coefficients. Dans la figure ci-dessous, on trace les projections selon deux des axes d'une marche aléatoire sur le groupe de Heisenberg qui à chaque pas est multipliée à droite par un élément de $\{X, Y, Z, X^{-1}, Y^{-1}, Z^{-1}\}$. Les axes x et y semblent être complètement symétriques si l'on ne regarde que la projection centrale. Cependant, les projections latérales montrent que les coordonnées sur les deux axes ne sont pas du tout corrélées de la même manière à la coordonnée sur l'axe z ! Cette asymétrie est due au choix d'un côté pour la multiplication matricielle à chaque pas. Si l'on multipliait l'état courant de la marche aléatoire à gauche, alors les rôles de x et y seraient inversés.

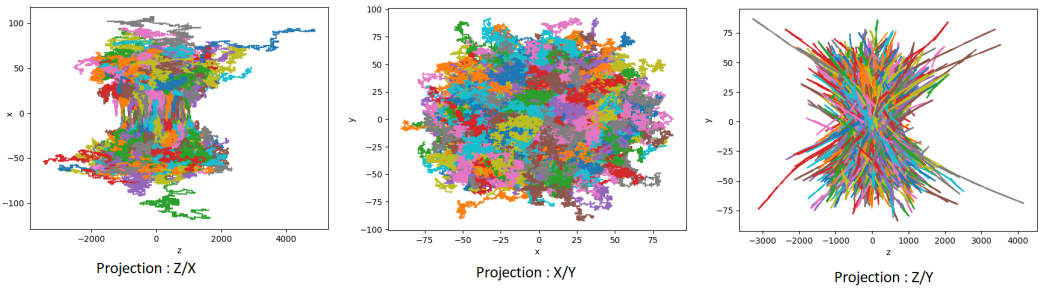

FIGURE 9 – 3000 réalisations de marches aléatoires de 2000 pas en partant de I_3 au sein du groupe de Heisenberg discret

Éléments de correction : 2. On pourra remarquer que le groupe de Heisenberg n'est pas abélien. 3. On remarque ici que tout commutateur est dans le centre du groupe de Heisenberg. 4. $[X, Y] = Z$ 6. On pourra commencer par remarquer que Z commute avec tous les éléments du groupe par les questions 3 et 4. On peut ensuite simplifier le reste du produit en remarquant que permuter un X et un Y "génère" un Z en vertu de la question 4. 9. On remarquera que le coefficient $(1, 2)$ donne directement x et que celui en $(2, 3)$ donne y. 10. Par les questions 8 et 9 on peut minorer B_n par $\sum_{S=0}^{n} \sum_{x=0}^{S} 1 + x(S - x)$ (S correspond à $x + y$). En permutant les sommes, on peut ensuite minorer la quantité précédente par : $\sum_{x=0}^{n} \frac{1}{2} x(1 - x)^2 \underset{n \longrightarrow \infty}{\sim} n^4 \frac{1}{2} \int_0^1 t(1 - t)^2 dt = \frac{n^4}{24}$ (somme de Riemann).

14.2 Formule de Burnside et trous d'eau dans un réacteur nucléaire

14.2.1 La formule de Burnside

Soit X un ensemble fini et G un groupe fini agissant sur X. C'est à dire que l'on se donne une opération "." :

$$G \times X \to X$$
$$(g, x) \mapsto g.x$$

telle que le neutre du groupe $e \in G$ vérifie $\forall x \in X, e.x = x$ et telle que $\forall x \in X,\ \forall g, g' \in G, g.(g'.x) = (gg').x$

Remarques : On omet ici de noter la loi du groupe (notation multiplicative implicite), par contre, pour des raisons de clarté, on utilisera toujours "." pour désigner l'action du groupe sur X. Voici un exemple pour clarifier les idées : on pourrait prendre $X := [|1, 8|]^{-1,13}$ l'ensemble des numérotations des sommets du cube et $G := \{R \in SO_3(\mathbb{R})|\ R([-1, 1]^3) = [-1, 1]^3\}$, c'est à dire l'ensemble des rotations de $\mathbb{R}^3$ qui envoient le cube sur lui-même. La loi de groupe est donnée dans ce cas par : $\forall g, x \in G \times X,\ (g.x)(\_) = x(g^{-1}(\_))$.

