Oraux ENS 2023-2024 :

Recueil d'exercices et solutions complètes

Mathématiques — Filière MP

Auteurs :

SABIR Ilyass

ZINE Akram

ETTOUSY Badr

Avril 2024

Oraux ENS 2023-2024

SABIR Ilyass - ZINE Akram - ETTOUSY Badr

N.B. : Si vous trouvez des erreurs de français ou de mathématiques, ou si vous avez des questions et/ou des suggestions,
n'hésitez pas à nous contacter en envoyant un mail à :

ilyass@steerai.autos ou **ilyasssabir7@gmail.com**

Ce document a été relu par SABIR Ilyass, ZINE Akram, ainsi que d'autres personnes ayant vérifié certaines solutions.
Un grand merci à tous les membres du groupe **Maths Community** pour leurs efforts dans la relecture de plusieurs parties de ce livre.

Licence

Avant-propos

Ce recueil est bien plus qu'une simple collection d'exercices : il est conçu comme un compagnon de route pour tous les étudiants de prépa aspirant à intégrer les institutions les plus prestigieuses, telles que l'École normale supérieure (ENS) et l'École polytechnique (l'X), mais aussi pour les candidats des autres grandes écoles et concours de haut niveau. Les exercices rassemblés ici ne sont pas des problèmes standards : ils sont tirés d'épreuves orales réelles des concours des années précédentes, garantissant ainsi une immersion totale dans la réalité des défis à venir.

Le niveau de difficulté de chaque exercice peut varier selon l'étudiant, raison pour laquelle nous n'avons pas jugé utile de les classer selon ce critère. En effet, la difficulté perçue est une donnée subjective et dépend largement de votre maîtrise des sujets abordés. C'est pourquoi nous vous encourageons à aborder chaque exercice avec un esprit ouvert, prêt à explorer, à questionner et à approfondir vos connaissances. Nous vous recommandons également de travailler ces exercices dans des conditions aussi proches que possible de celles des oraux : une durée de 50 minutes pour les oraux d'ULM et de 45 minutes pour ceux du concours commun ULSR. Cela vous permettra non seulement de vous habituer à la gestion du temps, mais aussi de simuler l'environnement stressant des épreuves, où chaque minute compte et où la clarté de pensée est cruciale.

La variété des exercices dans ce recueil reflète les multiples facettes des mathématiques enseignées et évaluées lors des concours. Vous trouverez des problèmes d'algèbre, d'analyse, de géométrie, et même des défis en théorie des nombres. Certains exercices mettront à l'épreuve votre capacité à manipuler des objets classiques tels que les wronskiens, les séries alternées ou les matrices antisymétriques. D'autres vous amèneront à plonger plus profondément dans des problématiques actuelles, comme les espaces de translation ou les sous-groupes des isométries affines. Le but n'est pas simplement de résoudre ces problèmes, mais de comprendre les mécanismes sous-jacents qui permettent d'aborder des situations nouvelles avec confiance.

Pour vous soutenir dans cet effort, nous avons également inclus des solutions détaillées en annexe, qui couvrent non seulement les épreuves récentes

de mathématiques A du concours X/ENS 2023 et 2024, mais aussi l'épreuve de mathématiques C du concours X/ENS 2018 et celle de l'agrégation externe de 2019. Ces solutions sont bien plus qu'une simple correction : elles vous guideront pas à pas dans le raisonnement et la méthodologie attendus au plus haut niveau.

En particulier, vous y trouverez une démonstration complète et rigoureuse du théorème de Dirichlet sur les progressions arithmétiques, un résultat fondamental qui revient régulièrement dans les concours. Cette démonstration, issue de l'épreuve ENS Paris-Lyon de 1993, est exposée avec minutie pour que chaque lecteur puisse en saisir tous les rouages, tant au niveau technique qu'intuitif.

En outre, nous vous invitons vivement à consulter les rapports des jurys des concours précédents. Ils vous permettront de mieux comprendre les attentes précises des examinateurs, les qualités qu'ils recherchent et les erreurs fréquentes à éviter. Enfin, en cas de difficulté, n'hésitez pas à recourir à des simplifications ou à des cas particuliers pour clarifier les concepts. Ce travail sur des versions plus abordables d'un problème peut souvent fournir des intuitions précieuses, vous permettant ensuite de revenir à l'énoncé général avec une meilleure compréhension.

La route vers l'excellence est exigeante, mais avec les bonnes méthodes et une persévérance inébranlable, elle est à votre portée. Nous espérons que ce recueil deviendra un compagnon de confiance dans cette aventure et vous aidera à aborder les oraux avec sérénité et confiance.

Bonne préparation, et que vos efforts soient couronnés de succès.

Les auteurs

Table des matières

Première partie

Les exercices posés à l'oral de l'ENS Ulm 2023

⋆⋆⋆

Dans cette première partie, nous allons explorer une série d'exercices extraits des épreuves orales du concours d'entrée à l'ENS ULM. Les sujets abordés couvrent des domaines variés des mathématiques, tels que l'analyse, l'algèbre linéaire et la géométrie. Vous serez confrontés à des problèmes classiques mais exigeants, tels que les Wronskiens et les systèmes de Tchebychev, la minimisation locale sur un graphe, ainsi que des questions de divisibilité dans des contextes algébriques complexes. Chaque exercice a été sélectionné pour refléter la rigueur et l'ingéniosité nécessaires lors des concours, et vous permettre de tester vos connaissances tout en affinant vos méthodes de raisonnement. À travers les résolutions, vous développerez des outils essentiels pour maîtriser des concepts allant des espaces fonctionnels aux propriétés géométriques et algébriques des matrices et groupes.

Vous trouverez l'énoncé des exercices à :

https ://mathexp.eu/lairez/math-ulm-2023.pdf

⋆⋆⋆

L'exercice 1 porte sur les wronskiens et les systèmes de Tchebychev. Il explore les propriétés des déterminants wronskiens et leur application à l'étude des zéros de combinaisons linéaires de fonctions. Cet exercice combine des aspects d'algèbre linéaire et d'analyse, mettant en évidence des liens profonds entre ces domaines.

Exercice 1. (Wronskiens et systèmes de Tchebychev)

Soit $I \subseteq \mathbb{R}$ un intervalle ouvert non vide. Soit $\mathcal{C}^r(I)$ le $\mathbb{R}$-espace vectoriel des fonctions sur I à valeurs réelles continument dérivables r fois. Pour toutes fonctions $f_1, \dots, f_r \in \mathcal{C}^{r-1}(I)$ on définit une fonction $I \to \mathbb{R}$ par :

$$\mathcal{W}[f_1, \dots, f_r](x) = \begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ f_1'(x) & \cdots & f_r'(x) \\ \vdots & & \vdots \\ f_1^{(r-1)}(x) & \cdots & f_r^{(r-1)}(x) \end{vmatrix}$$

1. Montrer que pour toute fonctions $g, f_1, \dots, f_r \in \mathcal{C}^{r-1}(I)$,

$$\mathcal{W}[gf_1, \dots, gf_r](x) = g(x)^r \mathcal{W}[f_1, \dots, f_r](x).$$

2. Soit $f_1, \dots, f_r \in \mathcal{C}^{r-1}(I)$ telles que $\mathcal{W}[f_1, \dots, f_k]$ est strictement positif sur I, pour tout $1 \leq k \leq r$. Montrer que pour tout $a_1, \dots, a_r \in \mathbb{R}$ non tous nuls, la fonction $a_1 f_1 + \cdots + a_r f_r$ admet au plus $r-1$ zéros sur I.

Solution. (SABIR Ilyass)

1. Soient $g, f_1, \dots, f_r \in \mathcal{C}^{r-1}(I)$ et $x \in \mathbb{R}$, on a :

$$\mathcal{W}[gf_1, \dots, gf_r](x) = \begin{vmatrix} (gf_1)(x) & \cdots & (gf_r)(x) \\ (gf_1)'(x) & \cdots & (gf_1)'(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix}$$

Or, pour tout $j,k \in [\![1,r]\!]$, on a :

$$(1) : (gf_j)^{(k)}(x) = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} g^{(i)}(x) f_j^{(k-i)}(x)$$

Donc

$$\begin{aligned}
[gf_1, \dots, gf_r](x) &= g(x) \begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ g(x)f_1'(x) + g'(x)f_1(x) & \cdots & g(x)f_r'(x) + g'(x)f_r(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix} \\
&= g(x) \begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ g(x)f_1'(x) & \cdots & g(x)f_r'(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix} \begin{matrix} \\ \\ \\ \\ L_2 \leftarrow L_2 - g'(x)L_1 \end{matrix} \\
&= g(x)^2 \begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ f_1'(x) & \cdots & f_r'(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix}
\end{aligned}$$

Soit $l \in [\![1, r-2]\!]$, supposons que :

$$\mathcal{W}[gf_1, \dots, gf_r](x) = g(x)^l \begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ f_1'(x) & \cdots & f_r'(x) \\ \vdots & & \vdots \\ f_1^{(l)}(x) & & f_r^{(l)}(x) \\ (gf_1)^{(l+1)}(x) & & (gf_r)^{(l+1)}(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix}$$

Et montrons que :

$$\mathcal{W}[gf_1,\dots,gf_r](x) = g(x)^{l+1}\begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ f_1'(x) & \cdots & f_r'(x) \\ \vdots & & \vdots \\ f_1^{(l+1)}(x) & & f_r^{(l+1)}(x) \\ (gf_1)^{(l+2)}(x) & & (gf_r)^{(l+2)}(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix}$$

Ce qui est évident, en effectuant l'opération $L_{l+1} \leftarrow L_{l+1} - \sum_{i=1}^{l} \begin{pmatrix} l \\ i \end{pmatrix} g^{(i)}(x) L_i$, (Selon (1)).

D'où par récurrence pour tout $l \in [\![1, r-1]\!]$, on a :

$$\mathcal{W}[gf_1,\dots,gf_r](x) = g(x)^{l}\begin{vmatrix} f_1(x) & \cdots & f_r(x) \\ f_1'(x) & \cdots & f_r'(x) \\ \vdots & & \vdots \\ f_1^{(l)}(x) & & f_r^{(l)}(x) \\ (gf_1)^{(l+1)}(x) & & (gf_r)^{(l+1)}(x) \\ \vdots & & \vdots \\ (gf_1)^{(r-1)}(x) & \cdots & (gf_r)^{(r-1)}(x) \end{vmatrix}$$

En particulier, pour $l = r-1$, on a alors :

$$\mathcal{W}[gf_1,\dots,gf_r](x) = g(x)^r \mathcal{W}[f_1,\dots,f_r](x)$$

2. Soient $f_1,\dots,f_r \in \mathcal{C}^{r-1}(I)$ telles que $\mathcal{W}[f_1,\dots,f_k]$ soit strictement positif sur I, pour tout $1 \leq k \leq r$. Soient $a_1,\dots,a_r \in \mathbb{R}$ non tous nuls. Montrons que la fonction $a_1f_1 + \cdots + a_rf_r$ admet au plus $r-1$ zéros sur I.

Commençons par examiner les petites valeurs de r.

Pour $r = 1$, on a pour tout $x \in I$

$$f_1(x) = \mathcal{W}[f_1](x) > 0$$

Donc pour tout $a \not= 0$, on a af_1 n'admet pas de zéros sur I.

Pour $r = 2$**,** on a pour tout $x \in I$,

$$\begin{cases} f_1(x) = \mathcal{W}[f_1](x) > 0 \\ f_2'(x)f_1(x) - f_1'(x)f_2(x) = \mathcal{W}[f_1, f_2](x) > 0 \end{cases}$$

Alors

$$\left(\frac{f_2}{f_1}\right)'(x) = \frac{\mathcal{W}[f_1, f_2](x)}{f_1(x)^2} > 0$$

Soient $a, b \in \mathbb{R}$ non tous nuls, montrons que la fonction $x \in I \longmapsto af_1(x) + bf_2(x)$ admet au plus 1 zéro sur I.

Si $b = 0$, il est clair que la fonction $x \in I \longmapsto af_1(x) + bf_2(x)$ n'admet pas de zéros sur I.

Sinon, les zéros de $x \in I \longmapsto af_1(x)+bf_2(x)$ sont exactement les zéros de la fonction $\gamma : x \in I \longmapsto a+b\frac{f_2(x)}{f_1(x)}$. Or, pour tout $x \in I$, on a $\gamma'(x) = b\left(\frac{f_2}{f_1}\right)'$, ce qui signifie que γ est strictement monotone sur I, par conséquent γ admet au plus un zéro sur I. D'où le résultat.

Dans toute la suite, on suppose que $\boldsymbol{r \geqslant 3}$, Le résultat n'est pas facile à démontrer, donc nous allons prouver dans un premier temps trois lemmes qui nous aideront à répondre à la question.

Définition.

Notons, pour tout $k \in [\![1, r]\!]$

$$\begin{cases} \varphi_1 := \mathcal{W}[f_1] \\ \varphi_2 := \frac{\mathcal{W}[f_1, f_2]}{\mathcal{W}[f_1]^2} \\ \varphi_k := \frac{\mathcal{W}[f_1,\ldots,f_{k-2}]\mathcal{W}[f_1,\ldots,f_k]}{\mathcal{W}[f_1,\ldots,f_{k-1}]^2} \text{ si } 3 \leqslant k \leqslant r \end{cases}$$

Et pour tout $k \in [\![1, r-1]\!]$, on définit l'opérateur différentiel D_k par :

$$D_k.f := \frac{d}{dx}\left(\frac{f}{\varphi_k}\right) \quad , \forall f \in \mathcal{C}^{r-1}(I) \text{ and } D_0.f = f$$

Lemme 1.

On a pour tout $k \in [\![1, r]\!]$

$$D_{k-1}.D_{k-2}\ldots D_1.f_k = \varphi_k$$

Preuve du lemme 1.

Montrons le résultat par récurrence sur $k \in [\![1, r]\!]$.

Le résultat est trivial pour $k = 1, 2$ ($c.f$ le cas $r = 1, 2$).

Soit $k \in [\![3, r]\!]$, supposons que pour tout $i \in [\![1, k-1]\!]$ $D_{i-1} \dots D_1.f_i = \varphi_i$. Montrons que $D_{k-1}.D_{k-2} \dots D_1.f_k = \varphi_k$.

On a d'après la question 1 :

$$\begin{aligned}
\frac{1}{\varphi_1^k}\mathcal{W}[f_1, \dots, f_k] &= \begin{vmatrix} 1 & \frac{f_2}{\varphi_1} & \cdots & \frac{f_k}{\varphi_1} \\ D_1.f_1 & D_1.f_2 & \cdots & D_1.f_k \\ \vdots & & & \vdots \\ D_1.f_1 & D_1.f_2 & \cdots & D_1.f_k \end{vmatrix} \\
&= \begin{vmatrix} 1 & \frac{f_2}{\varphi_1} & \cdots & \frac{f_r}{\varphi_1} \\ 0 & D_1.f_2 & \cdots & D_1.f_r \\ 0 & \frac{d}{dx}D_1.f_2 & & \frac{d}{dx}D_1.f_2 \\ \vdots & & & \vdots \\ 0 & \left(\frac{d}{dx}\right)^{r-2} D_1.f_2 & \cdots & \left(\frac{d}{dx}\right)^{r-2} D_1.f_r \end{vmatrix} \\
&= \mathcal{W}[D_1.f_2, \dots, D_1.f_k]
\end{aligned}$$

Ainsi,

$$\begin{aligned}
\frac{1}{\varphi_2^{k-1}}\mathcal{W}[D_1.f_2, \dots, D_1.f_k] &= \begin{vmatrix} \frac{1}{\varphi_2}D_1.f_2 & \cdots & \frac{1}{\varphi_2}D_1.f_r \\ D_2.D_1.f_2 & & D_2.D_1.f_2 \\ & & \vdots \\ \left(\frac{d}{dx}\right)^{r-3} D_2.D_1.f_2 & \cdots & \left(\frac{d}{dx}\right)^{r-3} D_2.D_1.f_2 \end{vmatrix} \\
&= \begin{vmatrix} 1 & \frac{1}{\varphi_2}D_1.f_3 & \cdots & \frac{1}{\varphi_2}D_1.f_r \\ 0 & D_2.D_1.f_3 & & D_2.D_1.f_2 \\ & & & \vdots \\ 0 & \left(\frac{d}{dx}\right)^{r-3} D_2.D_1.f_3 & \cdots & \left(\frac{d}{dx}\right)^{r-3} D_2.D_1.f_2 \end{vmatrix} \\
&= \mathcal{W}[D_2.D_1.f_3, \dots, D_2.D_1.f_k]
\end{aligned}$$

Ainsi, par récurrence, on a pour tout $j \in [\![0, k-1]\!]$:

$$\frac{1}{\varphi_j^{k-j+1}} \times \dots \times \frac{1}{\varphi_2^{k-1}} \times \frac{1}{\varphi_1^k}\mathcal{W}[f_1, \dots, f_k] = \mathcal{W}[D_j \dots D_1.f_{j+1}, \dots, D_j \dots D_1.f_k]$$

En particulier, pour $j = k-1$, on a :

$$\frac{1}{\varphi_{k-1}^2} \times \dots \times \frac{1}{\varphi_2^{k-1}} \times \frac{1}{\varphi_1^k}\mathcal{W}[f_1, \dots, f_k] = D_{k-1} \dots D_1.f_k$$

Ainsi, $D_{k-1}\dots D_1.f_k$ vaut :

$$\begin{aligned}
&= \mathcal{W}[f_1,\dots,f_k]\prod_{j=1}^{k-1}\frac{1}{\varphi_j^{k-j+1}}\\
&= \mathcal{W}[f_1,\dots,f_k]\times\frac{1}{\mathcal{W}[f_1]^k}\times\left(\frac{\mathcal{W}[f_1]^2}{\mathcal{W}[f_1,f_2]}\right)^{k-1}\times\prod_{j=3}^{k-1}\left(\frac{\mathcal{W}[f_1,\dots,f_{j-1}]^2}{\mathcal{W}[f_1,\dots,f_{j-2}]\mathcal{W}[f_1,\dots,f_j]}\right)^{k-j+1}\\
&= \mathcal{W}[f_1,\dots,f_k]\times\frac{\mathcal{W}[f_1]^{k-2}}{\mathcal{W}[f_1,f_2]^{k-1}}\times\frac{\prod_{j=2}^{k-2}\mathcal{W}[f_1,\dots,f_j]^{2(k-j)}}{\prod_{j=1}^{k-3}\mathcal{W}[f_1,\dots,f_j]^{k-j-1}\times\prod_{j=3}^{k-1}\mathcal{W}[f_1,\dots,f_j]^{k-j+1}}\\
&= \frac{\mathcal{W}[f_1,\dots,f_k]\mathcal{W}[f_1,\dots,f_{k-2}]}{\mathcal{W}[f_1,\dots,f_{k-1}]^2}\\
&= \varphi_k
\end{aligned}$$

D'où le résultat par récurrence.

lemme 2.

Soit $f\in\mathcal{C}^1(I)$ et $k\in[\![1,r-1]\!]$, s'il existe $a<b\in I$ tels que $f(a)=f(b)=0$, alors il existe $c\in]a,b[$ tel que $D_k.f(c)=0$

Preuve du lemme 2.

Trivial, en appliquant le théorème de Rolle à $\frac{f}{\varphi_k}$.

Lemme 3.

Soit $f\in\mathcal{C}^{r-1}(I)$. On suppose que f admet au moins r zéros sur I, alors pour tout $k\in[\![1,r-1]\!]$, on a $D_k.D_{k-1}\dots D_1.f$ admet au moins $r-k$ racines sur I.

Preuve du lemme 3.

Soit $f\in\mathcal{C}^{r-1}(I)$, on suppose que f admet au moins r zéros $\zeta_1<\ldots<\zeta_r$ sur I.

On va montrer le résultat par récurrence finie sur $k\in[\![1,r-1]\!]$.

Pour $k=1$, on a pour tout $j\in[\![1,r-1]\!]$, on a $f(\zeta_j)=f(\zeta_{j+1})=0$. Donc, via le lemme 2, il existe $\tau_j\in]\zeta_j,\zeta_{j+1}[$ tel que $D_1.f(\tau_j)=0$

Ainsi $D_1.f$ admet au moins $r-1$ zéros sur I.

Soit $k\in[\![1,r-2]\!]$, supposons que $D_k.D_{k-1}\dots D_1.f$ admet au moins $r-k$ zéros sur I et montrons que $D_{k+1}.D_k\dots D_1.f$ admet au moins $r-(k+1)$ zéros sur I.

Par le même raisonnement que précédemment, entre deux zéros de $D_k.D_{k-1}\dots D_1.f$, il existe un zéro de $D_{k+1}.D_k\dots D_1.f$.

D'où le résultat.

Revenons à notre question. Montrons que $a_1f_1+\cdots+a_rf_r$ admet au plus $r-1$ zéros sur I.

Par l'absurde, supposons que $a_1f_1+\cdots+a_rf_r$ admet au moins r zéros sur I.

Notons $I=\{k\in[\![1,r]\!], a_i\neq 0\}$ et $i_0=\max(I)$. On a d'après le lemme 1,

$$\begin{aligned} D_{i_0-1}\cdots D_1\left(\sum_{k=1}^{r}a_kf_k\right) &= D_{i_0-1}\cdots D_1\left(\sum_{k\in I}a_kf_k\right)\\ &= \sum_{k\in I\setminus\{i_0\}} a_k\, D_{i_0-1}\cdots D_{k+1}D_{k-1}\cdots D_1f_k + a_{i_0}\, D_{i_0-1}\cdots D_1f_{i_0}\\ &= a_{i_0}\,\varphi_{i_0}\end{aligned}$$

Or, via le lemme 3, $D_{i_0-1}\dots D_1.\left(\sum_{k=1}^{r}a_kf_k\right)$ admet au moins $r-i_0+1\geqslant 1$ zéros sur I.

Ainsi $a_{i_0}.\varphi_{i_0}$ s'annule sur I, absurde avec $\varphi_{i_0}>0$.

D'où $a_1f_1+\cdots+a_rf_r$ admet au plus $r-1$ zéros sur I.

Commentaire. Le résultat de la deuxième question semble intéressant pour caractériser certains types de fonctions.

1- Notons pour tout $i\in[\![1,r]\!]$ $f_i : x\longmapsto x^{i-1}$, on a alors pour tout $k\in[\![1,r]\!]$ et pour tout $x\in\mathbb{R}$

$$\begin{aligned}\mathcal{W}[f_1,\dots,f_k](x) &= \begin{vmatrix} 1 & x & \cdots & & x^{k-1}\\ 0 & 2 & \cdots & & (k-1)x^{k-2}\\ \vdots & & & & \vdots\\ 0 & & & (k-2)! & (k-2)!x\\ 0 & & \cdots & 0 & (k-1)! \end{vmatrix}\\ &= \prod_{i=1}^{k-1} i!\\ &> 0\end{aligned}$$

Donc pour tous $a_1,\dots,a_r$ non tous nuls, on a $x\longmapsto\sum_{k=1}^{r}a_kx^{k-1}$ admet au plus $r-1$ zéros sur $\mathbb{R}$.

Ainsi, pour tout polynôme $P \in \mathbb{R}[X]$ non nul, P admet au plus $\deg(P)$ racines sur $\mathbb{R}$.

2- Soient $t_1 < \cdots < t_r \in \mathbb{R}$

Pour tout $i \in [\![1, r]\!]$, et pour tout $f_k : x \longmapsto e^{t_k x}$, on a alors pour tout $k \in [\![1, r]\!]$ et pour tout $x \in \mathbb{R}$

$$\begin{aligned} \mathcal{W}[f_1, \ldots, f_k](x) &= e^{(t_1+\cdots+t_k)x} \begin{vmatrix} 1 & 1 & \cdots & 1 \\ t_1 & t_2 & \cdots & t_k \\ \vdots & & & \vdots \\ t_1^{k-1} & t_k^{k-1} & \cdots & t_k^{k-1} \end{vmatrix} \\ &= e^{(t_1+\cdots+t_k)x} \prod_{1 \leqslant i < j \leqslant k} (t_j - t_i) \\ &> 0 \end{aligned}$$

Ainsi pour tous $a_1, \ldots, a_r$ non tous nuls, on a $x \longmapsto \sum_{k=1}^{r} a_k e^{t_k x}$ admet au plus $r-1$ zéros sur $\mathbb{R}$.

✠✠✠✠✠✠✠

L'exercice 2 traite d'une propriété de divisibilité concernant le cardinal du groupe des matrices inversibles modulo un nombre premier. Il demande de démontrer que le cardinal de $GL_{n-1}(\mathbb{Z}/p\mathbb{Z})$ est divisible par n, pour $n \geq 3$ et p premier impair. Cet exercice combine des éléments d'algèbre linéaire et de théorie des groupes, avec une touche d'arithmétique modulaire.

Exercice 2. (Une propriété de divisibilité du cardinal des matrices inversibles modulo p)

Soit p un entier premier impair, et $n \geq 3$ un entier. Montrer que n divise le cardinal du groupe $\mathrm{GL}_{n-1}(\mathbb{Z}/p\mathbb{Z})$ des matrices inversibles de taille $n-1$ à coefficients dans $\mathbb{Z}/p\mathbb{Z}$.

Solution. (SABIR Ilyass)

Soient p un nombre premier impair, et $n \geqslant 3$ un entier.

Une matrice $M \in \mathcal{M}_{n-1}(\mathbb{Z}/p\mathbb{Z})$ est inversible si et seulement si les colonnes de M forment une famille libre.

On a $p^{n-1}-1$ possibilités de choisir la première colonne, pour tout $k \in [\![1, n-2]\!]$, si on choisit les k premiers colonnes, alors la $(k+1)$-ème colonne ne doit pas être une combinaison linéaire des k premiers colonnes. Donc on a $p^{n-1}-p^k$ possibilités pour choisir la $(k+1)-$è me colonne.

D'où

$$\mathrm{Card}(\mathrm{GL}_{n-1}(\mathbb{Z}/p\mathbb{Z})) = \prod_{k=0}^{n-2}(p^{n-1}-p^k)$$

Donc, il suffit de montrer que n divise le produit $\prod_{k=0}^{n-2}(p^{n-1}-p^k)$.

On a

$$\begin{aligned}\prod_{k=0}^{n-2}(p^{n-1}-p^k) &= \prod_{k=0}^{n-2}p^k(p^{n-k-1}-1)\\ &= p^{\frac{(n-2)(n-1)}{2}}\prod_{k=0}^{n-2}(p^{n-k-1}-1)\end{aligned}$$

Or, le théorème fondamental de l'arithmétique assure l'existence de $k, q \in \mathbb{N}$ tels que

$$n = p^k q \text{ and } p \wedge q = 1$$

Puisque $k < \frac{(n-2)(n-1)}{2}$, alors p^k divise $\prod_{k=0}^{n-2}(p^{n-1}-p^k)$.

Montrons maintenant que q divise $\prod_{k=0}^{n-2}(p^{n-1}-p^k)$ pour conclure.

Sans perte de généralité, on peut supposer que $q \geqslant 2$.

On a d'après le théorème de Fermat-Euler,

$$p^{\varphi(q)} = 1 (\mathrm{mod}\, q)$$

Avec $\varphi(q) \leqslant q \leqslant n-2$, alors

$$p^{n-1} = p^{\varphi(q)}p^{n-1-\varphi(q)} = p^{n-1-\varphi(q)} (\mathrm{mod}\, q)$$

Ainsi q divise $p^{n-1}-p^{n-1-\varphi(q)}$, et donc q divise $\prod_{k=0}^{n-2}(p^{n-1}-p^k)$.

Par suite q divise $\prod_{k=0}^{n-2}(p^{n-1}-p^k)$.

Or $p \wedge q = 1$, alors $p^k \wedge q = 1$, donc d'après le lemme d'Euclide $n = p^k q$ divise $\prod_{k=0}^{n-2}(p^{n-1}-p^k)$.

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice porte sur la minimisation locale sur un graphe. Il explore une méthode probabiliste pour trouver un minimum local d'une fonction définie sur un ensemble fini, en utilisant un échantillonnage aléatoire suivi d'une descente locale. L'exercice demande de prouver que cette méthode a une probabilité d'au moins 1/2 de trouver un minimum local.

Exercice 3. (Minimisation locale sur un graphe)

Soit E un ensemble fini et $V : E \to \mathcal{P}(E)$ une fonction de E vers les parties de E. Soit $f : E \to \mathbb{R}$ une fonction. Un point $a \in E$ est un *minimum local* si $f(a) \leq f(b)$ pour tout $b \in V(a)$.

Soit M un entier tel que $M \geq \sqrt{\#E}$. Soient $b_1, \ldots, b_M$ des variables aléatoires indépendantes et uniformément distribuées dans E. Soit k tel que $f(b_k) = \min_{1 \leq i \leq M} f(b_i)$.

Soit $(u_n)_{n \geq 0}$ une suite de E telle que $u_0 = b_k$ et pour tout $n \geq 0$:

- si u_n est un minimum local, alors $u_{n+1} = u_n$;
- sinon, $u_{n+1} \in V(u_n)$ et $f(u_{n+1}) < f(u_n)$.

Montrer que u_M est un minimum local avec probabilité au moins 1/2.

Solution. (SABIR Ilyass)

On cherche à montrer que $u_M$est un minimum local avec une probabilité au moins $\frac{1}{2}$.

Quitte à munir E d'une relation d'ordre, on peut supposer sans perte de généralité, que $E = [\![1, n]\!]$ et f est croissante sur E.

Nous cherchons à montrer que la probabilité de l'événement

$$\mathcal{E} = \{e \in E \mid u_M(e) \text{ est un minimum local}\}$$

est 1/2.

Soit $e \not\in \mathcal{E}$, alors u_M n'est pas un minimum local, et donc il existe $k \in [\![1, M]\!]$ et $(u_0, \ldots, u_M) \in E$ tels que :

$$u_0 = b_k(e), \quad f(b_k(e)) = \min_{1 \leqslant i \leqslant M} f(b_i(e)) \text{ and pour tout } i \in [\![0, M-1]\!], f(u_{i+1}) < f(u_i)$$

On a alors :

$$f(u_M) < f(u_{M-1}) < \cdots < f(u_1) < f\left(\min_{1\leqslant i\leqslant M} b_i(e)\right)$$

Par croissance de f, on a alors :

$$u_M < u_{M-1} < \cdots < u_1 < \min_{1\leqslant i\leqslant M} b_i(e)$$

Par suite $\min\limits_{1\leqslant i\leqslant M} b_i(e) \geqslant M+1$ (car $u_M, \ldots, u_1 \in \mathbb{N}$), en particulier

$$\bar{\mathcal{E}} \subset \{\min(b_1, \ldots, b_M) \geqslant M+1\} = \bigcap_{i=1}^{M} \{b_i \geqslant M+1\}$$

Ainsi par indépendance entre les variables $b_1, \ldots, b_M$, on a :

$$\begin{aligned} \mathbb{P}(\mathcal{E}) &= 1 - \mathbb{P}(\bar{\mathcal{E}}) \\ &\geqslant 1 - \prod_{i=1}^{M} \mathbb{P}(b_i \geqslant M+1) \\ &\geqslant 1 - \left(1 - \frac{M}{n}\right)^M \end{aligned}$$

Or $x \longmapsto (1-\frac{x}{n})^x = \exp\left(x \ln\left(1-\frac{x}{n}\right)\right)$ est décroissante sur $[0, n]$, en particulier

$$\mathbb{P}(\mathcal{E}) \geqslant 1 - \left(1 - \frac{1}{\sqrt{n}}\right)^{\sqrt{n}} \geqslant 1 - e^{-1} > \frac{1}{2}$$

D'où le résultat.

✠✠✠✠✠✠✠

L'exercice 4 s'intéresse à l'espace des translatées d'une fonction. Il examine les propriétés d'approximation d'un espace engendré par les translations entières d'une fonction intégrable. L'exercice demande de prouver un résultat d'approximation uniforme à partir d'une hypothèse d'approximation en norme L_1.

Exercice 4. (Espace des translatées d'une fonction)

Soit $g \in \mathcal{C}(\mathbb{R})$ une fonction intégrable. Pour $A \subseteq \mathbb{Z}$, on note $\mathcal{S}_A$ le sous-espace vectoriel de $\mathcal{C}(\mathbb{R})$ engendré par les fonctions $x \mapsto g(x-a)$, avec $a \in A$. On suppose que pour toute $f \in \mathcal{C}(\mathbb{R})$ intégrable et tout $\epsilon > 0$, il existe $h \in \mathcal{S}_{\mathbb{Z}}$ telle que

$$\int_{\mathbb{R}} |f(x) - h(x)| \mathrm{d}x < \epsilon.$$

Montrer que pour toute $f \in \mathcal{C}(\mathbb{R})$ intégrable et tout $\epsilon > 0$, il existe $L > 0$ tel que pour tout $y \in \mathbb{R}$, il existe $A \subset \mathbb{Z}$ et $h \in \mathcal{S}_A$ tels que

$$\#A \leq L \text{et } \int_{\mathbb{R}} |f(x-y) - h(x)| \mathrm{d}x < \epsilon.$$

Solution. (Zine Akram)

Pour tout $\varepsilon > 0$, il existe $R > 0$ tel que :

$$\int_{|x|>R} |f(x)|\, dx < \frac{\varepsilon}{4}.$$

Par définition de l'intégrale.

Considérons le domaine $[-R-1, R+1]$, qui est compact. Comme f est continue sur ce domaine compact, elle y est uniformément continue. Donc, il existe $\delta > 0$ tel que pour tous $x, x' \in [-R-1, R+1]$, si $|x-x'| < \delta$, alors :

$$|f(x) - f(x')| < \frac{\varepsilon}{4R}.$$

Nous voulons montrer que l'application $r \mapsto f(-r)$ est continue de $[0,1]$ dans $L^1(\mathbb{R})$.

Pour tout $r_0 \in [0,1]$ et tout $\eta > 0$, choisissons $\delta > 0$ tel que pour $|r - r_0| < \delta$:

- Sur $|x| \leq R$: Pour $x \in [-R, R]$ et $r, r_0 \in [0,1]$, $x - r$ et $x - r_0$ appartiennent à $[-R-1, R+1]$.

Donc,

$$|f(x-r) - f(x-r_0)| < \frac{\varepsilon}{4R}.$$

Ainsi,

$$\int_{-R}^{R} |f(x-r) - f(x-r_0)|\, dx \leq (2R) \times \frac{\varepsilon}{4R} = \frac{\varepsilon}{2}.$$

- Sur $|x| > R$: Comme f est intégrable et tend vers 0 à l'infini :

$$\int_{|x|>R} |f(x-r)|\,dx < \frac{\varepsilon}{4}, \quad \int_{|x|>R} |f(x-r_0)|\,dx < \frac{\varepsilon}{4}.$$

Par l'inégalité triangulaire :

$$\int_{|x|>R} |f(x-r)-f(x-r_0)|\,dx \leq \int_{|x|>R} |f(x-r)|\,dx + \int_{|x|>R} |f(x-r_0)|\,dx < \frac{\varepsilon}{2}.$$

Somme des deux contributions :

$$\begin{aligned} \int_{\mathbb{R}} |f(x-r)-f(x-r_0)|\,dx &= \int_{-R}^{R} |f(x-r)-f(x-r_0)|\,dx + \int_{|x|>R} |f(x-r)-f(x-r_0)dx \\ &< \frac{\varepsilon}{2}+\frac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

Cela montre que l'application $r \mapsto f(-r)$ est continue de $[0,1]$ dans $L^1(\mathbb{R})$.

L'intervalle $[0,1]$ est compact. L'image de $[0,1]$ par l'application continue $r \mapsto f(-r)$ est donc un ensemble compact dans $L^1(\mathbb{R})$. Par le théorème de Heine-Borel, cet ensemble compact peut être couvert par un nombre fini de boules de rayon $\varepsilon/2$ dans $L^1(\mathbb{R})$.

Autrement dit, il existe un entier N et des points $r_1, r_2, \ldots, r_N \in [0,1]$ tels que pour tout $r \in [0,1]$, il existe r_i avec :

$$\int_{\mathbb{R}} |f(x-r)-f(x-r_i)|\,dx < \frac{\varepsilon}{2}.$$

Par hypothèse, pour chaque $f(x-r_i)$ et pour ε, il existe $h_i \in S_{\mathbb{Z}}$ tel que :

$$\int_{\mathbb{R}} |f(x-r_i)-h_i(x)|\,dx < \frac{\varepsilon}{2}.$$

Chaque h_i est une combinaison linéaire finie de fonctions de la forme $g(x-a)$ avec $a \in \mathbb{Z}$. Notons $A_i \subset \mathbb{Z}$ l'ensemble des a utilisés dans h_i, et $L = \max\limits_{1\leq i\leq N} \#A_i$.

Pour un $y \in \mathbb{R}$ arbitraire, écrivons $y = n + r$, avec $n \in \mathbb{Z}$ et $r \in [0,1[$. D'après ce qui précède, il existe r_i tel que :

$$\int_{\mathbb{R}} |f(x-r)-f(x-r_i)|\,dx < \frac{\varepsilon}{2}.$$

Posons $h(x) = h_i(x-n)$. Alors, h appartient à S_A avec $A = A_i + n = \{a+n : a \in A_i\} \subset \mathbb{Z}$.

Le nombre de termes dans h est $\#A = \#A_i \leq L$.

On en conclut que pour tout $y \in \mathbb{R}$, il existe un ensemble $A \subset \mathbb{Z}$ avec $\#A \leq L$ et une fonction $h \in S_A$ telle que :

$$\int_{\mathbb{R}} |f(x-y) - h(x)|\, dx < \varepsilon.$$

✠✠✠✠✠✠✠

Cet exercice traite de la limite d'une série alternée. Il demande d'étudier la convergence et la limite d'une série alternée formée à partir d'une fonction décroissante tendant vers zéro. L'exercice combine des aspects d'analyse réelle et de théorie des séries.

Exercice 5. (Limite d'une série alternée)

Soit $f \in \mathcal{C}^1(\mathbb{R})$ décroissante et tendant vers 0 en $+\infty$. Montrer que la fonction

$$g(x) = \sum_{n=0}^{\infty} (-1)^n f(nx)$$

est bien définie pour $x > 0$. Donner sa limite en 0.

Solution. (ETTOUSY Badr)

Soit $x > 0$, on a $(f(nx))_{n\in\mathbb{N}}$ est une suite de réels positifs, décroissante et tendant vers 0. D'après le critère spécial des séries alternées, on a g est bien définie.

De plus :

$$\begin{aligned}
g(x) - \frac{1}{2}f(0) &= \sum_{k=0}^{+\infty} (f(2kx) - f((2k+1)x)) + \frac{1}{2}\int_0^{+\infty} f'(t)\,\mathrm{d}t \\
&= -\sum_{k=0}^{+\infty} \int_{2kx}^{(2k+1)x} f'(t)\,\mathrm{d}t + \frac{1}{2}\sum_{k=0}^{+\infty} \int_{2kx}^{(2k+2)x} f'(t)\,\mathrm{d}t \\
&= -\frac{1}{2}\sum_{k=0}^{+\infty} \left(\int_{2kx}^{(2k+1)x} f'(t)\,\mathrm{d}t - \int_{(2k+1)x}^{(2k+2)x} f'(t)\,\mathrm{d}t \right) \\
&= -\frac{1}{2}\sum_{k=0}^{+\infty} \int_{2kx}^{(2k+1)x} (f'(t) - f'(t+x))\,\mathrm{d}t
\end{aligned}$$

Par conséquent :

$$\begin{aligned}|g(x)-\frac{1}{2}f(0)| &\leqslant \frac{1}{2}\sum_{k=0}^{+\infty}\int_{2kx}^{(2k+1)x}|f'(t+x)-f'(t)|\,\mathrm{d}t\\ &\leqslant \frac{1}{2}\sum_{k=0}^{+\infty}\int_{2kx}^{(2k+2)x}|f'(t+x)-f'(t)|\,\mathrm{d}t\\ &\leqslant \frac{1}{2}\int_{0}^{+\infty}|f'(t+x)-f'(t)|\,\mathrm{d}t\end{aligned}$$

Soient $\varepsilon>0$ et $A>0$ suffisamment grand pour que :

$$\int_A^{+\infty}|f'(t)|\,\mathrm{d}t=\int_A^{+\infty}(-f'(t))\,\mathrm{d}t=f(A)\leq\frac{\varepsilon}{3}$$

Pour $x>0$, il en découle que :

$$\int_A^{+\infty}|f'(t+x)-f'(t)|\,\mathrm{d}t\leq\int_{A+x}^{+\infty}|f'(t)|\,\mathrm{d}t+\int_A^{+\infty}|f'(t)|\,\mathrm{d}t\leq\frac{2\varepsilon}{3}$$

Comme f' est continue sur le segment $[0,A+1]$, elle y est uniformément continue. Il existe donc $\alpha\in]0,1]$ tel que :

$$\forall(x,t)\in[0,A]\times]0,\alpha],\quad |f'(t+x)-f'(t)|\leq\frac{\varepsilon}{3A}$$

D'où, pour tout $x\in]0,\alpha]$:

$$\begin{aligned}|g(x)-\frac{1}{2}f(0)| &= \int_0^A|f'(t+x)-f'(t)|\,\mathrm{d}t+\int_A^{+\infty}|f'(t+x)-f'(t)|\,\mathrm{d}t\\ &\leqslant \int_0^A\frac{\varepsilon}{3A}\,\mathrm{d}t+\frac{2\varepsilon}{3}\\ &= \varepsilon\end{aligned}$$

D'où $g(x)\underset{x\to0}{\to}\frac{1}{2}f(0)$.