1. On pose la relation suivante : $\forall x, y \in X, x \sim y \iff \exists g \in G, y = g.x$. Montrer qu'il s'agit d'une relation d'équivalence. On notera alors $(X_i)_{1 \leq i \leq n}$ les classes d'équivalence de X pour cette relation. On cherche désormais à obtenir une formule pour n, le nombre de classes d'équivalence pour $\sim$ (aussi appelées orbites).
2. On pose :
$$\begin{cases} \forall g \in G, & \text{Fix}_g := \{x \in X | g.x = x\} \\ \forall x \in X, & G_x := \{g \in G | g.x = x\} \end{cases}$$
Montrer que
$$\sum_{g \in G} |\text{Fix}_g| = \sum_{i=1}^{n} \sum_{x \in X_i} |G_x|$$
3. Soit $i \in [|1, n|]$ et $x \in X_i$. On pose la relation $\forall g, g' \in G,\ g \triangle g' \iff {g'}^{-1} g \in G_x$. Montrer qu'il s'agit d'une relation d'équivalence. On notera désormais G/G_x l'ensemble des classes d'équivalence pour la relation $\triangle$ (il s'agit du groupe quotient).
4. Montrer que l'application :
$$G/G_x \to X_i$$
$$g \mapsto g.x$$
est bien définie, puis qu'elle définit une bijection entre G/G_x et X_i.
5. En déduire la *formule de Burnside*
$$n = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}_g|$$

14.2.2 Application : les trous d'eau dans un réacteur nucléaire

Intuitivement, la formule de Burnside permet de compter facilement le nombre d'éléments de X qui sont fondamentalement différents, c'est à dire qui ne peuvent pas être transformés l'un en l'autre par l'action du groupe de symétrie G.

On considère un (très petit) réacteur nucléaire à eau dont l'assemblage peut être modélisé par une grille 6×6. Chaque case de cette grille peut être occupée par un crayon contenant le combustible ou bien laissée vide. Une case vide sera donc simplement occupée par l'eau du coeur d'où l'appellation : trou d'eau.

1. Combien y a-t-il de configurations contentant k trous d'eau ?
2. On considère maintenant que deux configurations qui peuvent être envoyées l'une sur l'autre par rotation d'un quart de tour sont identiques. Cela implique que le groupe de symétrie est dans ce cas $G := C_4 := \{Id, r, r^2, r^3\}$ où r est la rotation d'un quart de tour. Il s'agit dans ce cas d'un groupe commutatif. En utilisant la formule de Burnside, combien y a-t-il désormais de configurations différentes contentant k trous d'eau ?
3. On considère désormais qu'en plus des rotations, deux configurations qui peuvent être obtenues par symétrie selon l'axe vertical (on notera s cette symétrie sont identiques. Montrer que le groupe $G := D_8 =< r, s >$ engendré par r et s contient 8 éléments. Il s'agit du groupe diédral d'ordre 8.

Éléments de correction : Partie (I) :
2. Montrer que le membre de gauche et le membre de droite sont tous deux égaux au cardinal de l'ensemble $\{(g, x) \in G \times X | g.x = x\}$ 4. Montrer que deux représentants d'une classe d'équivalence s'envoient bien sur le même élément de X et que cet élément appartient bien à X_i (bonne définition). Pour l'aspect bijectif, on peut simplement expliciter l'inverse de cette application, pour $y \in X_i$, on peut fixer $g \in G$ tel que $y = g.x$ par définition de X_i. Il suffit alors d'associer à y la classe de g pour obtenir l'inverse de l'application précédente. 5. G contient $|G/G_x|$ classes pour la relation $\triangle$ et chacune de ces classes contient G_x éléments. Comme celles-ci forment une partition de G, on a la relation : $|G| = |G_x||G/G_x| = |G_x||X_i|$ par la question précédente. En injectant l'expression de $|G_x|$ pour tout $x \in X$ dans la formule de la question 2, on obtient la formule de Burnside.
Partie (II) :
1. $\binom{36}{k}$ 2. Une configuration laissée invariante par r est déterminée par sa restriction à un quart du carré. Donc $|\text{Fix}_r| = \delta_{k\equiv 0[4]}\binom{9}{k/4}$. De même pour r^3. Pour r^2, la moitié du carré détermine la configuration totale pour un point fixe. On obtient :

$$\frac{1}{4}\left(\binom{36}{k} + 2\delta_{k\equiv 0[4]}\binom{9}{k/4} + \delta_{k\equiv 0[2]}\binom{18}{k/2}\right)$$

3. On peut également obtenir à partir de r et de s : une symétrie selon l'axe horizontal et deux symétries selon les diagonales. Cela fait bien 8 éléments avec Id, r, r^2, r^3. 4.

$$\frac{1}{8}\left(\binom{36}{k} + 2\delta_{k\equiv 0[4]}\binom{9}{k/4} + 3\delta_{k\equiv 0[2]}\binom{18}{k/2} + 2\sum_{j=1, j\equiv 0[2]}^{k/2}\binom{15}{j}\binom{6}{k-2j}\right)$$

Source : Merci à Thomas Delcambre pour l'idée de cet exercice. La preuve de la formule de Burnside a été simplifiée à partir de : Neumann-Stay-Thompson, *Groups and Geometry* p100.

14.3 Lemme de Poincaré

On désigne par $A \subset M_n(\mathbb{R})$ l'ensemble des matrices à coefficient dans $\{0, -1, 1\}$ qui ont sur chaque colonne au plus un 1 et au plus un -1

1. Montrer que le déterminant des éléments de A vaut 0 , -1 ou 1 (lemme de Poincaré)
2. Montrer que A est fini et contient autant de matrices de déterminant 1 que de matrices de déterminant -1
3. Montrer que le nombre de matrices de A non inversibles est impair
4. En déduire que le cardinal de A est impair
5. Dénombrer A
6. On note $\mathcal{I}$ l'ensemble des matrices de A qui sont inversibles, montrer que le cardinal de $\mathcal{I}$ est un multiple de $2^n n!$
7. On écrit $|\mathcal{I}| = k2^n n!$, montrer que $k \geq 2^{n-1}(n-1)!$

Remarque : Ce lemme peut sembler anecdotique, cependant il est fondamental dans la théorie de l'optimisation. En effet, supposons que l'on cherche à minimiser une fonction linéaire dépendant de paramètres entiers et avec des contraintes linéaires. On peut montrer que si la matrice définissant les contraintes est totalement unimodulaire (toutes ses sous-matrices carrées sont de déterminant 1) alors il est équivalent de chercher à minimiser la fonction sans supposer que les paramètres sont entiers (ce qui est beaucoup plus facile). Pour en savoir plus : `https://fr.wikipedia.org/wiki/Optimisation_lin%C3%A9aire_en_nombres_entiers`

Éléments de correction : 1. Procéder par récurrence en développant sur les colonnes tant qu'il existe une colonne ne contenant pas à la fois 1 et -1. Dans le cas ou toutes les colonnes comportent un 1 et -1, trouver un élément dans le noyau de la transposée. 2. Poser une bijection en opposant la première colonne. 3. Considérer la matrice nulle à part 5. $(n^2+n+1)^n$ 6. Partitionner en classes d'équivalences (M équivalent à N ssi il existe C tel que C soit obtenue en permutant les colonnes de N et que $M = C$ dans $\mathbb{Z}/2\mathbb{Z}$) 7. Considérer un processus de fabrication de « beaucoup » de matrices inversibles dans A, par exemple en partant de matrices triangulaires supérieures.

14.4 Solides de Platon

1. On considère un graphe connexe, non vide et planaire dessiné sur une sphère. C'est-à-dire un ensemble de points V sur une sphère connectés par un ensemble E d'arêtes qui ne se coupent pas (planaire) et qui permettent d'aller d'un point à n'importe quel autre (connexité). Les arêtes E découpent la sphère en plusieurs zones que l'on appelle faces et on note F l'ensemble des faces. On note avec des minuscules le cardinal de tous ces ensembles. Montrer que $v - e + f = 2$ (caractéristique d'Euler). (On attend une démonstration qui soit précise mais pas forcément très formelle puisque F n'est pas défini en termes formels).
2. Montrer que la relation $v - e + f = 2$ est toujours valable (dans un sens que l'on précisera) pour un polyèdre convexe (convexe = si deux points sont à l'intérieur du polyèdre alors l'ensemble du segment entre ces deux points aussi).
3. On cherche à trouver tous les polyèdres réguliers et convexes (régulier = les faces correspondent à un unique polygone régulier du plan un nombre constant de faces se touchent à chaque sommet). En déduire que pour ces polyèdres on obtient des équations supplémentaires sur v, e et f. On pourra introduire de nouveaux paramètres si besoin.
4. Donner toutes les solutions entières positives aux équations précédentes. En déduire les 5 solides de Platon.