✠✠✠✠✠✠✠

Cet exercice traite des unions dénombrables d'ensembles fermés. Il demande de prouver que l'intervalle ouvert$]0,1[$ne peut pas être écrit comme union dénombrable d'intervalles fermés disjoints d'intérieur non vide, puis d'étendre ce résultat au carré ouvert $]0,1[^2$ pour des disques fermés. L'exercice fait appel à des notions de topologie et de théorie de la mesure.

Exercice 6. (Unions de fermés)

Montrer que $]0,1[$ n'est pas l'union d'un nombre dénombrable d'intervalles fermés disjoints d'intérieur non vide.
Montrer que le carré ouvert $]0,1[^2$ n'est pas l'union d'un nombre dénombrable de disques fermés.

Solution. (SABIR Ilyass)

Pour répondre aux deux parties de l'exercice, on va montrer la généralisation suivante :

Généralisation de l'exercice :

Pour tout $n \in \mathbb{N}^*$, on a $]0,1[^n$ n'est pas l'union d'une suite dénombrable de fermées non vide deux à deux disjoints.

Soit $n \in \mathbb{N}^*$, Raisonnons par l'absurde en supposant que $]0,1[^n$ peut être décomposé en une union dénombrable de fermés non vides deux à deux disjoints, et montrons que cela conduit à une contradiction avec la propriété de connexité de $]0,1[^n$.

Supposons qu'il existe une famille dénombrable $(F_k)_{k\in\mathbb{N}}$ de sous-ensembles tels que :

— Pour tout $k \in \mathbb{N}$, $F_k \subset]0,1[^n$ est fermé dans $]0,1[^n$ et non vide.
— Pour tout $k, l \in \mathbb{N}$ avec $k \neq l$, $F_k \cap F_l = \emptyset$ (ils sont deux à deux disjoints).
— $]0,1[^n = \bigcup_{k=1}^{\infty} F_k$ (leur union est $]0,1[^n$).

Pour aboutir à une contradiction, on va utiliser le lemme suivant, qui présente une propriété fondamentale des espaces connexes.

Lemme 1.

Dans un espace connexe, la seule façon de le partitionner en fermés disjoints est que l'un des fermés soit l'espace entier et les autres soient vides. En d'autres termes, un espace connexe ne peut pas être décomposé en une union de plusieurs fermés non vides deux à deux disjoints.

Preuve du lemme 1.

Supposons que X est un espace topologique connexe, et qu'il existe une famille $(F_i)_{i\in I}$ de fermés de X tels que :

— Pour tout $i \in I$, F_i est fermé dans X et non vide.

— Les F_i sont deux à deux disjoints : $F_i \cap F_j = \emptyset$ pour $i \neq j$.

— Leur union est l'espace : $X = \bigcup_{i \in I} F_i$.

On va montrer que nécessairement un seul des F_i est égal à X et que les autres sont vides.

Supposons par l'absurde qu'il existe au moins deux fermés non vides disjoints F_1 et F_2 dans X.

Considérons les ensembles $A = F_1$ et $B = X \setminus F_1 = \bigcup_{i \in I} F_i$.

— A est fermé dans X (par hypothèse).

— B est l'union de fermés (les F_i pour $i \neq 1$), donc fermé dans X.

— A et B sont disjoints (puisque les F_i sont deux à deux disjoints).

— De plus, $A \cup B = X$.

Ainsi, nous avons partitionné X en deux fermés disjoints non vides A et B.

Selon la définition de la connexité, un espace connexe ne peut pas être partitionné en deux fermés disjoints non vides.

Cette situation contredit donc la connexité de X.

Donc, il n'est pas possible qu'il y ait au moins deux fermés non vides disjoints dans une telle partition de X.

Par suite, un seul des F_i est égal à X, et les autres F_i sont vides.

Revenons à notre hypothèse initiale sur $]0,1[^n$.

On a supposé que $]0,1[^n$ est décomposé en une union dénombrable de fermés non vides deux à deux disjoints $(F_k)_{k \in \mathbb{N}}$.

Puisque $]0,1[^n$ est un espace connexe (étant un ouvert connexe de $\mathbb{R}^n$), la propriété démontrée s'applique.

Selon cette propriété, il devrait y avoir un unique F_k égal à $]0,1[^n$ et les autres F_k seraient vides.

Cependant, par hypothèse, tous les F_k sont non vides, ce qui est en contradiction avec la conclusion de la propriété.

Ainsi, il est donc impossible que $]0,1[^n$ soit l'union dénombrable de fermés non vides deux à deux disjoints.

✠✠✠✠✠✠✠

L'exercice 7 porte sur une inégalité isopérimétrique discrète. Il demande de prouver une inégalité impliquant l'espérance de la valeur absolue de la différence entre une fonction sur un groupe abélien fini et sa moyenne. Cet exercice fait appel à des techniques de théorie des probabilités et d'analyse fonctionnelle discrète.

Exercice 7. (Une inégalité isopérimétrique discrète)

Soient n et d des entiers strictement positifs et $G = (\mathbb{Z}/n\mathbb{Z})^d$. Soit $S = \{\pm e_1, \dots, \pm e_d\}$, où $e_i = (0, \dots, 0, 1, 0, \dots, 0) \in G$, avec le 1 en i^{e} position. Soient X une variable aléatoire uniformément distribuée dans G et $f : G \to \mathbb{R}$ une fonction. Montrer que

$$\mathbb{E}[|f(X) - \mathbb{E}[f(X)]|] \leq \frac{dn}{2} \max_{s \in S} \mathbb{E}[|f(X) - f(X+s)|].$$

Solution. (ETTOUSY Badr)

D'après le théorème de transfert, on a :

$$\begin{aligned} \mathbb{E}[|f(X) - \mathbb{E}[f(X)]|] &= \frac{1}{n^d} \sum_{x \in G} \left| f(x) - \frac{1}{n^d} \sum_{y \in G} f(y) \right| \\ &\leqslant \frac{1}{n^{2d}} \sum_{x \in G} \sum_{y \in G} |f(x) - f(y)| \end{aligned}$$

Pour tout $z \in G$, l'application $y \longmapsto y + x$ est une bijection de G. Donc, on a :

$$\sum_{x \in G} \sum_{y \in G} |f(x) - f(y)| = \sum_{x \in G} \sum_{y \in G} |f(x) - f(x+y)|$$

Puisque G est fini, alors l'application $y \in G \longmapsto \frac{1}{n^d} \sum\limits_{x \in G} |f(x) - f(x+y)|$ est bornée et atteint ses bornes. En particulier il existe $y_0 \in G$ tel que :

$$\frac{1}{n^d} \sum_{y \in G} |f(x) - f(x+y_0)| = \max_{y \in G} \frac{1}{n^d} \sum_{y \in G} |f(x) - f(x+y)| := M$$

Pour conclure, il suffit de montrer que :

$$\frac{1}{n^d} \sum_{y \in G} |f(x) - f(x+y_0)| \leqslant \frac{nd}{2} \max_{s \in S} \mathbb{E}[|f(X) - f(X+s)|]$$

Soit $y \in G$ et $\varepsilon_i \in \{-1, 1\}$ pour tout $i \in [\![1, d]\!]$, on a

$$\begin{aligned}\frac{1}{n^d}\sum_{y\in G}|f(x)-f(x+y+\varepsilon_i e_i)| &\leqslant \frac{1}{n^d}\sum_{y\in G}|f(x+y)-f(x+y+\varepsilon_i e_i)| + \frac{1}{n^d}\sum_{y\in G}|f(x)-f(x+y)| \\ &\leqslant \frac{1}{n^d}\sum_{y\in G}|f(y)-f(y+\varepsilon_i e_i)| + M\end{aligned}$$

Notons $z = \sum_{i=1}^{d} \varepsilon_i u_i e_i$, avec $\varepsilon_1, \ldots, \varepsilon_d \in \{\pm 1\}$ et $u_1, \ldots, u_d \in [\![0, \lfloor \frac{n}{2} \rfloor]\!]$. On a, pour tout $i \in [\![1, d]\!]$,

$$\begin{aligned}\frac{1}{n^d}\sum_{y\in G}|f(y)-f(y+\varepsilon_i u_i e_i)| &= \sum_{i=1}^{d}|u_i| \times M \\ &\leqslant \frac{n \times d}{2} M\end{aligned}$$

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice propose une caractérisation des matrices antisymétriques. Il demande de prouver qu'une matrice carrée de taille impaire est antisymétrique si et seulement si son déterminant s'annule lorsqu'on lui ajoute toute matrice antisymétrique. L'exercice fait appel à des notions d'algèbre linéaire et de théorie des déterminants.

Exercice 8. (Une caractérisation des matrices antisymétriques)

Soit n entier positif impair. Soit $A \in \mathcal{M}_n(\mathbb{R})$ telle que, pour toute matrice antisymétrique $M \in \mathcal{M}_n(\mathbb{R})$, $\det(A+M) = 0$. Montrer que A est antisymétrique.

Solution. (ZINE Akram, SABIR Ilyass)

Méthode 1. (ZINE Akram)

Posons $A = B + C$, avec $B = \frac{1}{2}(A + A^T)$ et $C = \frac{1}{2}(A - A^T)$.

Puisque $n$est impair, alors il existe $U \in \mathrm{GL}_{n-1}(\mathbb{R})$. Il suffit de prendre,

par exemple :

$$U = \begin{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \cdots & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} & & \vdots \\ \vdots & & & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \cdots & \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \end{pmatrix}$$

Pour tout $x \in \mathbb{R}$, posons $V_x = x\,\mathrm{diag}(0, U)$.

Puisque B est symétrique, alors d'après le théorème spectral, B est orthogonalement diagonalisable, alors il existe une matrice diagonale $D = \mathrm{diag}(d_1, \ldots, d_n)$ avec $d_1, \ldots, d_n \in \mathbb{R}$, et $P \in \mathcal{O}_n(\mathbb{R})$, telle que $B = PDP^T$.

Pour tout $x \in \mathbb{R}$, posons $M := -C + PV_xP^T$. On a alors :

$$\det(D + V_x) = \det(A + M) = 0$$

Si $D \neq 0$, on peut supposer sans perte de généralité que $d_1 \neq 0$ (Il suffit de permuter les colonnes de P).

On a alors $\det(D + V_x)$ est un polynôme en $x$de degré $n - 1$.

Ainsi, il exite un $x_0 \in \mathbb{R}$ tel que $\det(D + V_{x_0}) \neq 0$, ce qui est absurde.

D'où $D = 0$, et par suite $A^T = -A$. Donc, A est antisymétrique.

Méthode 2. (SABIR Ilyass)

Soit $B = \frac{1}{2}(A + A^T)$, la question revient à prouver que $B = 0$.

Puisque pour toute matrice antisymétrique $M \in \mathcal{M}_n(\mathbb{R})$, $\det(A + M) = 0$, alors pour tout toute matrice antisymétrique $M \in \mathcal{M}_n(\mathbb{R})$, $\det(B + M) = 0$. (✠)

De plus B est orthogonalement diagonalisable, donc si B est orthogonalement semblable à $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, où $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.

La question revient à montrer que pour toute matrice antisymétrique $M \in \mathcal{M}_n(\mathbb{R})$

$$\det(M + \mathrm{diag}(\lambda_1, \ldots, \lambda_n)) = 0$$

Alors $\lambda_1 = \cdots = \lambda_n = 0$.

Lemme 1.

Le polynôme

$$\Psi(X) := \det(XI_n - \mathrm{diag}(\lambda_1, \ldots, \lambda_n)) = \prod_{i=1}^{n}(X - \lambda_i)$$

est impair.

Preuve du lemme 1.

Soit $a \neq 0$, on a :

$$Q(X) := \begin{vmatrix} \lambda_1 + X & a + X & a + X & \ldots & a + X \\ -a + X & \lambda_2 + X & a + X & \ldots & a + X \\ -a + X & -a + X & \lambda_3 + X & & \vdots \\ \vdots & \vdots & & & a + X \\ -a + X & & & -a + X & X + \lambda_n \end{vmatrix}$$

Q est polynôme de degré inférieur ou égal à 1, (il suffit de retrancher la première ligne à toutes les autres lignes par exemple).

Donc il existe $\alpha, \beta \in \mathbb{R}$ tels que $Q(X) = \alpha + \beta X$.

On a

$$\begin{cases} Q(a) = -\Psi(-a) \\ Q(-a) = -\Psi(a) \end{cases}$$

En particulier

$$Q(0) = \alpha = -\frac{1}{2}(\Psi(-a) + \Psi(a))$$

Or $Q(0) = 0$ (D'après (✠)).

D'où $\Psi(-a) = -\Psi(a)$.

Par continuité, pour tout $a \in \mathbb{R}$, on a : $\Psi(-a) = -\Psi(a)$.

D'où Ψ est impair.

Donc pour tout $i \in [\![1, n]\!]$,il existe $j \in [\![1, n]\!]$ on a $\lambda_j = -\lambda_i$.

Quitte à réarranger les valeurs propres (cela revient à permuter la base de diagonalisation), on peut supposer sans perte de généralité que pour tout $k \in [\![1, \frac{n-1}{2}]\!]$ $\lambda_{2k-1} = -\lambda_{2k} \geqslant 0$ et $\lambda_n = 0$.

Notons

$$P_n(X|\lambda_1,\dots,\lambda_n) := \begin{vmatrix} \lambda_1 & X & 0 & & 0 \\ -X & \lambda_2 & X & & \\ 0 & -X & & & 0 \\ & & & & X \\ 0 & & 0 & -X & \lambda_n \end{vmatrix}$$

Par développement suivant la première ligne, on a

$$P_n(X|\lambda_1,\dots,\lambda_n) = \lambda_1 P_{n-1}(X|\lambda_2,\dots,\lambda_n) + X^2 P_{n-2}(X|\lambda_2,\dots,\lambda_n)(\star)$$

Regardons les petites valeurs de n.

Pour $n=1$, $P_1(X|\lambda_1)=\lambda_1$,

Pour $n=2$, on a $P_2(X|\lambda_1,\lambda_2)=\lambda_1\lambda_2+X^2$

Pour $n=3$, on a $P_3(X|\lambda_1,\lambda_2,\lambda_3)=\lambda_1\lambda_2\lambda_3+(\lambda_1+\lambda_3)X^2$

Pour $n=4$, on a $P_4(X|\lambda_1,\lambda_2,\lambda_3,\lambda_4)=\lambda_1\lambda_2\lambda_3\lambda_4+(\lambda_1\lambda_2+\lambda_1\lambda_4+\lambda_3\lambda_4)X^2+X^4$

Pour $n=5$, on a

$$\begin{aligned} P_5(X|\lambda_1,\lambda_2,\lambda_3,\lambda_4,\lambda_5) &= \lambda_1 P_4(X|\lambda_2,\lambda_3,\lambda_4,\lambda_5) + X^2 P_3(X|\lambda_3,\lambda_4,\lambda_5) \\ &= \lambda_1\lambda_2\lambda_3\lambda_4\lambda_5 + (\lambda_1\lambda_2\lambda_3+\lambda_1\lambda_2\lambda_5+\lambda_1\lambda_4\lambda_5+\lambda_3\lambda_4\lambda_5)X^2 \\ &\quad +(\lambda_1+\lambda_3+\lambda_5)X^4 \end{aligned}$$

Lemme 2.

Pour tout $k\in[\![1,n]\!]$,

Si k est pair, alors Le polynôme $P_k(\lambda_{n-k+1},\dots,\lambda_n)$est unitaire de degré k.

Si k est impair, alors $P_k(\lambda_{n-k+1},\dots,\lambda_n)$ est de degré $\leqslant k-1$, et le coefficient de X^{k-1}est $\sum\limits_{j=\frac{n-k}{2}}^{\frac{n-1}{2}}\lambda_{2j+1}$.

Preuve du lemme 2.

Par récurrence sur $k\in[\![1,n]\!]$, en utilisant la formule $(\star)$.

D'après le lemme 2, on a le coefficient de X^{n-1} de $P_n(X|\lambda_1,\dots,\lambda_n)$ est

$$\sum_{j=0}^{\frac{n-1}{2}}\lambda_{2j+1}$$

Or, d'après (✠), on a $P_n(X|\lambda_1,\ldots,\lambda_n)=0$, donc $\sum_{j=0}^{\frac{n-1}{2}}\lambda_{2j+1}=0$,

Avec $\lambda_1,\lambda_3,\lambda_5,\ldots,\lambda_{n-2},\lambda_n\geqslant 0$, alors pour tout $j\in[\![0,\frac{n-1}{2}]\!]$ $\lambda_{2j+1}=0$.

Par conséquent, pour tout $j\in[\![1,n]\!]$, $\lambda_j=0$.

Ainsi, B est une matrice diagonalisable qui admet une seule valeur propre 0. alors $B=0$.

D'où le résultat.

✠✠✠✠✠✠✠

L'exercice 9 étudie les sous-groupes des isométries affines du plan. Il demande de prouver l'existence de certaines translations dans un sous-groupe d'isométries vérifiant des conditions spécifiques. L'exercice fait appel à des notions de géométrie affine et de théorie des groupes.

Exercice 9. (Étude des sous-groupes des isométries affines)

Soit G un sous-groupe du groupe des isométries du plan affine $\mathbb{R}^2$. On suppose que pour tout $x\in\mathbb{R}^2$, il existe $g\in G$ tel que $g(x)\neq x$. Montrer que G contient une translation non triviale.

Si de plus G ne stabilise aucune droite, montrer que G contient une deuxième translation non parallèle à la première.

Solution. (ZINE Akram)

Soit G un sous-groupe du groupe des isométries du plan affine $\mathbb{R}^2$. On suppose que pour tout $x\in\mathbb{R}^2$, il existe $g\in G$ tel que $g(x)\neq x$. Montrons que G contient une translation non triviale.

On utilisera pour les deux questions le fait que les 4 isométries possibles du plan sont :

1. Une transaltion
2. Une rotation
3. Une réflexion
4. Une réflexion glissante

Pour s'en convaincre il suffit d'utiliser la classification des isométries vectorielles du plan en rotation et réflexion, puis translater par un vecteur

v.

Lemme 1.

La composition d'une rotation et d'une réflexion dans le plan donne une réflexion glissante si le centre de rotation n'est pas situé sur la ligne de réflexion.

Preuve du lemme 1.

Alignons l'axe des x avec la ligne de réflexion l. Ainsi, la réflexion par rapport à l est donnée par :

$$M(x, y) = (x, -y)$$

Plaçons le centre de rotation O en $(0, d)$ où $d \neq 0$, puisque l ne passe pas par O.

Considérons une rotation autour du point O d'angle θ. La matrice de rotation est :

$$R_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Pour effectuer une rotation autour de O, nous devons translater les coordonnées de manière à ce que O soit à l'origine :

$$\tilde{P} = P - O.$$

Après la rotation, nous obtenons :

$$\tilde{P}' = R_\theta \tilde{P}.$$

Ensuite, nous revenons aux coordonnées d'origine :

$$P' = \tilde{P}' + O.$$

Ainsi , les coordonnées après translation vers O sont :

$$\tilde{P} = \begin{bmatrix} x \\ y - d \end{bmatrix}.$$

Après rotation de $\tilde{P}$:

$$\tilde{P}' = R_\theta \tilde{P} = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y - d \end{bmatrix}.$$

En combinant les composantes, nous obtenons :

$$\tilde{x}' = \cos\theta \cdot x - \sin\theta \cdot (y - d),$$

$$\tilde{y}' = \sin\theta \cdot x + \cos\theta \cdot (y - d).$$

Par suite,

$$x' = \tilde{x}',$$

$$y' = \tilde{y}' + d = \sin\theta \cdot x + \cos\theta \cdot (y - d) + d.$$

Ainsi,

$$y' = \sin\theta \cdot x + \cos\theta \cdot y - \cos\theta \cdot d + d.$$

Par suite,

$$y'' = -y' = -(\sin\theta \cdot x + \cos\theta \cdot y - \cos\theta \cdot d + d).$$

En combinant les composantes x'' et y'', nous obtenons :

$$x'' = \cos\theta \cdot x - \sin\theta \cdot (y - d),$$

$$y'' = -\sin\theta \cdot x - \cos\theta \cdot y + \cos\theta \cdot d - d.$$

En forme matricielle, cela donne :

$$\begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} \sin\theta \cdot d \\ \cos\theta \cdot d - d \end{bmatrix}.$$

Le terme $\begin{bmatrix} \sin\theta \cdot d \\ \cos\theta \cdot d - d \end{bmatrix}$ représente une translation, et la matrice

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{bmatrix}$$

indique qu'il s'agit d'une réflexion suivie d'une translation le long de l'axe de réflexion, c'est-à-dire une réflexion glissante.

Lemme 2.

La composition de deux rotations de centres différents dans le plan affine donne une rotation ou une translation. Plus précisément, si les angles de

rotation sont opposés, la composition donne une translation. Sinon, la composition reste une rotation. Dans les deux cas, on peut toujours construire une translation.

Preuve du lemme 2.

Définissons les deux rotations :

- Première rotation R_1 : de centre O_1 à la position $\vec{o_1}$ et d'angle θ_1.

- Deuxième rotation R_2 : de centre : O_2 à la position $\vec{o_2}$, et d'angle θ_2.

Nous allons analyser la composition $T = R_2 \circ R_1$. Une rotation dans le plan peut être représentée de la manière suivante :

1. Translater le point de sorte que le centre de rotation soit à l'origine.
2. Appliquer la matrice de rotation.
3. Translater le point de retour à sa position d'origine.

La matrice de rotation pour un angle θ est :

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

La fonction de transformation pour une rotation autour d'un point O est donnée par :

$$R(P) = R(\theta) \cdot (P - \vec{o}) + \vec{o}.$$

Appliquons d'abord R_1 à un point P, puis R_2 au résultat :

$$P' = R_1(P) = R(\theta_1) \cdot (P - \vec{o_1}) + \vec{o_1}.$$

Ensuite,

$$P'' = R_2(P') = R(\theta_2) \cdot (P' - \vec{o_2}) + \vec{o_2}.$$

La composition $T(P)$ s'exprime alors comme :

$$T(P) = R_2(R_1(P)) = R(\theta_2) \cdot [R(\theta_1) \cdot (P - \vec{o_1}) + \vec{o_1} - \vec{o_2}] + \vec{o_2}.$$

Développons l'expression :

$$T(P) = R(\theta_2) \cdot R(\theta_1) \cdot (P - \vec{o_1}) + R(\theta_2) \cdot (\vec{o_1} - \vec{o_2}) + \vec{o_2}.$$

On a :

$$R(\theta_2) \cdot R(\theta_1) = R(\theta_1 + \theta_2).$$

Ainsi, l'expression devient :

$$T(P) = R(\theta_1 + \theta_2) \cdot (P - \vec{o_1}) + R(\theta_2) \cdot (\vec{o_1} - \vec{o_2}) + \vec{o_2}.$$

Définissons :

— **Angle total de rotation** : $\theta = \theta_1 + \theta_2$.

— **Vecteur de translation** : $\vec{t} = R(\theta_2) \cdot (\vec{o_1} - \vec{o_2}) + \vec{o_2}$.

La transformation devient :

$$T(P) = R(\theta) \cdot (P - \vec{o_1}) + \vec{t}.$$

— **Cas 1 : La somme des angles est nulle** ($\theta = 0$)

Si $\theta_1 + \theta_2 = 0$, alors $R(\theta)$ est la matrice identité. La transformation $T(P)$ se simplifie en :

$$T(P) = (P - \vec{o_1}) + \vec{t} = P + (\vec{t} - \vec{o_1}).$$

C'est une translation par le vecteur $\vec{v} = \vec{t} - \vec{o_1}$.

— **Cas 2 : La somme des angles n'est pas nulle** ($\theta \neq 0$)

La transformation $T(P)$ est une rotation d'angle θ autour d'un nouveau point. Il existe un composant de translation supplémentaire. Par conséquent, T est une rotation autour d'un nouveau centre.

La composition de deux rotations R_1 et R_2 de centres différents est équivalente à :

— Une rotation d'angle $\theta_1 + \theta_2$ autour d'un nouveau point, sauf si les angles sont opposés. On peut aussi construire dans ce cas une translation, en combinant cette rotation avec la rotation d'angle -($\theta_1 + \theta_2$) qui est de centre différent d'après la même construction,(puisque le centre dépend de l'orientation).

— Dans le cas où $\theta_1 + \theta_2 = 0$ et $\vec{o_1} \neq \vec{o_2}$, la composition est une translation.

Lemme 3.

La composition de deux réflexions aux axes parallèles donne une translation.

Preuve du lemme 3.

Soient L_1 et L_2 deux droites parallèles distinctes dans le plan affine $\mathbb{R}^2$, faisant un angle θ avec l'axe des abscisses. Nous allons démontrer que la composition des réflexions par rapport à L_1 et L_2 est une translation.

— Supposons que les droites L_1 et L_2 soient parallèles et orientées selon un angle θ avec l'axe des abscisses. Ainsi, un vecteur directeur commun à ces droites est donné par :

$$\mathbf{u} = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}$$

— Un vecteur normal unitaire aux droites est :

$$\mathbf{n} = \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$

— Soit d la distance entre les droites L_1 et L_2.

La réflexion par rapport à une droite L orientée selon θ et située à une distance c de l'origine peut être exprimée comme une transformation affine :

$$R_L(\mathbf{x}) = A\mathbf{x} + \mathbf{t}$$

où A est la matrice de réflexion linéaire et $\mathbf{t}$ est le vecteur de translation.

— La matrice de réflexion par rapport à une droite orientée selon θ est :

$$A = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix}$$

— Le vecteur de translation dépend de la position de la droite. Pour une droite L située à une distance c le long du vecteur normal $\mathbf{n}$, le vecteur de translation est :

$$\mathbf{t} = 2c\mathbf{n} = 2c \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix}$$

Ainsi, les réflexions par rapport à L_1 et L_2 sont :

$$R_{L_1}(\mathbf{x}) = A\mathbf{x} + 2c_1\mathbf{n}$$

$$R_{L_2}(\mathbf{x}) = A\mathbf{x} + 2c_2\mathbf{n}$$

où c_1 et c_2 sont les distances de L_1 et L_2 par rapport à l'origine, respectivement.

Nous calculons la composition $R = R_{L_2} \circ R_{L_1}$.

$$R(\mathbf{x}) = R_{L_2}(R_{L_1}(\mathbf{x})) = R_{L_2}(A\mathbf{x} + 2c_1\mathbf{n}) = A(A\mathbf{x} + 2c_1\mathbf{n}) + 2c_2\mathbf{n}$$

Calculons chaque terme séparément :

$$A \cdot A\mathbf{x} = A^2\mathbf{x}$$
$$A \cdot 2c_1\mathbf{n} = 2c_1 A\mathbf{n}$$

On a :

$$A^2 = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} = I$$

$$A\mathbf{n} = \begin{pmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{pmatrix} \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} = \begin{pmatrix} -\cos 2\theta \sin\theta + \sin 2\theta \cos\theta \\ -\sin 2\theta \sin\theta - \cos 2\theta \cos\theta \end{pmatrix}$$

Donc,

$$A\mathbf{n} = \begin{pmatrix} \sin\theta \\ -\cos\theta \end{pmatrix} = \mathbf{n}$$

Maintenant, revenons à la composition $R(\mathbf{x})$:

$$R(\mathbf{x}) = A^2\mathbf{x} + 2c_1 A\mathbf{n} + 2c_2\mathbf{n} = I\mathbf{x} + 2c_1\mathbf{n} + 2c_2\mathbf{n} = \mathbf{x} + 2(c_1 + c_2)\mathbf{n}$$

La transformation R est donc donnée par :

$$R(\mathbf{x}) = \mathbf{x} + 2(c_2 - c_1)\mathbf{n}$$

où $2(c_2 - c_1)\mathbf{n}$ est le vecteur de translation.

Ainsi, la composition des réflexions $R_{L_2} \circ R_{L_1}$ est une translation de vecteur $\mathbf{t} = 2(c_2 - c_1)\mathbf{n}$, c'est-à-dire une translation parallèlement aux droites L_1 et L_2 et de longueur égale au double de la distance entre elles.

1- Examinons cas par cas :

— Si G contient une réflexion glissante alors on obtient une translation non triviale en la composant par elle-même.
— Si G ne contient que des rotations, alors il contient deux rotations de centre différents d'après l'hypothèse de l'énoncé, et donc d'après le **Lemme 2** on peut construire une translation.
— Si G contient une rotation et une réflexion dont la droite ne passe pas par le centre de rotation, et dans ce cas on peut construit une translation d'après le **Lemme 1**.
— Si G ne contient que des réflexions : Si au moins deux présentent des axes qui sont parallèles alors la composition des deux réflexions résulte en une translation d'après le **Lemme 3**. Sinon, On a aux moins trois réflexions qui présentent des axes sécants. Et leur composition donne deux matrices de rotations différentes (Il suffit de multiplier les matrices de réflexion).

2- Supposons que G contienne une rotation R. Alors, pour toute translation $T_{\mathbf{v}} \in G$, nous avons

$$R^{-1} \circ T_{\mathbf{v}} \circ R = T_{R^{-1}(\mathbf{v})}.$$

Ainsi, nous obtenons une nouvelle translation $T_{R^{-1}(\mathbf{v})}$. Comme R ne stabilise que son centre de rotation, cette nouvelle translation n'est pas triviale et peut avoir une direction différente de la translation initiale.

Ensuite, si G ne contient que des translations, et que ces translations sont parallèles à une direction commune. Cela implique que les droites parallèles à cette direction sont stabilisées par G, ce qui contredit l'hypothèse selon laquelle G ne stabilise aucune droite.

Considérons maintenant le cas où G contient des réflexions mais pas de rotations. Soit M une réflexion dans G. Alors, pour toute translation $T_{\mathbf{v}} \in G$, nous avons

$$M \circ T_{\mathbf{v}} \circ M = T_{M(\mathbf{v})}.$$

Si pour toutes les réflexions $M \in G$, on a $M(\mathbf{v}) = \mathbf{v}$, alors G stabilise une droite parallèle à $\mathbf{v}$, ce qui est une contradiction avec l'hypothèse que G ne stabilise aucune droite.

Ainsi, G doit contenir une seconde translation dont la direction est différente de la première.

✠✠✠✠✠✠✠

Cet exercice porte sur le résultant de deux polynômes. Il s'agit de prouver certaines propriétés du résultant, notamment sa symétrie et son lien avec un déterminant spécifique. L'exercice fait appel à des notions d'algèbre linéaire et de théorie des polynômes.

Exercice 10. (Résultant)

Soient $A, B \in \mathbb{C}[X]$ deux polynômes unitaires, de degrés respectifs a et b. Soit $M_{A,B}$ l'endomorphisme de $\mathbb{C}[X]/(A)$ défini par $M_{A,B}([P]) = [BP]$.

Soit $\mu_{A,B} = \det M_{A,B}$. Montrer que $\mu_{A,B} = (-1)^{ab}\mu_{B,A}$.

Soit $F_{A,B}$ l'unique endomorphisme de $\mathbb{C}[X]_{a+b-1}$ tel que pour tout $U \in \mathbb{C}[X]_{a-1}$ et tout $V \in \mathbb{C}[X]_{b-1}$, $F_{A,B}(U + X^a V) = BU + AV$.

Montrer que $\det(F_{A,B}) = \mu_{A,B}$

Le nombre $\mu_{A,B}$ est le résultant de A et de B.

Solution. (SABIR Ilyass)

Soit $A, B \in \mathbb{C}[X]$, deux polynômes unitaires de degrés respectifs a et b.

Soit $M_{A,B}$ l'endomorphisme de $\mathbb{C}[X]/(A)$ défini par $M_{A,B}([P]) = [BP]$ et soit $\mu_{A,B} = \det M_{A,B}$.

Montrons que

$$\mu_{A,B} = (-1)^{ab}\mu_{B,A}$$

Pour cela, on va montrer que :

$$\mu_{A,B} = \prod_{i=1}^{a}\prod_{j=1}^{b}(\alpha_i - \beta_j) (✠)$$

L'identité (✠) nous permettra également de traiter la seconde partie de l'énoncé de l'exercice.

Notons $A = \prod_{k=1}^{a}(X - \alpha_k)$ et $B = \prod_{k=1}^{a}(X - \beta_k)$ avec $\alpha_1, \ldots, \alpha_a, \beta_1, \ldots, \beta_b \in \mathbb{C}$.

Supposons dans un premier temps que $\alpha_1, \alpha_2, \ldots, \alpha_a$ (respectivement $\beta_1, \beta_2, \ldots, \beta_b$) sont deux à deux distincts.

Pour tout $j \in [\![1, a]\!]$, on définit le polynôme $P_j := \prod_{\substack{k=1 \\ k\neq j}}^{a} \frac{X-\alpha_k}{\alpha_j-\alpha_k}$. On a $(P_j)_{1\leqslant j\leqslant a}$ est une base de $\mathbb{C}[X]/(A)$. De plus, pour tout $j \in [\![1, a]\!]$, il existe $Q_j \in \mathbb{R}[X]$ tel que

$$B.P_j = Q_j A + M_{A,B}(P_j)$$

Pour tout $i \in [\![1, a]\!]\backslash\{j\}$, on a $M_{A,B}(P_j)(\alpha_i) = 0$ et $M_{A,B}(P_j)(\alpha_j) = B(\alpha_j)$

On en déduit, par interpolation de Lagrange, que

$$M_{A,B}(P_j) = B(\alpha_j)P_j$$

Ainsi,

$$\begin{aligned} \mu_{A,B} &= \det(M_{A,B}) \\ &= \prod_{j=1}^{a} B(\alpha_j) \\ &= \prod_{i=1}^{a}\prod_{j=1}^{b}(\alpha_i - \beta_j) \end{aligned}$$

Puisque l'ensemble des polynômes sindés à racines simples dense dans l'ensemble des polynômes scindés, et que l'application $(A, B) \in \mathbb{C}[X]^2 \longmapsto \mu_{A,B}$ est continue (car elle est une composition d'applications continues).

On a pour $A := \prod_{k=1}^{a} (X-\alpha_k)$ et $B := \prod_{k=1}^{a} (X-\beta_k)$, avec $\alpha_1, \ldots, \alpha_a, \beta_1, \ldots, \beta_b \in \mathbb{C}$.

On a

$$\mu_{B,A} = \prod_{j=1}^{b}\prod_{i=1}^{a}(\beta_j - \alpha_i)$$

En particulier, par symétrie :

$$\begin{aligned} \mu_{B,A} &= \prod_{j=1}^{b}\prod_{i=1}^{a}(\beta_j - \alpha_i) \\ &= \prod_{i=1}^{a}\prod_{j=1}^{b}(-1)(\alpha_i - \beta_j) \\ &= (-1)^{ab}\mu_{A,B} \end{aligned}$$

Montrons maintenant que $\det(F_{A,B}) = \mu_{A,B}$.
Notons $A = \sum_{k=0}^{a} \lambda_k X^k$ et $B = \sum_{k=0}^{b} \gamma_k X^k$, où $\lambda_0, \dots, \lambda_a, \gamma_0, \dots, \gamma_b \in \mathbb{C}$.
On a alors pour tout $n \in [\![0, a-1]\!]$,

$$\begin{aligned} F_{A,B}(X^n) &= B.X^n \\ &= \sum_{k=0}^{b} \gamma_k X^{n+k} \end{aligned}$$

Et pour tout $n \in [\![a, a+b-2]\!]$

$$\begin{aligned} F_{A,B}(X^n) &= A.X^{n-a} \\ &= \sum_{k=0}^{a} \lambda_k X^{n-a+k} \end{aligned}$$

La matrice de $F_{A,B}$ dans la base $\mathcal{B} = (X^n)_{0 \leqslant n \leqslant a+b-2}$ est donc :

$$\mathrm{mat}_{\mathcal{B}}(F_{A,B}) = \begin{pmatrix} \lambda_0 & \lambda_1 & \dots & \lambda_a & 0 & 0 & 0 & \dots & 0 \\ 0 & \lambda_0 & \lambda_1 & \dots & \lambda_a & 0 & 0 & \dots & 0 \\ \vdots & & & \ddots & & & & & \vdots \\ 0 & 0 & \dots & 0 & 0 & \lambda_0 & \lambda_1 & \dots & \lambda_a \\ \beta_0 & \beta_1 & \dots & \beta_b & 0 & 0 & 0 & \dots & 0 \\ 0 & \beta_0 & \beta_1 & \dots & \beta_b & 0 & 0 & \dots & 0 \\ \vdots & & & \ddots & & & & & \vdots \\ 0 & 0 & \dots & 0 & 0 & \beta_0 & \beta_1 & \dots & \beta_b \end{pmatrix} \text{ (Matrice de Sylvester)}$$

Pour conclure, il suffit de montrer que $\det(F_{A,B}) = \prod_{j=1}^{b} \prod_{i=1}^{a} (\beta_j - \alpha_i)$.
Soient $k, l \in \mathbb{C}$. Si l'on remplace A par kA et B par lB, on a :

$$\det(F_{kA,lB}) = k^b l^a \det(F_{A,B})$$

En effet, les b premières lignes de la matrice sont multipliées par k (contribution de k^b), les a dernières lignes sont multipliées par l (contribution de l^a).

Par homogénéité, on peut se ramener au cas où A et B sont unitaires. Il suffit donc de démontrer l'égalité pour :

$$A(X) = \prod_{i=1}^{a}(X - \alpha_i) \quad \text{et} \quad B(X) = \prod_{j=1}^{b}(X - \beta_j)$$

où $\alpha_1, \ldots, \alpha_a$ et $\beta_1, \ldots, \beta_b$ sont les racines respectives de A et B.

On a alors $\det(F_{A,B}) \in \mathbb{C}[\alpha_1, \ldots, \alpha_a, \beta_1, \ldots, \beta_b]$. Pour tous $i \in [\![1, a]\!]$ et $j \in [\![1, b]\!]$, $(\beta_j - \alpha_i)$ divise $\det(F_{A,B})$.

Si $\alpha_i = \beta_j$, alors : $A(X) = (X - \alpha_i)A_1(X)$ et $B(X) = (X - \beta_j)B_1(X)$

On peut construire un vecteur non nul v dans le noyau de $F_{A,B}$:

$$v = X^b A_1 - X^a B_1$$

Ce vecteur est non nul car les degrés des polynômes sont différents. Donc $F_{A,B}$ n'est pas inversible et $\det(F_{A,B}) = 0$.

Par les points précédents, on peut écrire :

$$\det(F_{A,B}) = \lambda \prod_{j=1}^{b}\prod_{i=1}^{a}(\beta_j - \alpha_i)$$

où λ est une constante dans $\mathbb{C}$.

Pour calculer λ, considérons le cas particulier où :

$$A(X) = X^a \quad \text{et} \quad B(X) = 1$$

Dans ce cas, la matrice $F_{A,B}$ devient triangulaire, et tous les éléments diagonaux sont égaux à 1.

Donc $\det(F_{A,B}) = 1$.

Par conséquent, $\lambda = 1$.

On a donc démontré que :

$$\det(F_{A,B}) = \prod_{j=1}^{b}\prod_{i=1}^{a}(\beta_j - \alpha_i) = \mu_{A,B}$$

✠✠✠✠✠✠✠

L'exercice 11 s'intéresse aux composantes connexes d'ensembles de polynômes. Il demande de décrire les composantes connexes par arcs de certains

ensembles de polynômes unitaires à coefficients réels, définis par des conditions sur leurs racines. L'exercice combine des aspects de topologie et de théorie des polynômes.

Exercice 11. (Composantes connexes d'ensembles de polynômes)

Soit $d \geq 1$ un entier. Soit P l'ensemble des polynômes unitaires de degré d à coefficients réels.
Décrire les composantes connexes par arcs de

$$\{(f,x) \in P \times \mathbb{R} | f(x) = 0 \text{et } f'(x) \neq 0\}.$$

Décrire les composantes connexes par arcs de

$$\{f \in P | \forall x \in \mathbb{R}, f(x) \neq 0 ou f'(x) \neq 0\}.$$

Solution. (ZINE Akram)

Si $d = 1$, l'ensemble H est évidemment connexe par arcs car il est convexe. Nous passons maintenant au cas où $d \geq 2$.

Pour $d \geq 2$, nous allons montrer que les composantes connexes par arcs de $H = \{(P,x) \in \mathcal{P}_d \times \mathbb{R} \mid P(x) = 0, P'(x) \neq 0\}$ sont :

$$H_{>0} := \{(P,x) \in H \mid P'(x) > 0\} \quad \text{et} \quad H_{<0} := \{(P,x) \in H \mid P'(x) < 0\}.$$

Vérification que $H_{>0}$ et $H_{<0}$ sont non vides :

- Pour $H_{>0}$, on peut prendre $P(X) = X^d + X$, et pour $x = 0$, on a $P(0) = 0$ et $P'(0) = 1 > 0$, donc $(P,0) \in H_{>0}$.