Remarque : Les noms des ensembles de la question 1 viennent de la dénomination anglaise : V (vertex, vertices), E (edge, edges), F (face, faces). On obtient en question 4 les solides de Platon : `https://fr.wikipedia.org/wiki/Solide_de_Platon`

Éléments de correction : 1. Par exemple une récurrence sur e. 2. On prend un polyèdre avec des faces transparentes. On le place à l'intérieur d'une sphère, on choisit ensuite un point quelconque à l'intérieur du polyèdre et on place une source lumineuse en ce point, cette source projette alors sur la sphère un graphe qui a autant d'arêtes, de faces et de sommets que le polyèdre convexe. 3. Par exemple, on peut introduire n le nombre d'arêtes par polygone et q le nombre de polygones qui se touchent à chaque sommet. On a alors $v = nf/q$ et$e = nf/2$. 4. Montrer que $1/q + 1/n > 1/2$ puis énumérer toutes les possibilités en remarquant que $n \geq 3$ et $q \geq 3$.

15 Probabilités

15.1 Polynômes de Bernstein et Courbes de Bézier

Soit $f : [0,1] \longrightarrow \mathbb{R}$ continue et $x \in [0,1]$.

1. Soit $X_1, \ldots, X_n$ des variables aléatoires indépendantes et identiquement distribuées suivant une loi de Bernoulli de paramètre x. Que vaut $\mathbb{E}\left(f\left(\frac{X_1+\ldots+X_n}{n}\right)\right)$?
2. On pose : $Y_n := X_1 + ... + X_n$. Montrer que pour $\epsilon > 0$, il existe $\delta > 0$ tel que :
$$\left| f\left(\frac{Y_n}{n}\right) - f(x) \right| \leq \epsilon \mathbb{1}_{|\frac{Y_n}{n}-x|\leq\delta} + 2 \mid\mid f \mid\mid_\infty \mathbb{1}_{|\frac{Y_n}{n}-x|\geq\delta}$$
3. (Théorème d'approximation de Weierstrass) Montrer qu'il existe P_n une suite de polynômes à coefficients réels tels que :
$$\mid\mid f - P_n \mid\mid_\infty \underset{n\longrightarrow\infty}{\longrightarrow} 0$$
4. On pose, pour $k \in [|0,n|]$ le k-ième polynôme de Bernstein :
$$B_k^n = \binom{n}{k} X^k (1-X)^{n-k}$$
Montrer que
$$\int_0^1 B_k^n(x)dx = \frac{1}{n+1}$$
5. Si l'on intègre la différence de f avec son interpolée via les polynômes de Bernstein, puis que l'on fait tendre n vers l'infini, quel résultat d'intégration retrouve-t-on ?
6. (Courbes de Bézier) Soit $z_0, ..., z_n \in \mathbb{C}$. On pose
$$z : t \in [0,1] \mapsto \sum_{i=0}^{n} B_i^n(t) z_i$$
   (a) Que valent $z(0)$ et $z(1)$?
   (b) Montrer que pour tout $t \in [0,1]$, $z(t)$ appartient à l'enveloppe convexe de $(z_i)_{0\leq i\leq n}$.
   (c) Que valent $z'(0)$ et $z'(1)$?
   (d) Montrer que z ne peut pas décrire un arc de cercle non trivial, quel que soit le choix des points $(z_i)_{0\leq i\leq n}$
7. Montrer que les $(B_i^n)_{0\leq i\leq n}$ forment une base de $\mathbb{R}_n[X]$

Remarque : Les courbes de Bézier ont été développées pour tracer des carrosseries de voitures. Elles sont désormais très utilisées pour le dessin assisté par ordinateur. Les courbes de Bézier permettent par exemple de définir des courbes relativement élégantes et complexes avec très peu d'informations (seulement les points de contrôle). Ainsi cela permet de créer des polices très efficacement ou bien alors des logos (format SVG par exemple). Il me semble que le tracé des "lignes courbes" sur Paint se fait via des courbes de Bézier de degré 4 ce qui permet de comprendre beaucoup mieux comment placer les points pour parvenir à la courbe que l'on souhaite. En effet, $z'(0)$ est colinéaire à $z_1 - z_0$ et $z'(1)$ est colinéaire à $z_3 - z_2$. Il peut être assez intéressant et amusant de réaliser l'expérience cognitive suivante : demander à quelqu'un de réaliser une courbe particulière via Paint et observer si celui-ci parvient à inférer au fil de multiples essais, les propriétés de la question 6.

Éléments de correction : 1. Utiliser la formule de transfert 2. Utiliser la continuité uniforme de f 6b. Considérer comment on peut exprimer 1 à partir des polynômes de Bernstein. 6c. Considérer la nature polynomiale de la norme au carré.

15.2 Borne entropique sur la compression de données

Soit T un arbre binaire dont chaque noeud a 0 ou 2 fils et P une loi de probabilité sur l'ensemble des feuilles F. On tire aléatoirement une feuille selon la loi P. Et on définit H la variable aléatoire qui correspond à la profondeur de la feuille. On cherche à donner une minoration de l'espérance de H.

1. Montrer par récurrence sur la hauteur de l'arbre que $\mathbb{E}(H) \geq -\sum_{f \in F} p_f \log_2(p_f)$
2. Soit S une variable aléatoire de loi P. On encode chaque issue de S en une séquence de bits de façon univoque : Aucune séquence ne peut être préfixe d'une autre séquence. Montrer que la longueur moyenne de cette séquence aléatoire est de taille supérieure ou égale à $-\sum_{y \in S(\Omega)} P_y \log_2(P_y)$ (Borne entropique de Shannon).
3. Pour atteindre cette borne, quelle longueur de bits doit en moyenne être allouée à un symbole de probabilité p ?
4. Supposons que $S(\Omega) = \{A, B, C\}$ et que $\mathbb{P}(S = A) = 1/2$, $\mathbb{P}(S = B) = 1/4$ et $\mathbb{P}(S = C) = 1/4$. Donner dans ce cas un encodage des issues de S qui réalise l'égalité dans l'inégalité précédente.
5. Si l'on considère S_1 et S_2 indépendant, quelle borne obtient t'on pour la longueur d'encodage des issues du couple (S_1, S_2) ? Est-ce surprenant ?

Éléments de correction : 1. Considérer les deux sous-arbres issus de la racine. 2. Remarquer qu'un encodage par une séquence de bits peut être vu comme un arbre binaire. 3. $-\log_2(p)$, c'est un principe fondamentale en théorie de l'information. 4. Par exemple :

— A : 1
— B : 01
— C : 00

5. L'entropie du couple est donnée par la somme des entropies : puisque ces variable sont indépendantes, la quantité d'information apportée par leur couple est égale à la somme des quantités d'informations apportées par chacune d'entre elles.

Remarque : L'article original de Shannon (*A Mathematical Theory of Communication*) qui présente ce concept d'entropie sous l'angle informationnel est remarquablement aisé à lire, et ne fait pas appel à beaucoup de notions du formalisme probabiliste.

15.3 Estimateur non biaisé de la variance

On considère $X_1, \ldots, X_n$ des variables aléatoires i.i.d d'espérance m et de variance σ^2. On cherche à estimer σ^2. Pour cela on considère naïvement l'expression de la variance empirique :

$$V = \frac{1}{n}\sum_{i=1}^{n}(X_i - M)^2$$

où M désigne la moyenne empirique :

$$M := \frac{1}{n}\sum_{i=1}^{n} X_i$$

1. On cherche à calculer $\mathbb{E}(V)$. Montrer que l'on peut supposer que m=0
2. Calculer $\mathbb{E}(V)$
3. En déduire un meilleur estimateur de la variance

Éléments de correction : 1. Remarquer que l'expression de V est invariante par ajout d'une constante à chaque X_i. 3. Il suffit, de façon assez surprenante, de remplacer n par $n-1$ pour obtenir un estimateur non biaisé :

$$V_2 = \frac{1}{n-1}\sum_{i=1}^{n}(X_i - M)^2$$

On retrouve cette expression dans de nombreux formulaires de physique et contrairement à ce que l'on pourrait penser de prime abord, le $n-1$ n'est pas dû à une erreur de comptage !

Remarque : Cet exercice rentre dans le cadre de la théorie plus générale des estimateurs. Le but est toujours de parvenir à estimer des paramètres inconnues d'une loi à partir de plusieurs réalisations de celle-ci. Il peut être intéressant de lire l'introduction donné sur l'article Wikipédia : `https://fr.wikipedia.org/wiki/Estimateur_(statistique)`.

15.4 Graphe aléatoire et Diffusion d'un secret

On considère un ensemble de $n+1$ personnes. Chaque personne choisit un confident aléatoirement et uniformément parmi ses n camarades. On étudie la propagation d'une information. Une seule personne est au courant de l'information au début, puis elle la transmet à son confident, qui fait de même et ainsi de suite jusqu'à ce que ce que l'information ne se propage plus. On note N le nombre de personnes au courant de l'information à la fin de l'expérience aléatoire.

1. Calculer $\mathbb{P}(N > k)$ pour $k \in \mathbb{N}$
2. En déduire $\mathbb{E}(N)$
3. Donner la probabilité p qu'une personne tirée au hasard uniformément soit au courant de l'information.
4. Que devient $\mathbb{E}(N)$ si l'on suppose que x personnes choisies aléatoirement sont initialement au courant ?