- Pour $H_{<0}$, on peut prendre $P(\text{xX}) = X^d - X$, et pour $x = 0$, on a $P(0) = 0$ et $P'(0) = -1 < 0$, donc $(P,0) \in H_{<0}$.

Séparation des composantes :

Considérons la fonction $\gamma : (P,x) \mapsto P'(x)$, qui est continue sur $\mathcal{P}_d \times \mathbb{R}$. Soit C une partie connexe par arcs de H. $\gamma(C)$ doit être un intervalle de $\mathbb{R}$ ne contenant pas 0, car $P'(x) \neq 0$ pour tout $(P,x) \in H$. Ainsi, $\gamma(C)$ est inclus dans $\mathbb{R}_+^*$ ou $\mathbb{R}_-^*$, et par conséquent, $C \subset H_{>0}$ ou $C \subset H_{<0}$.

Connexité de $H_{>0}$:

Pour prouver que $H_{>0}$ est connexe par arcs, nous définissons une fonction continue $f(t)$ reliant deux éléments quelconques de $H_{>0}$. Soient $(P, x) \in H_{>0}$ et $(Q, y) \in H_{>0}$. Nous définissons $f(t)$ comme suit :

$$f(t) = (tP(X+x-(1-t)y-tx)+(1-t)Q(X+y-(1-t)y-tx), tx+(1-t)y)$$

Le premier composant, $tP(X + x - (1 - t)y - tx) + (1 - t)Q(X + y - (1 - t)y - tx)$, est continu en t grâce à la continuité des polynômes et à la formule de Taylor, tandis que le second composant, $tx + (1 - t)y$, est une interpolation linéaire continue entre x et y.

- Pour $t = 0$, on a $f(0) = (Q(X), y) \in H_{>0}$.
- Pour $t = 1$, on a $f(1) = (P(X), x) \in H_{>0}$.

De plus, pour tout $t \in [0, 1]$, $f(t) \in H_{>0}$.

Ainsi, la fonction $f(t)$ fournit un chemin continu reliant (P, x) à (Q, y) à l'intérieur de $H_{>0}$, prouvant que $H_{>0}$ est connexe par arcs.

Connexité de $H_{<0}$:

Un raisonnement similaire s'applique pour $H_{<0}$.

En conclusion, les composantes connexes par arcs de H sont $H_{>0}$ et $H_{<0}$ si $d \geq 2$. Chaque partie connexe de H est incluse soit dans $H_{>0}$, soit dans $H_{<0}$, et chacune de ces parties est connexe par arcs.

Composantes connexes par arcs de T :

Soit P l'ensemble des polynômes unitaires de degré d. Définissons l'ensemble T comme suit :

$$T = \{f \in P \mid \forall x \in \mathbb{R}, f(x) \neq 0 \text{ ou } f'(x) \neq 0\}$$

Autrement dit, T est l'ensemble des polynômes qui n'ont ni racines multiples, ni racines où la dérivée s'annule. Nous cherchons à décrire les composantes connexes par arcs de T.

Structure de T et description des composantes connexes :

On note que l'ensemble T_m, défini comme suit :

$$T_m = \{f \in T \mid n_f = m\}$$

où n_f représente le nombre de racines réelles distinctes de f, constitue une composante connexe par arcs de T. Il est également important de noter que T_m est non vide ssi $m \equiv d \pmod 2$, avec d étant le degré du polynôme. Autrement dit, le nombre de racines réelles m doit avoir la même parité que le degré d du polynôme. Dans ce cas, les T_m présentent exactement les composantes connexes par arcs de T.

Construction de T_m :

Pour mieux comprendre la structure de T_m, considérons l'application suivante :

$$f : S \times D \to T_m$$

Où :

— S est l'ensemble des polynômes de degré $d - m$ qui sont strictement positifs sur tout $\mathbb{R}$,

— D est l'ensemble des m-uplets de réels distincts et ordonnés de manière croissante.

L'application f est définie par :

$$f(Q, (x_1, \ldots, x_m)) = Q \cdot \prod_{i=1}^{m} (X - x_i)$$

où $Q \in S$ et $(x_1, \ldots, x_m) \in D$. Cette application est continue, et comme S et D sont des ensembles convexes, leur produit cartésien $S \times D$ est également convexe. Par conséquent, l'image de f, qui est précisément T_m, est connexe par arcs.

Pour en finir nous souhaitons maintenant montrer que la fonction n_P, qui associe à un polynôme $P \in T$ le nombre n_P de ses racines réelles distinctes, est continue. Cela impliquerai la séparation des composantes connexes.

Preuve de la continuité de n_P :

Soit (P_n) une suite de polynômes dans T qui converge vers un polynôme $P \in T$. Autrement dit, les coefficients de P_n convergent vers ceux de P, ce

qui implique que la convergence est également uniforme sur tout compact. Supposons que P ait m racines réelles distinctes. Entre chacune de ces racines, le signe de P est constant, puisque P ne s'annule pas en dehors de ses racines simples.

Pour n suffisamment grand, le polynôme P_n conserve le même signe que P entre ces racines, par continuité. Par le *théorème des valeurs intermédiaires (TVI)*, P_n doit avoir au moins m racines réelles, c'est-à-dire $n_{P_n} \geq n_P$.

Réciproque (preuve par l'absurde) :

Supposons maintenant que $n_{P_n} \geq m+1 = n_P+1$ pour une suite P_n. Cela signifierait que P_n a au moins $m+1$ racines réelles. Puisque les racines réelles de P sont bornées dans un intervalle de la forme $[-Md, Md]$ (où $M \geq 1$ est une constante dépendant des coefficients de P), il existe un $M \geq 1$ tel que, pour tout n, le vecteur $(x_{n,1}, \ldots, x_{n,m+1})$ représentant les $m+1$ racines réelles de P_n se trouve dans le compact $[-Md, Md]^{m+1}$. Pour voir cela, il suffit d'annuler le polynôme en l'une de ces racines et de distinguer si la valeur absolue de la racine est ≥ 1.

Ainsi, on peut extraire de cette suite une sous-suite convergente dont les racines tendent vers $y_1, \ldots, y_{m+1}$, qui seraient des racines réelles de P. Comme P a exactement m racines réelles distinctes, il existe un indice i tel que $y_i = y_{i+1}$. Par le théorème de Rolle, il existe un point $z_n \in [x_{i,\varphi(n)}, x_{i+1,\varphi(n)}]$ tel que $P_n'(z_n) = 0$.

En passant à la limite, $z_n \to y_i$, ce qui implique que y_i est une racine double de P. Cependant, ceci contredit le fait que toutes les racines de P sont simples. Par conséquent, la supposition $n_{P_n} \geq m+1$ est fausse, ce qui prouve que $n_{P_n} \leq n_P$.

Ainsi, nous avons montré que $n_{P_n} = n_P$ pour n suffisamment grand, ce qui prouve la continuité de la fonction n_P, et donc la séparation des T_m.

✠✠✠✠✠✠✠

Cet exercice traite de l'impossibilité de la densité d'un certain espace de translations. Il demande d'étudier l'ensemble des translations qui laissent

invariant un espace engendré par les translatés entiers d'une fonction à support compact. L'exercice fait appel à des notions d'analyse fonctionnelle.

Exercice 12. (Impossibilité de la densité d'un certain espace de translations)

Soit $B(\mathbb{R})$ l'espace vectoriel des fonctions bornées sur $\mathbb{R}$ muni de la norme uniforme. Soit $g : \mathbb{R} \to \mathbb{R}$ une fonction à support compact. On note $W(g) \subseteq B(\mathbb{R})$ l'espace engendré par les translatés $x \mapsto g(x-n)$ pour $n \in \mathbb{Z}$.
Etudier l'ensemble $t \in \mathbb{R}$ tels que $\overline{W(g)}$ est invariant par translation par t.

Solution. (ZINE Akram)

On suppose que g est non nulle, sans quoi le problème est trivial et $G = \mathbb{R}$. Raisonnons par l'absurde en supposant que l'ensemble des $t \in \mathbb{R}$ pour lesquels l'adhérence de $W(g)$, notée $\overline{W(g)}$, est invariante par translation, est dense dans $\mathbb{R}$. Autrement dit, supposons que ce sous-groupe $G \subset \mathbb{R}$ soit dense.

Puisque $\overline{W(g)}$ est invariant par t pour tout $t \in G$, prenons un élément $t \in G$. Par définition de l'invariance par translation, cela signifie que $g(x-t)$ peut être exprimée comme une combinaison linéaire des translatés de g par des entiers, soit :

$$g(x-t) = \sum_{n\in\mathbb{Z}} \alpha_n g(x-n).$$

Notre objectif est maintenant de faire intervenir la transformée de Fourier pour mieux comprendre cette expression. Définissons une suite de sommes partielles

$$g_N(x-t) = \sum_{|n|\leq N} \alpha_n g(x-n)$$

qui converge uniformément vers $g(x-t)$, car g est bornée et de support compact. Cela signifie que g_N est majorée par une fonction de support compact f pour tout N et tout x.

Ainsi, nous pouvons appliquer le théorème de convergence dominée pour justifier l'interversion entre la transformée de Fourier et la limite, en concluant

que la transformée de Fourier de g_N converge vers la transformée de Fourier de g lorsque $N \to \infty$.

Lemme 1.

La transformée de Fourier d'une fonction g à support compact est analytique.

Preuve du lemme 1.

La transformée de Fourier d'une fonction g à support compact est donnée par :

$$\hat{g}(\xi) = \int_{-a}^{a} g(t) e^{-2i\pi\xi t}\, dt,$$

où g est à support dans $[-a, a]$.

Nous pouvons développer l'exponentielle complexe en série de Taylor :

$$e^{-2i\pi\xi t} = \sum_{k\geq 0} \frac{(-2i\pi t\xi)^k}{k!}$$

Ainsi,

$$\begin{aligned} \hat{g}(\xi) &= \int_{-a}^{a} g(t) \left(\sum_{k\geq 0} \frac{(-2i\pi t\xi)^k}{k!} \right) dt \\ &= \sum_{k\geq 0} \xi^k \int_{-a}^{a} g(t) \frac{(-2i\pi t)^k}{k!}\, dt \end{aligned}$$

où l'interversion de la somme et de l'intégrale est permise par la convergence de

$$\int_{-a}^{a} \sum_{k\geq 0} \left| \frac{(-2i\pi t\xi)^k}{k!} \right| |g(t)|\, dt$$

Cela montre que $\hat{g}(\xi)$ est exprimée comme une série entière en ξ, ce qui signifie que $\hat{g}(\xi)$ est analytique en tant que fonction de la variable complexe ξ dans le plan complexe.

Utilisons le lemme suivant pour montrer qu'il existe ξ et $\xi + 1$, telles que $\hat{g}(\xi)$ et $\hat{g}(\xi + 1)$ soient non nulles.

D'après le lemme précédent, si la transformée de Fourier est non nulle, alors elle est analytique, et donc ses zéros sont isolés. Si $\hat{g}$ ne s'annule pas, la démonstration est terminée.

Sinon, il existe un ξ tel que $\hat{g}(\xi) = 0$. Comme les zéros sont isolés, il existe $\epsilon' > 0$ tel que pour tout $\epsilon \in]0, \epsilon']$, on ait $\hat{g}(\xi + \epsilon) \neq 0$.

D'autre part, pour la même raison, il existe $t \in]0, \epsilon']$ tel que $\hat{g}(\xi+1+t) \neq 0$.

Finalement, il existe ξ et $\xi + 1$, telles que $\hat{g}(\xi)$ et $\hat{g}(\xi + 1)$ soient non nulles.

La transformé de Fourier donne :

$$\hat{g}(\xi) \left(e^{-2i\pi t\xi} - \sum_{n\in\mathbb{Z}} \alpha_n e^{-2i\pi n\xi} \right) = 0.$$

.

En prenant les valeur pour $\hat{g}(\xi)$ et $\hat{g}(\xi + 1)$ et on observant que $e^{-2i\pi n\xi}$ est périodique de période 1. On obtient que $e^{-2i\pi t} = 1$, et donc $t \in \mathbb{Z}$.

Reprenons le cas où $\hat{g} = 0$. Ceci implique, par injectivité de la transformée de Fourier, que $g = 0$ presque partout au sens de la mesure de Lebesgue.

Soit S le support de g. Montrons qu'il existe $x \in S$, et $t \in G$ $n \in \mathbb{Z}$, $x - n - t \notin S$.

Raisonnons par l'absurde et supposons que

$$\forall x \in S, \forall t \in G, \exists n \in \mathbb{Z}, x - n - t \in S$$

Ainsi, $G+S \subset \mathbb{Z}+S$. Posons $A = \mathbb{Z}+S$ est fermé. En effet, soit $(x_n) \in A^{\mathbb{N}}$ tel que (x_n) converge vers x.

Ainsi, il existe $(z_n) \in \mathbb{Z}^{\mathbb{N}}$ et il existe $(s_n) \in S^{\mathbb{N}}$ telles que $x_n = z_n + s_n$.

La suite (z_n) est bornée car S est compact et (x_n) converge. Il existe donc une extractrice ϕ telle que $(z_{\phi(n)})$ converge vers $z \in \mathbb{Z}$. $(s_{\phi(n)})$ converge vers $s \in S$. Ainsi, $(x_{\phi(n)})$ converge vers $z + s$.

Donc, (x_n) converge vers $z + s$.

Ce qui montre que A est fermé et dense, car il contient $S + G$ et donc $A = \mathbb{R}$.

Or, puisque la mesure de Lebesgue de S est nulle(comme on a supposé que $\hat{g}$ est nulle), alors la mesure de Lebesgue de A l'est aussi. Contradiction.

Ainsi, il existe $x \in S$ et $t \in G$, tels que pour tout $n \in \mathbb{Z}$, $\quad x - n - t \notin S$

Écrivons

$$g(x) = \sum_{n \in \mathbb{Z}} \alpha_n g(x - n - t)$$

On trouve que $g(x) = 0$, ce qui est absurde car $x \in S$. Ainsi, G est discret. Comme il contient $\mathbb{Z}$, on en conclut que $G = \frac{1}{n}\mathbb{Z}$, avec $n \in \mathbb{N}^*$.

✠✠✠✠✠✠✠

L'exercice 13 porte sur la valuation $p-$adique d'un produit. Il demande de majorer la valuation $p-$adique d'un produit spécifique impliquant des puissances d'un nombre premier distinct de p. L'exercice fait appel à des notions d'arithmétique et de théorie des nombres p-adiques.

Exercice 13. (Valuation p-adique d'un produit)

Soient p et q deux entiers premiers distincts. Montrer qu'il existe une constante $c > 0$ (que l'on estimera) tel que pour tout entier $m > 0$, la valuation p-adique du produit

$$N(m) = (q-1)(q^2-1)\dots(q^m-1),$$

est majorée par $c.m.\log m$.

Solution. (ZINE Akram)

Lemme 1. (LTE : Lifting The Exponent)

Soit p un nombre premier, x and y des entiers, $n > 0$, tels que $p|(x-y)$ mais $p \nmid x$ et $p \nmid y$. Alors

(1) Si p est impair,

$$v_p(x^n - y^n) = v_p(x-y) + v_p(n);$$

(2) : Si $p = 2$ et n est pair,

$$v_2(x^n - y^n) = v_2(x-y) + v_2(n) + v_2(x+y) - 1.$$

(3) Si $p = 2$ et n impair,

$$v_2(x^n - y^n) = v_2(x-y).$$

Preuve du lemme 1.

Cas de base (p impair et n est impair).

Supposons que $p \not| x, p \not| y, p \not| n$, et $p|x-y$. Alors $x \equiv y \pmod{p}$, ce qui implique :

$$x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \ldots + y^{n-1} \equiv nx^{n-1} \not\equiv 0 \pmod{p}$$

En utilisant la formule de Bernoulli :

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \ldots + y^{n-1})$$

On peut conclure que $\nu_p(x^n - y^n) = \nu_p(x-y)$.

Cas général (p impair)

Pour $n = p$, il faut montrer que :

$$\nu_p(x^p - y^p) = \nu_p(x-y) + 1$$

On a :

$$x^{p-1} + x^{p-2}y + \ldots + y^{p-1} \equiv px^{p-1} \equiv 0 \pmod{p}$$

mais ce n'est pas un multiple de p^2, d'où le résultat.

En écrivant n sous la forme $p^a b$ où $p \nmid b$, le cas de base donne :

$$\nu_p(x^n - y^n) = \nu_p((x^{p^a})^b - (y^{p^a})^b) = \nu_p(x^{p^a} - y^{p^a})$$

Par récurrence sur a, on obtient :

$$\nu_p(x^{p^a} - y^{p^a}) = \nu_p(x-y) + a$$

Cas p=2 et n pair

Si $4|(x-y)$ alors

$$\nu_2(x^n - y^n) = \nu_2(x-y) + \nu_2(n)$$

En effet pour chaque nombre premier p tel que $p \gcd(n,p) = 1$ et $p|(x-y)$ mais $p \nmid x$ et $p \nmid y$ on a

$$\nu_p(x^n - y^n) = \nu_p(x-y)$$

. Ainsi il suffit de prouver l'égalité

$$\nu_2(x^n - y^n) = \nu_2(x - y) + \nu_2(n)$$

pour les n qui sont des puissances de 2. La preuve est directe par récurrence en utilisant le fait que $(a^2 - b^2) = (a - b)(a + b)$. Dans le cas général on a $4|(x^2 - y^2)$ et $n = m.2^k$ et une récurrence permet de conclure.

Cas p pair et n impair

Regarder le cas de base au début de la preuve

Lemme 2. (Formule de Legendre)

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

Preuve du lemme 2.

On peut dire que $\nu_p(n!)$ est le nombre de multiples de p inférieurs à n, ou $\left\lfloor \frac{n}{p} \right\rfloor$.

Cependant, les multiples de p^2 ne sont comptés qu'une fois, alors qu'on doit les compter deux fois. Donc on ajoute donc $\left\lfloor \frac{n}{p^2} \right\rfloor$. Mais cela compte p^3 deux fois, alors qu'on doit les compter trois fois. Donc on ajoute $\left\lfloor \frac{n}{p^3} \right\rfloor$. On continue ainsi jusqu'à ce que $\nu_p(n!) = \sum\limits_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor$. Cela est vrai puisque la somme est finie.

Soit

$$A = \{n \in [1, m], p|q^n - 1\}$$

On suppose que A est non vide, sans quoi la majoration est directe. Soit

$$l = min(A)$$

On trouve par division euclidienne que

$$\forall k \in A, \quad l|k$$

En notant le produit par

$$N(m) := \prod_{k=1}^{m} (q^k - 1)$$

on trouve :

$$\nu_p(N(m)) = \sum_{k=1}^{\lfloor \frac{m}{l} \rfloor} \nu_p(q^{kl} - 1)$$

Si p est impair, d'après LTE on a :

$$\nu_p(N(m)) = \sum_{k=1}^{\lfloor \frac{m}{l} \rfloor} (\nu_p(q^l - 1) + \nu_p(\lfloor \frac{m}{l} \rfloor !)$$

D'après la formule de Legendre. On a :

$$\nu_p(\lfloor \frac{m}{l} \rfloor ! \leq \frac{m}{l(p-1)}$$

On pourrait affiner à

$$\nu_p(\lfloor \frac{m}{l} \rfloor ! \leq \frac{m-1}{l(p-1)}$$

mais on se contentera de la première inégalité, vu qu'on ne nous demande pas de trouver la meilleure constante de majoration.

On trouve alors que :

$$\nu_p N(m) \leq m \log_p(q) + \frac{m}{l(p-1)}$$

On trouve ainsi une majoration linéaire avec :

$$c_{\text{linéaire}} = \log_p(q) + \frac{1}{l(p-1)}$$

et une majoration logarithmique avec :

$$c_{\log} = \frac{c_{\text{linéaire}}}{\log(2)}$$

car m est supérieur à 1.

Si p est pair, on a

$$\nu_2 N(m) = \sum_{k=1}^{\lfloor \frac{m}{l} \rfloor / 2} (\nu_2(q^l - 1)) + \nu_2 \left(\left\lfloor \frac{\lfloor \frac{m}{l} \rfloor}{2} \right\rfloor ! \right) + \sum_{k=1}^{\lfloor \frac{\lfloor \frac{m}{l} \rfloor - 1}{2} \rfloor} (\nu_2(q^l - 1))$$

On trouve ainsi en majorant $\frac{1}{2}$ par 1 une majoration linéaire avec :

$$c_{\text{linéaire}} = \log_p(q) + \frac{1}{l(p-1)}$$

et une majoration logarithmique avec :

$$c_{\log} = \frac{c_{\text{linéaire}}}{\log(2)}$$

✠✠✠✠✠✠✠

Cet exercice s'intéresse aux générateurs d'un groupe de matrices. Il demande de prouver qu'un certain sous-groupe de $\mathrm{GL}_2(\mathbb{Z})$ est engendré par deux matrices spécifiques. L'exercice fait appel à des notions de théorie des groupes et d'algèbre linéaire.

Exercice 14. (Générateurs d'un groupe de matrices)

Soit G le sous-ensemble de $\mathrm{GL}_2(\mathbb{Z})$ des matrices à coefficients entiers $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $a \equiv d \equiv 1 - c \equiv 1 \pmod 3$ et $ad - bc = 1$.

Montrer que G est un sous-groupe engendré par $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$.

C'est une variante, à peine plus subtile, d'un résultat analogue sur $\mathrm{SL}_2(\mathbb{Z})$.

Solution. (SABIR Ilyass)

Soit H le sous-groupe de G engendré par $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $B = \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix}$.

Montrons que $H = G$.

On a pour tout $n, m \in \mathbb{Z}$

$$A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

Et

$$B^m = \begin{pmatrix} 1 & 0 \\ 3m & 1 \end{pmatrix}$$

Ces matrices sont dans G, et comme G est stable par produit, donc $H \subseteq G$.

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.

Considérons l'ensemble E des matrices de la forme MQ avec $Q \in H$. Toutes ces matrices sont dans G, car G est stable par produit. Parmi ces matrices, choisissons $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ qui minimise $|a'|$.

Pour tous $m, n \in \mathbb{Z}$, définissons :

$$\begin{aligned} A'' &:= A'A^{-n}B^{-m} \\ &= \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -3m & 1 \end{pmatrix} \\ &= \begin{pmatrix} a' - 3m(b' - na') & * \\ * & * \end{pmatrix} \end{aligned}$$

Par minimalité de $|a'|$, on a pour tout $m, n \in \mathbb{Z}$:

$$|a'| \leq |a' - 3m(b' - na')|$$

Supposons que pour tout $n \in \mathbb{Z}$, $b' - na' \neq 0$. Choisissons $n_0 \in \mathbb{Z}$ l'entier le plus proche de $\frac{b'}{a'}$. Alors :

$$\begin{aligned} 0 &< |b' - n_0 a'| \\ &= |a'| \cdot |\frac{b'}{a'} - n_0| \\ &\leqslant |a'| \cdot \frac{1}{2} \end{aligned}$$

Choisissons ensuite $m_0 \in \mathbb{Z}$ l'entier le plus proche de $\frac{a'}{3(b' - n_0 a')}$. On obtient :

$$\begin{aligned} |a'| &\leqslant |a' - 3m_0(b' - n_0 a')| \\ &= 3|b' - n_0 a'| \cdot |\frac{a'}{3(b' - n_0 a')} - m_0| \\ &< 3 \cdot \frac{1}{2}|a'| \cdot \frac{1}{2} \\ &= \frac{3}{4}|a'| \end{aligned}$$

Ceci est absurde, car $a' \neq 0$ (car $a' \equiv 1 \pmod 3$).

Donc, il existe $n \in \mathbb{Z}$ tel que $b' = na'$. En prenant $m = 0$, on a : $A'' = A'A^{-n} = \begin{pmatrix} a' & 0 \\ c' & d' \end{pmatrix} \in G$

Comme $A'' \in G$, on a $a'd' = 1$ et $a' \equiv d' \equiv 1 \pmod 3$. Donc $a' = d' = 1$.

Posons $c' = 3q$ avec $q \in \mathbb{Z}$. Alors :

$$A'' = \begin{pmatrix} 1 & 0 \\ 3q & 1 \end{pmatrix} = B^q$$

On a donc : $A' = B^q A^n$, et comme $A' = MQ$ avec $Q \in H$, on obtient : $M = B^q A^n Q^{-1} \in H$

D'où $G = H$

Ainsi, G est bien le sous-groupe de $GL_2(\mathbb{Z})$ engendré par A et B.

✠✠✠✠✠✠✠

Cet exercice porte sur les angles d'un pavage. Il étudie un sous-groupe du groupe des isométries du plan complexe, demandant de prouver que l'ensemble des dérivées en 0 des éléments du groupe est fini et que son cardinal divise 6. L'exercice fait appel à des notions de géométrie complexe et de théorie des groupes.

Exercice 15. (Angles d'un pavage)

Soit $G = \{z \to az + b | a, b \in \mathbb{C}, |a| = 1\}$. C'est un sous-groupe du groupe des bijections $\mathbb{C} \to \mathbb{C}$ muni de la composition. Soit $H \subseteq G$ un sous-groupe contenant deux translations selon des vecteurs $b_1, b_2 \in \mathbb{C}$ formant une famille libre sur $\mathbb{R}$. On suppose de plus que pour tout $h \in H$, soit $h(0) = 0$, soit $|h(0)| \geq 1$.

Montrer que l'ensemble $\{h'(0) | h \in H\}$ est fini.

Montrer que le cardinal de cet ensemble divise 6.

Solution. (ZINE Akram)

Lemme 1.

Soit $\Gamma \subset \mathbb{C}$ sous-groupe discret de $\mathbb{C}$. Alors, on peut construire une base b_1, b_2 avec $< b_1, b_2 > \neq 0$ pour ce groupe, telle que chaque élément du groupe soit une combinaison linéaire à coefficients entiers des éléments de cette base.

Définition 1. (Parallélépipède fondamental fermé)

Soit $b_1, b_2 \in \mathbb{C}$ des vecteurs linéairement indépendants. Le parallélépipède fondamental fermé associé à ces vecteurs est défini comme :

$$\mathcal{P}(b_1, b_2) = \{x_1 b_1 + x_2 b_2 \mid 0 \leq x_1, x_2 \leq 1\}.$$

Preuve du lemme 1.

Choisissons $x \in \Gamma$ tel qu'il n'y ait aucun vecteur du groupe entre le vecteur nul et x. Posons $b_1 = x$. Il suffit de considérer l'infimum des modules et de prendre un élément qui l'atteint. Un tel élément existe car le groupe est discret (et donc fermé).

Choisissons maintenant un vecteur y qui n'est pas dans $\mathrm{Vect}(b_1, b_2)$. Considérons le parallélépipède fondamental fermé $\mathcal{P}(b_1, y)$. Ce parallélépipède contient au moins un point du groupe (à savoir y) et contient un nombre fini de points du groupe. Choisissons un vecteur $z \in \mathcal{P}(b_1, y) \setminus \mathrm{Vect}(b_1)$ tel que la distance

$$\mathrm{dist}(z, \mathrm{Vect}(b_1))$$

soit la plus petite et que $< b_1, z > \neq 0$. Nous pouvons faire cela car nous avons seulement un nombre fini de points à choisir par compacité du Parallélépipède et discrétion du sous-groupe. Posons $b_2 = z$. On peut le choisir telle que $< b_1, b_2 > \neq 0$. En effet si $< b_1, y > \neq 0$ Alors c'est terminé. Dans le cas contraire, et si c'est y qui minimise la distance, on peut prendre dans ce cas $b_2 = y + b_1$, qui garde la même distance et qui satisfait à la contrainte $< b_1, b_2 > \neq 0$.

Il reste à montrer que tout vecteur $z \in \Gamma$ peut être exprimé comme une combinaison linéaire entière de b_1, b_2, c'est-à-dire que

$$\Gamma \subset \{x_1 b_1 + x_2 b_2 \mid x_1, x_2 \in \mathbb{Z}\}.$$

Soit $z = z_1 b_1 + z_1 b_1 \in \Gamma$ un vecteur quelconque du réseau, où $z_1, z_2 \in \mathbb{R}$. Posons $z_0 = \lfloor z_1 \rfloor b_1 + \lfloor z_2 \rfloor b_2 \in \Gamma$. Alors, $z - z_0 \in \Gamma$.

Nous allons montrer que tous les coefficients z_1, z_2 doivent être des entiers. Exprimons $z - z_0$ comme suit :

$$z - z_0 = (z_2 - \lfloor z_2 \rfloor) b_2 + \mathrm{Vect}(b_1) = (z_2 - \lfloor z_2 \rfloor) \tilde{b}_2 + \mathrm{Vect}(b_1),$$

où $\tilde{b}_2$ est le vecteur projeté de b_2 orthogonal à $\mathrm{Vect}(b_1)$.

Maintenant,

$$\mathrm{dist}(z - z_0, \mathrm{Vect}(b_1)) = (z_2 - \lfloor z_2 \rfloor)\|\tilde{b}_2\|.$$

De même,

$$\mathrm{dist}(b_2, \mathrm{Vect}(b_1)) = \|\tilde{b}_2\|.$$

En outre, comme $0 \leq z_2 - \lfloor z_2 \rfloor < 1$, nous avons :

$$\mathrm{dist}(z - z_0, \mathrm{Vect}(b_1)) < \mathrm{dist}(b_2, \mathrm{Vect}(b_1)).$$

Mais comme b_2 a été choisi comme le vecteur le plus proche de $\mathrm{Vect}(b_1)$, cela implique que $z - z_0$ doit être linéairment dépendant de b_1. Donc, $z_2 - \lfloor z_2 \rfloor = 0$, ce qui signifie que $z_2 \in \mathbb{Z}$.

On obtient aussi $z_1 - \lfloor z_1 \rfloor = 0$ car $|z - z_0| = |(z_1 - \lfloor z_1 \rfloor)b_1| < |b_1|$

Soit H' le sous-groupe de H constitué des translations.

Soit Γ le sous-groupe de $\mathbb{C}$ constitué des vecteurs associés aux translations de H'. Γ est discret, car $\forall b, b' \in H', b \neq b'$ on a $|b - b'| \geq 1$.

Le lemme nous permet de construire une nouvelle base (b'_1, b'_2), telle que :
$\forall b \in V \quad \exists (m, n) \in \mathbb{Z}, b = mb'_1 + nb'_2$.

Ainsi, toute translation dans H peut s'écrire comme :

$$z \mapsto z + mb'_1 + nb'_2, \quad m, n \in \mathbb{Z}.$$

Le sous-groupe des translations forme donc un réseau discret dans $\mathbb{C}$.

On le note par

$$\Lambda' = \{mb'_1 + nb'_2 \mid m, n \in \mathbb{Z}\}$$

Pour tout $c \in \Lambda'$, où $\Lambda' = \{mb'_1 + nb'_2 \mid m, n \in \mathbb{Z}\}$, considérons la conjugaison :

$$h \circ t_c \circ h^{-1}(z) = h(h^{-1}(z) + c) = z + ac,$$

où $t_c(z) = z + c$ et $h(z) = az + b$.

Par conséquent,

$$a\Lambda' \subseteq \Lambda'.$$

et donc en considérant a^{-1}

$$a\Lambda' = \Lambda'.$$

Soit A la matrice de rotation associée :

$$A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix},$$

où $\theta \in [0, 2\pi[$. On a $A\Lambda' = \Lambda'$. Soit f l'endomorphisme canoniquement associé à A, alors

$$f(\Lambda') = \Lambda'$$

Cela signifie que f doit envoyer chaque vecteur de la base (b'_1, b'_2) sur une combinaison entière de b'_1 et b'_2.

Soit M la matrice de f dans la base (b'_1, b'_2). La trace de la matrice A est donnée par :

$$\mathrm{Tr}(A) = \mathrm{Tr}(M) = 2\cos(\theta) \in \mathbb{Z}$$

Les seules valeurs entières possibles de $2\cos(\theta)$ pour θ réel sont :

$$2\cos(\theta) \in \{-2, -1, 0, 1, 2\}.$$

Cela correspond aux angles θ suivants modulo 2π :

$$\theta \in \left\{0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi\right\}.$$

Parmi les angles possibles, l'angle droit ne préserve pas le réseau car $< b_1, b_2 > \neq 0$, .
Supposons que Λ' soit un réseau généré par deux vecteurs non orthogonaux b_1 et b_2, et supposons par l'absurde que Λ' soit invariant par une rotation de $\pi/2$.

Puisque Λ' est invariant par rotation de $\pi/2$, nous avons :

$$\begin{cases} ib_1 = m_1 b_1 + n_1 b_2, \\ ib_2 = m_2 b_1 + n_2 b_2, \end{cases}$$

où $m_1, m_2, n_1, n_2 \in \mathbb{Z}$.

À partir de la première équation, nous obtenons :

$$(i - m_1)b_1 = n_1 b_2,$$

et à partir de la deuxième équation :

$$(i - n_2)b_2 = m_2 b_1.$$

En multipliant ces deux équations pour éliminer b_1 et b_2, nous obtenons :

$$(i - m_1)(i - n_2) = n_1 m_2.$$

En identifiant les parties réelle et imaginaire, nous obtenons :

$$m_1 n_2 - 1 = m_2 n_1 \quad \text{et} \quad m_1 + n_2 = 0.$$

Comme $m_1 + n_2 = 0$, nous pouvons substituer $n_2 = -m_1$ dans l'équation $m_1 n_2 - 1 = m_2 n_1$, ce qui donne :

$$n_1 m_2 = -(n_2^2 + 1).$$

Nous prenons le conjugué de la première équation puis multiplions la par la deuxième :

$$-(i + n_2)^2 b_1 \overline{b_2} = n_1 m_2 b_1 \overline{b_2}.$$

En développant davantage, et en utilisant la relation obtenue précedemment, nous obtenons :

$$(1 + n_2^2)\mathrm{Im}(b_1 \overline{b_2}) + n_2 b_1 \overline{b_2} = 0.$$

Ainsi, nous trouvons :

$$\begin{cases} n_2 \mathrm{Im}(b_1 \overline{b_2}) = 0, \\ (1 + n_2^2)\mathrm{Im}(b_1 \overline{b_2}) + m_2 \mathrm{Re}(b_1 \overline{b_2}) = 0. \end{cases}$$

À partir de ces équations, nous déduisons puisque $n_2 \neq 0$ que :

$$\mathrm{Re}(b_1 \overline{b_2}) = 0.$$

Cela implique que $\langle b_1, b_2 \rangle = 0$, ce qui contredit l'hypothèse selon laquelle b_1 et b_2 sont non orthogonaux.

Par conséquent, le réseau Δ ne peut pas être invariant par une rotation de $\pi/2$ s'il est généré par des vecteurs non orthogonaux b_1 et b_2.

Les angles $\theta = 0, \frac{\pi}{3}, \frac{2\pi}{3}, \pi$ correspondent à des racines de l'unité dont l'ordre divise 6 :

$$\theta = 0 \quad \text{(ordre 1)}, \quad \theta = \frac{\pi}{3} \quad \text{(ordre 6)}, \quad \theta = \frac{2\pi}{3} \quad \text{(ordre 3)}, \quad \theta = \pi \quad \text{(ordre 2)}.$$

Ainsi, l'ordre de chaque élément de A doit diviser 6. Et donc $A \subset \mathbb{U}_6$. Ainsi l'ordre de A divise 6.

✠✠✠✠✠✠✠

L'exercice 16 s'intéresse aux valeurs rationnelles du cosinus. Il demande de décrire l'ensemble des nombres rationnels r tels que $\cos(r\pi)$ est rationnel. Cet exercice combine des aspects de trigonométrie et de théorie des nombres algébriques.

Exercice 16. (Valeurs rationnelles du cosinus)

Décrire l'ensemble des nombres rationels r tels que $\cos(r\pi)$ soit rationel.

Solution. (SABIR Ilyass)

Notons $S = \{r \in \mathbb{Q} | \cos(r\pi) \in \mathbb{Q}\}$.

Puisque pour tout $n \in \mathbb{Z}$, on a $\cos((n+r)\pi) = (-1)^n \cos(r\pi)$, alors

$$S = (S \cap [0,1[) + \mathbb{Z}$$

On peut donc se concentrer seulement sur les nombres rationnels $r \in [0,1[$ tels que $\cos(r\pi) \in \mathbb{Q}$.

Soit $r \in \mathbb{Q} \cap [0,1[$ tel que $\cos(r\pi) \in \mathbb{Q}$.

Si $r = 0$, on a $\cos(r\pi) = 1 \in \mathbb{Q}$. Dans toute la suite, on suppose que $r > 0$.

Notons $\frac{r}{2} = \frac{p}{q}$ avec $p, q \in \mathbb{N}$ tels que $q \geqslant 2$, $p < \frac{q}{2}$ et $p \wedge q = 1$.

On a alors, $e^{i\pi r} = e^{2i\pi \frac{p}{q}}$, qui est une racine primitive q-ème de l'unité. Donc $e^{i\pi r}$ annule :

$$\Phi_q = \prod_{\substack{k \in [\![1,q]\!] \\ k \wedge q = 1}} \left(X - e^{2i\pi \frac{k}{q}} \right)$$

Lemme 1. (Classique)

Pour tout $n \in \mathbb{N}^*$, $\Phi_n := \prod_{\substack{k \in [\![1,q]\!] \\ k \wedge q = 1}} \left(X - e^{2i\pi \frac{k}{n}}\right)$ est irréductible dans $\mathbb{Q}[X]$.

Preuve du lemme 1.

Nous allons démontrer ce lemme en utilisant le critère d'Eisenstein après un changement de variable approprié.

Définissons le polynôme

$$\Psi_n(X) = \Phi_n(X + 1)$$

Les racines de $\Psi_n(X)$ sont les nombres

$$\alpha_k = e^{2i\pi k/n} - 1, \text{où} \quad k \wedge n = 1$$

On peut montrer facilement que les polynômes cyclotomiques ont des coefficients entiers, par suite $\Psi_n(X) \in \mathbb{Z}[X]$.

Soit p un nombre premier tel que p divise n mais p^2 ne divise pas n. Cela signifie que p est un facteur premier de n apparaissant avec multiplicité 1 dans la décomposition en facteurs premiers de n.

Nous allons montrer que $\Psi_n(X)$ satisfait le critère d'Eisenstein pour le nombre premier p :

1. Tous les coefficients a_i pour $i \geq 1$ sont divisibles par p.
2. Le coefficient dominant a_0 n'est pas divisible par p.
3. Le terme constant a_n n'est pas divisible par p^2.

Les coefficients de $\Psi_n(X)$ sont des sommes symétriques des racines α_k. Pour $i \geq 1$, les coefficients sont donnés par :

$$a_i = (-1)^i \sum_{1 \leq k_1 < \ldots < k_i \leq \varphi(n)} \alpha_{k_1} \cdots \alpha_{k_i}.$$

On va montrer que p divise chaque a_i pour $i \geq 1$.

Les racines α_k peuvent être exprimées en termes de sommes de racines de l'unité, et en exploitant les propriétés des sommes cyclotomiques modulo p, on montre que les sommes symétriques sont divisibles par p.

Le coefficient dominant a_0 est égal à 1, car $\Psi_n(X)$ est un polynôme unitaire. Donc, p ne divise pas a_0.

Le terme constant a_n est donné par

$$a_n = (-1)^n \prod_{k=1}^{\varphi(n)} \alpha_k.$$

on doit montrer que p^2 ne divise pas a_n.

Le terme constant est le produit des $\alpha_k = e^{2i\pi k/n} - 1$. On peut montrer que modulo p, ce produit est congru à p ou $-p$, mais pas divisible par p^2.

En effet, $k \wedge n = 1$, les nombres k parcourent un système complet de représentants des unités modulo n. Quand on réduit modulo p, les racines $e^{2i\pi k/n}$ deviennent des racines primitives p-ièmes de l'unité, et on peut utiliser des identités classiques des racines de l'unité pour établir la non-divisibilité par p^2.

Étant donné que toutes les conditions du critère d'Eisenstein sont satisfaites pour $\Psi_n(X)$, on conclut que $\Psi_n(X)$ est irréductible dans $\mathbb{Q}[X]$.

Comme $\Psi_n(X)$ est irréductible dans $\mathbb{Q}[X]$ et que $\Phi_n(X) = \Psi_n(X-1)$, il en résulte que $\Phi_n(X)$ est également irréductible dans $\mathbb{Q}[X]$.

D'où le lemme.

On a pour tout $k \in [\![1, q-1]\!]$ si $k \wedge q = 1$, alors $(q-k) \wedge q = 1$.

$$\begin{aligned}
\Phi_q &= \prod_{\substack{k \in [\![1,q]\!] \\ k \wedge q = 1}} \left(X - e^{2i\pi \frac{k}{q}} \right) \\
&= \prod_{\substack{k \in [\![1, \lfloor \frac{q}{2} \rfloor]\!] \\ k \wedge q = 1}} \left(X - e^{2i\pi \frac{k}{q}} \right) \left(X - e^{2i\pi \frac{(q-k)}{q}} \right) \\
&= \prod_{\substack{k \in [\![1, \lfloor \frac{q}{2} \rfloor]\!] \\ k \wedge q = 1}} \left(X^2 - 2\cos\left(2\pi \frac{k}{q} \right) X + 1 \right)
\end{aligned}$$

Puisque $\cos(\pi r) = \cos\left(2\pi \frac{p}{q}\right) \in \mathbb{Q}$, alors $X^2 - 2\cos(\pi r)X + 1 \in \mathbb{Q}[X]$, alors par irréductibilité de Φ_q, on a

$$\Phi_q = X^2 - 2\cos(\pi r)X + 1$$

En particulier $\deg(\Phi_q) = 2$.