Éléments de correction : 1. Pour $k \leq N$, $\mathbb{P}(N > k)\frac{n!}{(n-k)!n^k}$ 2. $E(N) = \sum_{k=0}^{+\infty}\mathbb{P}(\mathbb{N} > \Bbbk)$ puisque N est à valeurs entières. On pourrait ensuite approcher cette espérance numériquement. 3. Décomposer N en somme d'indicatrices 4. Utiliser le résultat de la question 3 pour voir chaque propagation d'information comme une expérience indépendante des autres.

15.5 Aire aléatoire entière

Soit n un entier pair non nul. On note e_1, e_2 la base canonique de $\mathbb{R}^2$ Soit f une fonction qui envoie aléatoirement et uniformément e_1 et e_2 sur deux éléments de $[|0, n|[^2$ Quelle est la probabilité pour que l'aire du triangle formé par 0, $f(e_1)$ et $f(e_2)$ soit entière ?

Source : Merci à Romain Ageron pour l'idée de cet exercice.

Éléments de correction : Utiliser le déterminant pour calculer l'aire, puis raisonner modulo 2, on obtient : 5/8.

15.6 Application à la cuisine

On souhaite cuire n rondelles de carottes à la poêle. Après un certain de temps de cuisson initial, on souhaite retourner les rondelles. On peut pour cela secouer la poêle, cela entraînera le retournement de chaque rondelle avec une probabilité p. Combien de fois faut-il secouer la poêle pour maximiser l'espérance du nombre de carottes retournées ? On suppose que l'on n'adapte pas le nombre de fois où l'on secoue la poêle en fonction du nombre effectif de patates retournées au cours de l'expérience.

15.7 Mécanique quantique, bosons, fermions, principe de Pauli

Cet exercice, très simple d'un point de vue mathématique, a pour but de faire découvrir les aspects élémentaires de la modélisation de plusieurs particules en mécanique quantique.
Une particule quantique peut être mesurée dans n états distincts. On décrit son état par un vecteur X dans $\mathbb{R}^n$ qui représente sa loi de probabilité. La probabilité de mesurer la particule dans l'état i est donnée par $x_i^2/||X||^2$

1. On se donne désormais deux particules qui peuvent chacune être mesurée dans n états. Dans combien d'états peut-on mesurer le système des deux particules ? Comment décrire algébriquement sa loi de probabilité ?
2. On considère deux particules qui sont indépendantes qui ont chacune des lois marginales définies par les vecteurs X et Y. Donner un représentant de la loi jointe en fonction de X et Y.
3. Montrer qu'il existe certains états qui ne peuvent s'écrire sous la forme XY^T (forme factorisée), ces états sont dits intriqués.
4. A cause de l'indiscernabilité des particules, les états physiquement réalisables ne correspondent pas à $M_n(\mathbb{R})$ tout entier pour certaines paires de particules
   (a) Dans le cas des bosons (comme les photons par exemple), il s'agit en fait de $S_n(\mathbb{R})$ (matrices symétriques) seulement. Quelle est la dimension de cet espace ? Quels sont les états de $S_n(R)$ qui peuvent s'écrire sous forme factorisée ? Est-ce que tous les états peuvent s'écrire sous forme factorisée ?
   (b) Dans le cas des fermions (électrons par exemple), les états accessibles correspondent seulement à $A_n(\mathbb{R})$ (antisymétriques), même questions.
   (c) Démontrer le principe d'exclusion de Pauli : deux fermions ne peuvent jamais être dans le même état quantique avec des lois indépendantes.
5. Démontrer que $S_n(\mathbb{R}) + A_n(\mathbb{R}) = M_n(\mathbb{R})$ et que la somme est orthogonale
6. Dans le cas n=2 (système à deux états), donner une base adaptée à la décomposition précédente et interpréter

Remarque : Ce modèle peut sembler très simple mais décrit parfaitement la plupart des difficultés liées à la modélisation de particules identiques. La seule inexactitude vient du fait que les coefficients sont a priori complexes (ce qui ne change pas grand-chose tant que l'on ne parle pas de l'équation de Schrodinger). Pour généraliser à plus que 2 particules, il est commode d'éliminer la description par matrices (on aurait par exemple un cube de coefficient pour 3 particules) et d'introduire la notion de produit tensoriel.