D'autre part,

$$\deg(\Phi_q) = \sum_{\substack{k\in[\![1,q]\!] \\ k\wedge q=1}} 1 = \varphi(q)$$

Avec φ désigne l'indicatrice d'Euler.

Ainsi, $q \in \mathbb{N}$, vérifie l'équation, $\varphi(q) = 2$.

D'après le théorème fondamental de l'arithmétique, on a l'existence de $\alpha, \beta \in \mathbb{N}$ et $a_1, \ldots, a_r \in \mathbb{N}$ et $p_1, \ldots, p_r > 3$ des nombres premiers tels que

$$q = 2^\alpha 3^\beta \prod_{i=1}^{r} p_i^{a_i}$$

On a, alors

$$\varphi(q) = 2^\alpha 3^{\beta-1} \prod_{i=1}^{r} (p_i - 1) p_i^{a_i-1}$$

Or, $2^\alpha 3^{\beta-1} \prod_{i=1}^{r} (p_i - 1) p_i^{a_i-1} = 2$ si et seulement si $r = 0$ et $\alpha = 1$ et $\beta = 1$, ainsi

$$q = 6$$

Par suite $\frac{r}{2} = \frac{1}{6}$. (Car $p \in \{1, 2, 3\}$ avec $p \wedge q = 1$, donc $p = 1$)

Ainsi $r = \frac{1}{3}$, réciproquement $\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}$.

Par suite

$$S = \left\{0, \frac{1}{3}\right\} + \mathbb{Z}$$

D'où les seuls rationnels $r \in \mathbb{Q}$ tel que $\cos(r\pi) \in \mathbb{Q}$ sont décrits par l'ensemble $\left\{n, n + \frac{1}{3} | n \in \mathbb{Z}\right\}$.

Commentaire.

On a utilisé des résultats très classiques de la théorie des nombres algébriques. Pour plus de détails sur les méthodes utilisées dans cet exercice, vous pouvez consulter l'énoncé de X/ENS, épreuve Math A, MP, 2019.

✠✠✠✠✠✠✠

Cet exercice, intitulé "Théorème de Peano", traite des wronskiens et de leurs propriétés. Il demande de prouver une condition suffisante pour que

des fonctions forment une famille liée, basée sur leurs wronskiens. L'exercice fait appel à des notions d'analyse et d'algèbre linéaire.

Exercice 17. (Théorème de Peano)

Soit $I \subseteq \mathbb{R}$ un intervalle ouvert non vide. Soit $\mathcal{C}^r(I)$ le $\mathbb{R}$-espace vectoriel des fonctions sur I à valeurs réelles continuellement dérivables r fois. Pour toutes fonctions $f_1, \ldots, f_r \in \mathcal{C}^r(I)$ on définit une fonction $I \to \mathbb{R}$ par :

$$\mathcal{W}[f_1, \ldots, f_r] = \begin{vmatrix} f_1 & \cdots & f_r \\ f_1' & \cdots & f_r' \\ \vdots & & \vdots \\ f_1^{(r-1)} & \cdots & f_r^{(r-1)} \end{vmatrix}.$$

Soient $f_1, \ldots, f_r \in \mathcal{C}^r(I)$. On note $W = \mathcal{W}[f_1, \ldots, f_r]$ et, pour $1 \leq i \leq r$,

$$V_i = (-1)^i \mathcal{W}[f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_r].$$

Montrer que si V_r ne s'annule pas sur I et si $W \equiv 0$, alors les $f_1, \ldots, f_r$ forment une famille liée.

Solution. (ZINE Akram)

Dans le Wronskien :

$$V = \begin{vmatrix} f_1 & f_2 & \cdots & f_n \\ f_1' & f_2' & \cdots & f_r' \\ \vdots & \vdots & \ddots & \vdots \\ f_1^{(r-1)} & f_2^{(r-1)} & \cdots & f_r^{(r-1)} \end{vmatrix}$$

On désigne par $V_1, V_2, \ldots, V_r$ les mineurs correspondants aux éléments de la dernière ligne.

On a alors :

$$V_1 f_1^{(i)} + V_2 f_2^{(i)} + \ldots + V_r f_r^{(i)} = 0 \quad (i = 0, 1, \ldots, r-1) \quad (1)$$

Il suffit de développer par rapport à la dernière ligne pour $i = r-1$. Pour les autres valeurs de i, on peut modifier la matrice liée à V en mettant dans

la dernière ligne le vecteur $(f_1^{(i)}, \ldots, f_r^{(i)})$. Cette ligne apparaît forcément comme une duplication d'une ligne précédente, et donc le déterminant reste toujours nul.

Développons de la même façon par rapport à la première colonne. On obtient :

$$\forall 1 \leq k \leq r, \quad w = V_r f_k^{(r-1)} + \sum_{i=0}^{r-2} \alpha_i f_k^{(i)} = 0$$

où les α_i sont les mineurs liés aux $r-1$ premiers éléments de la première colonne.

Comme V_r ne s'annule pas, les f_k sont solutions d'une équation différentielle d'ordre $r-1$.

D'après l'équation (1), on a $\forall 0 \leq i \leq r-1$:

$$f_r^{(i)}(0) = -\sum_{k=1}^{r-1} \frac{V_k(0)}{V_r(0)} f_k^{(i)}(0).$$

D'où, d'après le théorème de Cauchy, on trouve que :

$$f_r(x) = -\sum_{k=1}^{r-1} \frac{V_k(0)}{V_r(0)} f_k(x).$$

D'où le résultat.

Autre méthode :

En différenciant chacune des $r-1$ premières identités de l'équation (1) et en les soustrayant à la suivante, nous obtenons :

$$V_1' f_1^{(i)} + V_2' f_2^{(i)} + \ldots + V_r' f_r^{(i)} = 0 \quad (i = 0, 1, \ldots, r-2).$$

Ajoutons maintenant ces identités ensemble, après avoir multiplié la i-ème d'entre elles (pour $i = 1, 2, \ldots, r-1$) par le premier mineur de V_r, noté $\tilde{V}_1$, correspondant à $f_1^{(i-1)}$. Cela donne :

$$\sum_{k=1}^{r} V_k' \sum_{i=1}^{r-1} \tilde{V}_1 f_k^{(i-1)} = 0.$$

La somme $\sum_{i=1}^{r-1} \tilde{V}_1 f_k^{(i-1)}$ est nulle sauf pour $k = 1$ et $k = r$, où elle vaut respectivement V_r et $-V_1$. Nous obtenons alors :

$$V_1' V_r - V_r' V_1 = 0.$$

Puisque V_r ne s'annule pas sur I, en considérant que la dérivée de $\frac{V_1}{V_r}$ est nulle, on trouve des constantes $c_1, \ldots, c_{r-1}$ telles que :

$$V_1 = -c_1 V_r, \quad V_2 = -c_2 V_r, \quad \ldots, \quad V_{r-1} = -c_{r-1} V_r.$$

Par conséquent, l'identité :

$$V_1 f_1 + V_2 f_2 + \ldots + V_r f_r = 0$$

peut être écrite sous la forme :

$$V_r(-c_1 f_1 - c_2 f_2 - \ldots - c_{r-1} f_{r-1} + f_r) = 0.$$

Et, puisque V_r ne s'annule pas, on trouve que :

$$f_r = c_1 f_1 + c_2 f_2 + \ldots + c_{r-1} f_{r-1}.$$

✠✠✠✠✠✠✠

L'exercice 18 introduit une distance sur les matrices symétriques définies positives. Il demande de prouver certaines propriétés de cette distance, notamment son invariance par conjugaison. L'exercice fait appel à des notions d'algèbre linéaire et de géométrie des espaces de matrices.

Exercice 18. (Une distance sur les matrices symétriques)

On note $\mathcal{S}_n^{++}$ l'ensemble des matrices réelles symétriques de taille n définies positives. Montrer que pour toute paire $A, B \in \mathcal{S}_n^{++}$, il existe $G \in \mathrm{GL}_n(\mathbb{R})$ tel que $B = GAG^t$.
Pour toute fonction $f : \mathbb{R}_+^* \to \mathbb{R}$ et $A \in \mathcal{S}_n^{++}$, donner un sens à $f(A)$.
À l'aide de cette définition, on pose

$$d(A, B) = \| \log(A^{-1/2} B A^{-1/2}) \|,$$

où $\|.\|$ est la norme d'opérateur relative à la norme euclidienne sur $\mathbb{R}^n$.
Montrer que

$$d(GAG^t, GBG^t) = d(A, B)$$

pour tout $G \in \mathrm{GL}_n(\mathbb{R})$, puis que d définit une distance sur $\mathcal{S}_n^{++}$.

Solution. (ZINE Akram)

Soit $R \in \mathcal{S}_n^{++}$ tel que $A = R^T R$ et soit $S \in \mathcal{S}_n^{++}$ tel que $B = S^2$. On pose $G = R^{-1}S \in \mathrm{GL}_n(\mathbb{R})$. Alors, nous avons :

$$G^T A G = S(R^{-1}RR^{-1})S = S^2 = B.$$

Ainsi, pour toute paire $A, B \in \mathcal{S}_n^{++}$, il existe $G \in \mathrm{GL}_n(\mathbb{R})$ tel que $B = G^T A G$.

Soit $G \in O_n(\mathbb{R})$ et $\lambda_1, \ldots, \lambda_n > 0$ tels que $A = G\mathrm{Diag}(\lambda_1, \ldots, \lambda_n)G^{-1}$. On définit :

$$f(A) = G\mathrm{Diag}(f(\lambda_1), \ldots, f(\lambda_n))G^{-1}.$$

Pour montrer que cette définition ne dépend pas de la décomposition, soit $\Sigma \subseteq \mathbb{R}_+$ le spectre de A. Il existe un polynôme interpolateur de Lagrange $Q \in \mathbb{R}[X]$ tel que :

$$\forall \lambda \in \Sigma, \quad f(\lambda) = Q(\lambda).$$

Ainsi,

$$f(A) = G\mathrm{Diag}(Q(\lambda_1), \ldots, Q(\lambda_n))G^{-1}.$$

Soit $R \in \mathcal{S}_n^{++}$ tel que $R^2 = A$. Alors, $R^{-1}BR^{-1} \in \mathcal{S}_n^{++}$, et on note ses valeurs propres par $0 < \lambda_1 \leq \ldots \leq \lambda_n$. On a :

$$\lambda_n = \sup_{y \neq 0} \frac{\langle By, y\rangle}{\langle Ay, y\rangle}, \quad \lambda_1 = \inf_{y \neq 0} \frac{\langle By, y\rangle}{\langle Ay, y\rangle}.$$

La matrice $S = \ln(R^{-1}BR^{-1})$ a pour valeurs propres $\ln(\lambda_1), \ldots, \ln(\lambda_n)$. La distance est alors définie par :

$$d(A, B) = \max(|\ln(\lambda_1)|, |\ln(\lambda_n)|) = \sup_{y \neq 0} \left|\ln\left(\frac{\langle By, y\rangle}{\langle Ay, y\rangle}\right)\right|.$$

Montrons que $d(G^T AG, G^T BG) = d(A, B)$ pour tout $G \in \mathrm{GL}_n(\mathbb{R})$. On a :

$$\begin{aligned} d(G^T AG, G^T BG) &= \sup_{Y \neq 0} \left|\ln\left(\frac{\langle G^T BGY, Y\rangle}{\langle G^T AGY, Y\rangle}\right)\right| \\ &= \sup_{Y \neq 0} \left|\ln\left(\frac{\langle BGY, GY\rangle}{\langle AGY, GY\rangle}\right)\right| \\ &= \sup_{Z \neq 0} \left|\ln\left(\frac{\langle BZ, Z\rangle}{\langle AZ, Z\rangle}\right)\right| \\ &= d(A, B) \end{aligned}$$

Ainsi, la distance est invariante par changement de base.

Vérification des propriétés de distance

- **Symétrie** : Il est clair que $d(A,B) = d(B,A) \geq 0$.

- **Séparation** : Si $d(A,B) = 0$, alors $\ln(R^{-1}BR^{-1}) = 0$, donc $R^{-1}BR^{-1} = I_n$, ce qui implique $A = B$.

Pour l'inégalité triangulaire, soit $C \in \mathcal{S}_n^{++}$. Pour tout $Y \in M_{n,1}(\mathbb{R})\backslash\{0\}$:

$$\frac{\langle BY, Y\rangle}{\langle AY, Y\rangle} = \frac{\langle BY, Y\rangle}{\langle CY, Y\rangle} \times \frac{\langle CY, Y\rangle}{\langle AY, Y\rangle}.$$

En appliquant le logarithme, on obtient :

$$\left|\ln\left(\frac{\langle BY, Y\rangle}{\langle AY, Y\rangle}\right)\right| \leq \left|\ln\left(\frac{\langle BY, Y\rangle}{\langle CY, Y\rangle}\right)\right| + \left|\ln\left(\frac{\langle CY, Y\rangle}{\langle AY, Y\rangle}\right)\right|.$$

En prenant la borne supérieure, on obtient :

$$d(A,B) \leq d(A,C) + d(C,B).$$

Cela prouve que $d(A,B)$ définit bien une distance sur $S_{++}^n(\mathbb{R})$.

✠✠✠✠✠✠✠

Cet exercice porte sur la norme de l'inverse d'une matrice à lignes unitaires. Il demande de prouver une borne sur la norme de l'inverse d'une telle matrice, sous certaines conditions sur la distance entre ses lignes. L'exercice fait appel à des notions d'algèbre linéaire et d'analyse matricielle.

Exercice 19. (Norme de l'inverse d'une matrice à lignes unitaires)

Soit A une matrice réelle carrée de taille $n \geq 1$ donc les lignes $L_1, \ldots, L_n$ sont des vecteurs unitaires. Soit $\epsilon > 0$ tel que, pour tout $1 \leq i \leq n$, la distance euclidienne de L_i au sous espace engendré par les L_j, avec $j \neq i$, est minorée par ϵ.
Montrer que A est inversible et que $\|A^{-1}x\|_2 \leq \epsilon^{-1}\|x\|_1$, pour tout $x \in \mathbb{R}^n$, où $\|x\|_1 = \sum_i |x_i|$ et $\|x\|_2^2 = \sum_i x_i^2$.

Solution. (SABIR Ilyass)

Commençons par montrer que la matrice A est inversible.

Supposons par l'absurde que A n'est pas inversible. Alors, les lignes de A sont linéairement dépendantes, c'est-à-dire qu'il existe des scalaires $\alpha_1, \alpha_2, \ldots, \alpha_n$, non tous nuls, tels que :

$$\sum_{i=1}^{n} \alpha_i L_i = 0$$

Choisissons un indice i_0 tel que $\alpha_{i_0} \neq 0$. On peut alors écrire :

$$L_{i_0} = -\frac{1}{\alpha_{i_0}} \sum_{\substack{j=1 \\ j \neq i_0}}^{n} \alpha_j L_j.$$

Ainsi, L_{i_0} appartient au sous-espace vectoriel engendré par les L_j avec $j \neq i_0$. Cela contredit le fait que la distance de L_{i_0} à ce sous-espace est strictement supérieure à $\varepsilon > 0$.

Par conséquent, A est inversible.

Soit $x = (x_1, x_2, \ldots, x_n)^\top \in \mathbb{R}^n$. Nous allons montrer que :

$$\|A^{-1}x\|_2 \leq \frac{1}{\varepsilon}\|x\|_1,$$

où $\|x\|_1 = \sum_{i=1}^n |x_i|$ et $\|x\|_2 = \left(\sum_{i=1}^n x_i^2\right)^{1/2}$.

Notons $C_j(A^{-1})$ la j-ième colonne de A^{-1}. On peut écrire :

$$A^{-1}x = \sum_{j=1}^{n} x_j C_j(A^{-1}).$$

Par l'inégalité triangulaire, on obtient :

$$\|A^{-1}x\|_2 \leq \sum_{j=1}^{n} |x_j| \|C_j(A^{-1})\|_2.$$

Il suffit donc de majorer $\|C_j(A^{-1})\|_2$ pour chaque j.

Considérons l'identité matricielle :

$$AA^{-1} = I_n,$$

En exprimant cette identité ligne par ligne, pour chaque $i \in \{1, \ldots, n\}$, on a :

$$L_i(A)A^{-1} = e_i^\top,$$

où $e_i^\top$ est le vecteur ligne ayant un 1 en i-ème position et des zéros ailleurs.

Cela signifie que pour chaque i et j :

$$L_i(A) \cdot C_j(A^{-1}) = \delta_{ij},$$

où δ_{ij} est le symbole de Kronecker (égal à 1 si $i = j$ et 0 sinon).

Ainsi, pour $j \neq i$, on a :

$$L_i(A) \cdot C_j(A^{-1}) = 0,$$

ce qui implique que $C_j(A^{-1})$ est orthogonal à $L_i(A)$.

Pour $j = i$, on a :

$$L_i(A) \cdot C_i(A^{-1}) = 1.$$

Puisque les lignes $L_i(A)$ sont des vecteurs unitaires, la distance δ_i de $L_i(A)$ au sous-espace engendré par les $L_j(A)$ avec $j \neq i$ est donnée par :

$$\delta_i = \frac{1}{\|C_i(A^{-1})\|_2}.$$

En effet, $C_i(A^{-1})$ est un vecteur normal au sous-espace engendré par les $L_j(A)$ avec $j \neq i$, et sa norme est l'inverse de la distance de $L_i(A)$ à ce sous-espace.

Étant donné que $\delta_i \geq \varepsilon$, on obtient :

$$\|C_i(A^{-1})\|_2 \leq \frac{1}{\varepsilon}.$$

Cette inégalité est valable pour tout $i \in \{1, \ldots, n\}$.

En combinant les résultats précédents, on a :

$$\|A^{-1}x\|_2 \leq \sum_{j=1}^{n} |x_j| \|C_j(A^{-1})\|_2 \leq \frac{1}{\varepsilon} \sum_{j=1}^{n} |x_j| = \frac{1}{\varepsilon}\|x\|_1.$$

Ainsi, pour tout $x \in \mathbb{R}^n$, on a bien démontré que :

$$\|A^{-1}x\|_2 \leq \frac{1}{\varepsilon}\|x\|_1.$$

✠✠✠✠✠✠✠

L'exercice 20 traite de la construction de suites de disques et de carrés. Il demande de prouver l'existence de suites de carrés dans un disque et de disques dans un carré, satisfaisant certaines conditions sur leurs aires et leurs intersections. L'exercice fait appel à des notions de géométrie et d'analyse.

Exercice 20. (Disques et carrés)

Soit D le disque fermé de centre 0 et rayon 1 dans $\mathbb{R}^2$. Montrer qu'il existe une suite $C_0, C_1, \ldots$ de carrés de $\mathbb{R}^2$ tels que :

1. $\forall i \geq 0, C_i \subseteq D$;
2. $\forall i, j \geq 0 : i \neq j \Rightarrow \mathring{C}_i \cap \mathring{C}_j = \varnothing$;
3. $\sum_{i \geq 0} \text{Aire}(C_i) = \pi$.

Soit $C = [-1, 1]^2$. Montrer qu'il existe une suite $D_0, D_1, \ldots$ de disques de $\mathbb{R}^2$ tels que :

1. $\forall i \geq 0, D_i \subseteq C$;
2. $\forall i, j \geq 0 : i \neq j \Rightarrow \mathring{D}_i \cap \mathring{D}_j = \varnothing$;
3. $\sum_{i \geq 0} \text{Aire}(D_i) = 4$.

Solution. (ZINE Akram)

Lemme 1. Pour chaque point $(x, y) \in \mathbb{R}^2$ et pour tout entier $n \geq 1$, il existe au plus deux carrés dyadiques de taille 2^{-n} qui contiennent le point (x, y), et ce point ne peut être intérieur à deux carrés en même temps.

Preuve du lemme 1.

Un carré dyadique de taille 2^{-n} dans $\mathbb{R}^2$ est de la forme :

$$C_{k_1,k_2} = \left[\frac{k_1}{2^n}, \frac{k_1+1}{2^n}\right] \times \left[\frac{k_2}{2^n}, \frac{k_2+1}{2^n}\right],$$

où $k_1, k_2 \in \mathbb{Z}$. Les carrés dyadiques forment une grille qui couvre tout le plan.