Éléments de correction : 1. Le couple de particules peut être mesuré dans n^2 états différents. On représentera donc la loi du couple par une matrice (loi jointe) 2. XY^T 3. Considérer le rang. 4c. Une matrice antisymétrique ne peut jamais s'écrire sous forme factorisée sans être nulle.

16 Séries

16.1 Convergence de l'exponentielle matricielle

1. Montrer que $||A|| := \sqrt{Tr(tAA)}$ est une norme sous-multiplicative, c'est-à-dire que $||AB|| < ||A|| * ||B||$
2. Montrer que pour tout coefficient a de A on a : $|a| \leq ||A||$
3. Soit $A \in M_n(\mathbb{R})$, on note B_n les sommes partielles $B_n := \sum_{k=0}^{n} \frac{A^k}{k!}$ Montrer que pour tout i, j dans $[|1, n|]$ $(B_n)_{i,j}$ est une suite de Cauchy.
4. En déduire que B_n converge coefficient par coefficient quand n tend vers l'infini. On note $\exp(A)$ sa limite.
5. Soit N une matrice nilpotente. Montrer que $ln(Id + N)$ est bien définie (par son DL(0)) et que $\exp(ln(Id + N)) = Id + N$

Éléments de correction 1. Majorer chacun des coefficients de AB avec Cauchy-Schwarz puis sommer. 3. Exploiter la convergence de l'exponentielle réelle pour contrôler la différence entre sommes partielles.

16.2 Exponentielle matricielle et groupe de Lie

1. Soit $A_2(\mathbb{R})$ les matrices antisymétriques. Montrer que pour tout $A \in A_2(\mathbb{R})$, $\exp(A) := \sum_{k=0}^{\infty} \frac{A^k}{k!}$ converge coefficient par coefficient vers une limite que l'on précisera.
2. On admet que l'exponentielle converge coefficient par coefficient sur $M_n(\mathbb{R})$. Montrer que $\exp(A_n(\mathbb{R}))$ est inclus dans $O_n(\mathbb{R})$.
3. On va monter que $\exp(A_3(\mathbb{R})) = SO_3(\mathbb{R})$. Pour cela, on commence par réduire $SO_3(\mathbb{R})$
   (a) Soit $O \in SO_3(\mathbb{R})$, montrer qu'il existe $X \in \mathbb{R}_3$ non nul et $a \in R$ tel que $OX = aX$ puis que $|a| = 1$
   (b) Montrer que O stabilise l'orthogonal de $Vect(X)$
   (c) Réduire O en utilisant une base adaptée à X et à son orthogonal
   (d) Montrer que $SO_3(\mathbb{R})$ est inclus $\exp(A_3(\mathbb{R}))$
   (e) Bonus : Montrer qu'il s'agit en fait d'une égalité. *Indication : on pourra faire appel à la trigonalisation matricielle pour calculer le déterminant d'une exponentielle*

Remarques :

1. On a toujours $det(\exp(A)) = \exp(Tr(A))$ pour des matrices à coefficients complexes (par trigonalisation)
2. On retrouve ici un lien très fort entre les matrices antisymétriques et les rotations. Les antisymétriques correspondent à la géométrie locale du groupe des rotations autour de l'identité (espace tangent en l'identité), l'exponentielle permet de "réenrouler" cette version aplatie du groupe sur elle-même. Cela est extrêmement clair dans le plan complexe : Si l'on considère le groupe des complexes unitaires (cercle unité), son espace tangent en 1 est une droite dont la direction est $i * \mathbb{R}$. Si désormais on considère $\exp(i * \mathbb{R})$ on retrouve bien le cercle unité ! En dimension supérieur, ce résultat relie les matrices antisymétriques et les rotations :

   $$\exp(A_n(\mathbb{R})) = SO_n(\mathbb{R})$$

   Il s'agit en fait d'un résultat encore plus général pour les groupes "lisses" de matrices (groupe de Lie). Si l'on considère leur espace tangent en l'identité on obtient un espace vectoriel (algèbre de Lie) (stable par le crochet de Lie, ie : si A et Bsont dans l'algèbre de Lie alors $AB - BA$ aussi). En prenant l'exponentielle de cet espace on retrouve bien le groupe de Lie initial sous certaines hypothèses.

Éléments de correction : 1. On pourra remarquer une certaine structure dans les puissances d'une matrice antisymétrique 2×2 puis invoquer une des expressions en série du cosinus et du sinus. 2. La transposition commute avec l'exponentielle. 3a. Poser le polynôme caractéristique, remarquer que la dimension 3 impose l'existence d'une racine réelle. 3d. Remarquer que $\exp(PAP^{-1}) = P\exp(A)P^{-1}$

16.3 Exponentielle matricielle et formule de Taylor

1. Soit D l'opérateur de dérivation de $\mathbb{R}_n[X]$ dans lui-même, montrer que D est de trace nulle
2. Soit h un réel, montrer qu'il existe A dans $L(\mathbb{R}_n[X])$ tel que $A(P) = P(X + h)$
3. Montrer que $\exp(hD) := \sum_{k=0}^{\infty} \frac{(hD)^k}{k!}$ est bien définie puis que $A = \exp(hD)$
4. Que vaut le déterminant de A ?

Remarque : On démontre ici pour les polynômes une assertion très utilisée en mécanique quantique : « La dérivation est le générateur infinitésimal des translations » c'est-à-dire pour $h \in \mathbb{R}$:

$$\exp(hD)(P) = P(X + h)$$

Par ailleurs, on a toujours la formule remarquable :

$$det(\exp(A)) = \exp(Tr(A))$$

pour des matrices à coefficients complexes (par trigonalisation).

Éléments de correction : 1. Déjà la question a du sens puisque la trace est un invariant de similitude. Ensuite écrire la matrice de D dans une base qui rend le calcul de sa trace aisé. On trouve $Tr(D) = 0$ 2. Remarquer la linéarité de l'opération de translation de l'argument. 3. Utiliser la formule de Taylor pour les polynômes. 4. Dans la base canonique, A est triangulaire supérieure et il est clair que $det(A) = 1$

17 Équations différentielles

17.1 Caustique aquatique

On considère un fond d'aquarium 2D que l'on remplit avec un peu d'eau. On incline l'aquarium, l'eau forme alors un triangle rectangle dont l'hypoténuse correspond à la surface libre. On trace pour différents angles d'inclinaison le segment délimitant la surface de l'eau. Tous les segments tracés sont tangents à une courbe enveloppante. Donner l'équation de cette courbe en supposant que celle-ci est deux fois dérivable.

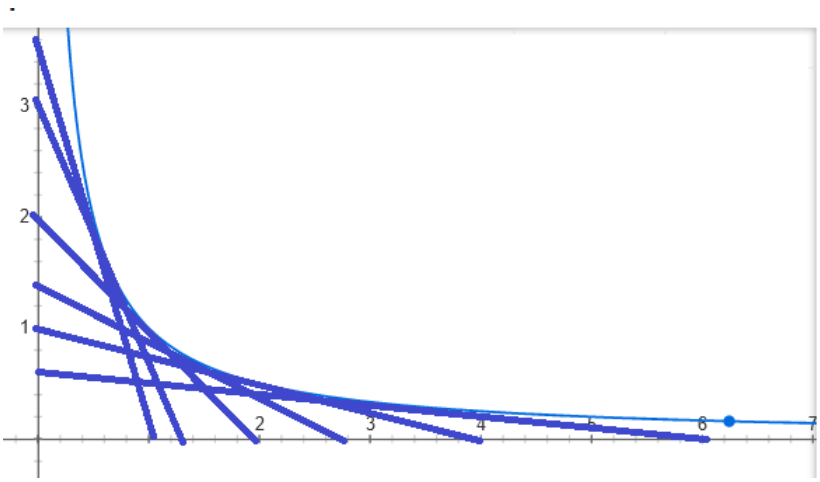

FIGURE 10 – Tracé du niveau d'eau pour plusieurs inclinaisons

Éléments de correction : Tous les segments vérifient une équation de conservation de l'aire. Cela se traduit en une équation différentielle sur l'enveloppe $y(x)$: $(y-y'x)(x-y/y') = cst$ On dérive cette équation pour faire disparaître la constante et on obtient après simplifications :

$$y''(\frac{y^2}{y'^2} - x^2) = 0$$

On retrouve ici les solutions affines ($y'' = 0$) et l'équation différentielle de l'enveloppe : $y^2/y'^2 = x^2$ qui se résout en $y : x \mapsto \frac{A}{x}$.

Remarque : Ce genre de résolution est assez classique quand on recherche l'équation d'une courbe enveloppante. Si on avait considéré le problème additif ou l'on suppose que la somme des intersections avec les axes est maintenue constante, on aurait obtenu : $(y - y'x) + (x - \frac{y}{y'}) = cst$ qui est une équation différentielle de Clairault : `https://fr.wikipedia.org/wiki/%C3%89quation_diff%C3%A9rentielle_de_Clairaut` Il s'agit d'un exemple canonique de résolution de ce genre d'équation.