Pour chaque point $(x, y) \in \mathbb{R}^2$, nous devons trouver les indices $k_1, k_2 \in \mathbb{Z}$ tels que le carré dyadique C_{k_1,k_2} contient le point. Le critère pour que (x, y)

soit dans ce carré est :

$$\frac{k_1}{2^n} \leq x < \frac{k_1+1}{2^n} \quad \text{et} \quad \frac{k_2}{2^n} \leq y < \frac{k_2+1}{2^n}.$$

Les indices k_1 et k_2 qui satisfont les inégalités ci-dessus sont donnés par :

$$k_1 = \lfloor 2^n x \rfloor \quad \text{et} \quad k_2 = \lfloor 2^n y \rfloor,$$

où $\lfloor \cdot \rfloor$ est la fonction partie entière.

1- Pour montrer qu'il existe une suite $\{C_i\}_{i\geq 0}$ de carrés vérifiant les conditions données, nous allons construire cette suite en nous basant sur des carrés dyadiques.

Considérons une suite de disques fermés D_n de centres 0 et de rayons $1 - \frac{\sqrt{2}}{2^n}$ pour $n \geq 1$. Ce rayon est choisi pour que chaque carré de coté 2^{-n} soit contenu à l'intérieur du disque unité.

Chaque disque D_n est contenu dans le disque D de rayon 1, et lorsque $n \to \infty$, les rayons de ces disques tendent vers 1, couvrant ainsi tout le disque D.

Pour chaque disque D_n, nous choisissons un ensemble fini de carrés dyadiques de côté 2^{-n} pour le couvrir, conformément au lemme. Chaque carré dyadique est de la forme :

$$\left[\frac{k_1}{2^n}, \frac{k_1+1}{2^n}\right] \times \left[\frac{k_2}{2^n}, \frac{k_2+1}{2^n}\right],$$

où $k_1, k_2 \in \mathbb{Z}$. Comme D_n est de taille finie, il peut être couvert par un nombre fini de ces carrés dyadiques de cotés 2^{-n}.

Nous commençons par couvrir le plus petit disque C_1 en utilisant des carrés dyadiques de côté $2^{-1} = \frac{1}{2}$.

Ensuite, pour chaque disque suivant D_{n+1}, nous conservons tous les carrés utilisés pour couvrir D_n et nous ajoutons de nouveaux carrés dyadiques de côté $2^{-(n+1)}$ pour couvrir la partie non couverte entre D_n et D_{n+1}. (Ceci est possible car deux carrés dyadiques différents tels que l'un n'est pas inclu dans l'autre ne peuvent s'intersecter que sur le coté).

Les nouveaux carrés ajoutés sont donc de côté $2^{-(n+1)}$, plus petits que ceux ajoutés à l'étape précédente.

L'ensemble des carrés $\{C_{n,i}\}$ est indexé par deux indices n et i, et peut être vu comme un élément de $\mathbb{N}^2$.

À chaque étape n, nous avons un ensemble fini de carrés dyadiques qui couvrent le disque D_n à savoir $((C_{1,1}, ..., C_{1,k_1}, ..., C_{n,1}, ..., C_{n,k_n})$.Puisque $\mathbb{N}^2$ est dénombrable, il existe une bijection entre $\mathbb{N}^2$ et $\mathbb{N}$.

Cela signifie que nous pouvons réorganiser la suite doublement indexée $\{C_{n,i}\}$ en une suite simple $\{C_m\}_{m\in\mathbb{N}}$, c'est-à-dire $(C_1, C_2, C_3, \ldots)$.

L'union de ces ensembles de carrés forme une couverture complète du disque D lorsque $n \to \infty$.

En effet, ces carrés couvrent le disque de rayon $1 - \frac{\sqrt{2}}{2^n}$, il existe une suite (k_i) telle que pour tout $n \geq 1$

$$\pi \left(1 - \frac{\sqrt{2}}{2^n}\right)^2 \leq \sum_{i=1}^{n} Aire(C_{k_i}) \leq \pi$$

D'où le résultat.

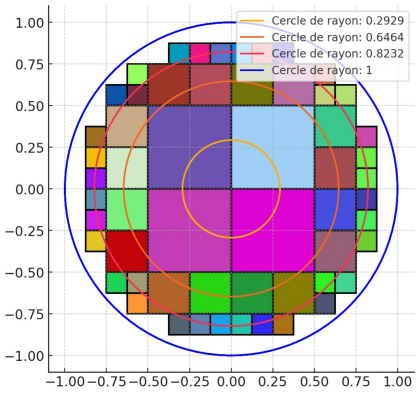


FIGURE 1 – Carrés dyadiques de tailles 1/8, 1/4, et 1/2, ainsi que des disques de rayons $1 - \frac{\sqrt{2}}{2^n}$ pour $n = 1, 2, 3$ et le disque de rayon 1.

2- Soit $C = [-1, 1]^2$ le carré centré à l'origine avec un côté de longueur 2. Nous cherchons à montrer qu'il existe une suite $\{D_i\}_{i\geq 0}$ de disques disjoints tels que :

$$\sum_{i\geq 0} \text{Aire}(D_i) = 4.$$

Considérons le carré C moins un disque inscrit de rayon 1/2, centré à l'origine. L'aire de ce disque est donc $\frac{\pi}{4}$.

On commence d'abord par remarquer que tout carré dyadique de taille 2^i partiellement extérieur à C ne peut partager une partie avec l'intérieur de C. En effet, empilons dans C 4 carrés dyadiques de cotés 1.

Ainsi, si un carré dyadique partage une partie avec l'intérieur C, il la partage forcément avec l'intérieur de l'un de ces 4 carrés, ce qui est absurde car les carrés dyadiques ne peuvent pas se croiser grace au lemme.

De manière similaire à la première partie du problème, la région restante dans le carré C peut être approximée aussi précisément que souhaité par un nombre fini de carrés dyadiques.

En effet, On va considérer une suite de disques de rayons $\frac{1}{2} + \frac{\sqrt{2}}{2^{n+1}}$ avec $n \geq 1$ (Pour qu'ils soient inclus dans le carré). Mais cette fois, on pave la région entre chaque disque D_n et le carré par des carrés dyadiques de cotés ayant pour longueur $1/2^{n+1}$, comme pour la première question, l'observation clé ici est que chaque carré qui possède des points dans cette région est forcément à l'extérieur du disque de rayon $1/2$. (On pourra s'en convaincre par inégalité triangulaire).

On pourra ainsi construire une suite de carrés dyadiques qui s'empilent complètement dans la région entre le carré et le disque de rayon $1/2$.

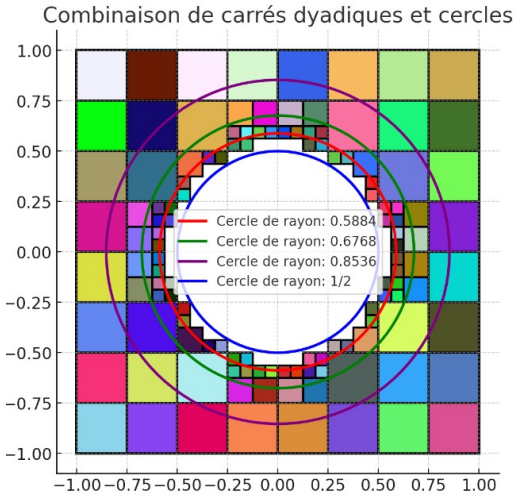


FIGURE 2 – Carrés dyadiques de tailles $1/16$, $1/8$, et $1/4$, ainsi que des disques de rayons $1 + \frac{\sqrt{2}}{2^{n+1}}$ pour $n = 1, 2, 3$ et le disque de rayon $1/2$ dans le carré $[-1, 1]^2$.

On construit la suite de disques par récurrence avec un processus diagonal :

Pour $n = 1$, on place dans notre carré les carrés dyadiques de coté $\frac{1}{2^{n+1}}$ avec $n = 1$, de façon à qu'ils ne soient pas intérieur du disque de rayon $\frac{1}{2} + \frac{\sqrt{2}}{2^{n+1}}$.

Ces carrés sont en nombre fini et correspondent aux carrés de niveau 1 pour le carré $[-1, 1]^2$(Voir la figure).

À l'intérieur de ces carrés, on place aussi par homothétie des carrés dyadiques de niveau 1 qui contiennent aussi un disque inscrit, en gardant le même rapport homothétique.

Ces carrés contiennent à leur tour d'autres carrés de niveau 1 (c'est le processus diagonal qui permet de construire notre suite disjointe de disques).

Ensuite, on inscrit des carrés dyadiques de niveau 2 dans tous les carrés, et on considère une seconde couche de profondeur, c'est-à-dire que dans les carrés dyadiques inscrits dans les carrés dyadiques déjà construits, on inscrit deux niveaux de carrés dyadiques supplémentaires, avec leurs disques associés.

On construit ainsi une suite disjointe de disques pour notre carré, noté (D'_n).

Pour tout carré C, on note $D'_n(C) = ((x_n(C), y_n(C), r_n(C)))$ la suite des disques inscrits dans ce carré, en réalisant une homothétie sur la suite construite dans le carré $[-1, 1]^2$.

Introduisons le rapport :

$$A_C = \frac{\sum_{n=1}^{\infty} \pi r_n^2(C)}{\text{aire}(C)}$$

Soit C le carré utilisé. On remarque que A_C ne dépend pas du choix du carré, par homothétie. Notons le par A. L'aire totale couverte par les disques est donnée par :

$$4A = \frac{\pi}{4} + A \sum_{i=1}^{\infty} Aire(C_n) = \frac{\pi}{4} + \left(4 - \frac{\pi}{4}\right) A,$$

où $\frac{\pi}{4}$ est l'aire du disque inscrit, et $\left(4 - \frac{\pi}{4}\right) A$ est l'aire des disques insérés dans la suite des carrés dyadiques C_n.

On trouve donc que $A = 1$.

✠✠✠✠✠✠✠

Cet exercice, intitulé “Certification de racines", propose un critère pour garantir l'existence et l'unicité d'un zéro d'une fonction différentiable dans une boule donnée. L'exercice fait appel à des notions d'analyse et de topologie.

Exercice 21. (Certification de racines)

Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une application de classe $\mathcal{C}^1$. Soit $x \in \mathbb{R}^n$, soit B la boule unité fermée. On suppose que pour tout $u, v \in B$,

$$-f(x) + v - \mathrm{d}f(x+u) \cdot v \in \tfrac{1}{2}B.$$

Montrer que f admet un unique zéro dans la boule $x + B$.

Solution. (ZINE Akram)

Soit $x \in B$, alors $\|f(x) - x\| \leq \frac{1}{2}$. En effet,

$$f(x) = f(0) + \int_0^1 df_{tx}(x)\, dt = f(0) + \int_0^1 (x - f(0) + h(t))\, dt,$$

avec $\|h(t)\| \leq \frac{1}{2}$ pour tout $t \in [0,1]$. Donc,

$$\|f(x) - x\| = \left| \int_0^1 h(t)\, dt \right| \leq \int_0^1 \|h(t)\|\, dt \leq \frac{1}{2}.$$

Soit $g(x) = \|f(x)\|^2$ sur B. Comme g est continue sur le compact B, elle admet un minimum.

Avec $v = 0$, on a $\|f(0)\| \leq \frac{1}{2}$. Si $x \in \partial B$, alors $\|f(x)\| \geq \frac{1}{2}$. Donc, le minimum de g sur B est au plus $\frac{1}{4}$. Si le minimum est atteint en 0, c'est fait, sinon il est atteint à l'intérieur de B.

Soit $a \in \overset{\circ}{B}$ un point où g atteint son minimum. Alors $dg_a = 0$, c'est-à-dire pour tout $h \in \mathbb{R}^n$, $\langle df_a(h), f(a) \rangle = 0$. Si df_a est inversible, on en déduit $f(a) = 0$.

Pour prouver que df_a est injective, supposons le contraire. Alors, il existe $w \in \ker(df_a)$, $\|w\| = 1$. On a aussi $df_a(-w) = 0$. Donc, $\|w - f(0)\| \leq \frac{1}{2}$ et $\| - w - f(0)\| \leq \frac{1}{2}$, ce qui est impossible, car $\|w - (-w)\| = 2$ alors que la sphère $S(f(0), \frac{1}{2})$ a un diamètre de 1.

Enfin, supposons qu'il existe $a, b \in B$ tels que $f(a) = f(b) = 0$ et $a \neq b$. On a :

$$0 = \int_0^1 df_{(1-t)a+tb}(b-a)\,dt = \|a-b\| \int_0^1 df_{(1-t)a+tb}\left(\frac{b-a}{\|b-a\|}\right) dt.$$

Or,

$$df_{(1-t)a+tb}\left(\frac{b-a}{\|b-a\|}\right) = \frac{b-a}{\|b-a\|} - f(0) + h(t),$$

avec $\|h(t)\| \leq \frac{1}{2}$. On obtient alors

$$\frac{b-a}{\|b-a\|} = f(0) - \int_0^1 h(t)dt.$$

Puisque $\|f(0)\| \leq \frac{1}{2}$ et $\|h\| \leq \frac{1}{2}$, on a égalité dans l'inégalité triangulaire :

$$f(0) = -\int_0^1 h(t)dt = \frac{b-a}{2\|b-a\|}.$$

En procédant de manière similaire, on trouve $f(0) = \frac{a-b}{2\|b-a\|}$, ce qui implique $a = b$, ce qui est une contradiction.

✠✠✠✠✠✠✠

L'exercice 22 porte sur la médiane de moyennes de variables aléatoires. Il demande de prouver une borne de probabilité sur l'écart entre cette médiane et la moyenne théorique. L'exercice fait appel à des notions de probabilités et de statistiques.

Exercice 22. (Médiane de moyennes)

Soient $n, m \geq 1$ des entiers et soient $X_{i,j}$, pour $1 \leq i \leq n$ et $1 \leq j \leq m$, des variables aléatoires discrètes i.i.d. de variance σ^2 et de moyenne μ. Pour $1 \leq i \leq n$, soit $Y_i = \frac{1}{m}\sum_{j=1}^m X_{i,j}$. Soit Z une médiane de l'ensemble $\{Y_1, \ldots, Y_n\}$.

Montrer que

$$\mathbb{P}\left[|Z-\mu| \leq \frac{2\sigma}{\sqrt{m}}\right] \geq 1 - \left(\frac{3}{4}\right)^{\frac{n}{2}}.$$

Solution. (ZINE Akram, SABIR Ilyass)

Espérance et Variance :

$$E[Y_i] = \mu \quad \text{et} \quad \text{Var}(Y_i) = \frac{\sigma^2}{m}.$$

Pour chaque Y_i, appliquons l'inégalité de Chebyshev pour estimer la probabilité que Y_i s'écarte de μ de plus de $\frac{2\sigma}{\sqrt{m}}$:

$$P\left(|Y_i - \mu| > \frac{2\sigma}{\sqrt{m}}\right) \leq \frac{\text{Var}(Y_i)}{\left(\frac{2\sigma}{\sqrt{m}}\right)^2} = \frac{\sigma^2/m}{4\sigma^2/m} = \frac{1}{4}.$$

Ainsi,

$$P\left(|Y_i - \mu| \leq \frac{2\sigma}{\sqrt{m}}\right) \geq \frac{3}{4}.$$

La médiane Z de l'ensemble $\{Y_1, Y_2, \ldots, Y_n\}$ sera dans l'intervalle $\left[\mu - \frac{2\sigma}{\sqrt{m}}, \mu + \frac{2\sigma}{\sqrt{m}}\right]$ si au moins la moitié des Y_i se trouvent dans cet intervalle.

Définissons S comme le nombre de Y_i satisfaisant $|Y_i - \mu| \leq \frac{2\sigma}{\sqrt{m}}$. Chaque Y_i satisfait cette condition avec une probabilité $p \geq \frac{3}{4}$, indépendamment des autres. Ainsi, S suit une loi binomiale $\mathcal{B}(n, p)$ avec $p \geq \frac{3}{4}$.

Pour obtenir une borne sur $P\left(S > \frac{n}{2}\right)$, nous allons considérer la probabilité complémentaire $P\left(S \leq \frac{n}{2}\right)$ et la majorer.

Pour tout $t > 0$, l'inégalité de Markov donne :

$$P(S \leq k) = P(e^{-tS} \geq e^{-tk}) \leq \frac{E[e^{-tS}]}{e^{-tk}}.$$

Ici, nous choisissons $k = \frac{n}{2}$.

Comme $S = \sum_{i=1}^{n} I_i$, où I_i est l'indicateur que Y_i est dans l'intervalle, et les I_i sont indépendants, nous avons :

$$E[e^{-tS}] = \prod_{i=1}^{n} E[e^{-tI_i}] = (pe^{-t} + (1-p))^n.$$

Nous devons choisir t pour minimiser la borne. Pour cela, posons :

$$f(t) = (pe^{-t} + 1 - p)e^{t/2}.$$

Calculons la dérivée de $f(t)$:

$$f'(t) = \frac{d}{dt}[(pe^{-t} + 1 - p)e^{t/2}] = e^{t/2}\left(-pe^{-t} + \frac{1}{2}(pe^{-t} + 1 - p)\right).$$

Pour trouver le minimum, résolvons $f'(t) = 0$, cela revient à résoudre l'équation

$$-pe^{-t} + \frac{1}{2}(pe^{-t} + 1 - p) = 0$$

Par suite,

$$-2pe^{-t} + pe^{-t} + 1 - p = 0$$

Ainsi,

$$pe^{-t} = 1 - p$$

Donc,

$$t = -\ln\left(\frac{1-p}{p}\right)$$

Substituons $t = -\ln\left(\frac{1-p}{p}\right)$ dans $f(t)$:

$$\begin{aligned} f(t) &= (pe^{-t} + 1 - p)e^{t/2} \\ &= \left(p \cdot \frac{1-p}{p} + 1 - p\right)\left(\frac{p}{1-p}\right)^{1/2} \\ &= 2(1-p) \cdot \frac{p}{1-p} = 2(p(1-p))^{\frac{1}{2}} \end{aligned}$$

Ainsi, on a :

$$P\left(S \leq \frac{n}{2}\right) \leq (4p(1-p))^{n/2}.$$

$p(1-p)$ décroit pour $p \geq \frac{1}{2}$
Pour $p = \frac{3}{4}$, calculons cette expression :

$$4p(1-p) = 4 \cdot \frac{3}{4} \cdot \frac{1}{4} = \frac{3}{4}.$$

Donc,

$$P\left(S \leq \frac{n}{2}\right) \leq \left(\frac{3}{4}\right)^{n/2}.$$

Par conséquent,

$$P\left(S \geq \frac{n}{2}\right) \geq P\left(S > \frac{n}{2}\right) \geq 1 - \left(\frac{3}{4}\right)^{n/2}.$$

Nous obtenons la borne souhaitée :

$$P\left(|Z - \mu| \leq \frac{2\sigma}{\sqrt{m}}\right) \geq 1 - \left(\frac{3}{4}\right)^{n/2}.$$

✠✠✠✠✠✠✠

Cet exercice s'intéresse aux sous-espaces stables d'un espace vectoriel normé de dimension finie. Il demande de prouver l'existence d'un supplémentaire stable pour le sous-espace des vecteurs invariants par deux endomorphismes commutant avec leur commutateur. L'exercice fait appel à des notions d'algèbre linéaire et de théorie des groupes.

Exercice 23. (Sous-espace stable)

Soit V un espace vectoriel normé de dimension finie. On considère deux endomorphismes de V, notés h_1 et h_2, préservant la norme, et tels que h_1 et h_2 commutent avec leur commutateur $h_1 h_2 h_1^{-1} h_2^{-1}$.
Montrer que le sous-espace des vecteurs invariants par h_1 et h_2 admet un supplémentaire également stable par h_1 et h_2.

Solution. (ZINE Akram)

Lemme 1.

Soit u un endomorphisme isométrique d'un espace vectoriel normé de dimension finie.

Notons $\mathrm{Inv}(u)$ l'espace des vecteurs invariants par u et $S(u)$ son supplémentaire.

En notant, $\mathrm{Inv}(u) = \ker(u - \mathrm{Id})$ et $S(u) = \mathrm{Im}(u - \mathrm{Id})$. Alors $V = \mathrm{Inv}(u) \oplus S(u)$.

Preuve du lemme 1.

oit $x \in \mathrm{Inv}(u) \cap S(u)$. Alors, il existe $y \in V$ tel que $u(y) = x + y$. Comme $x \in \mathrm{Inv}(u)$, on a $u(x) = x$.

Soit n un entier positif. En itérant, on obtient $u^n(y) = nx + y$.

Puisque u est une isométrie, pour tout k, on a

$$\|u^k(y)\| = \|y\|$$

On a donc

$$\|y + nx\| = \|y\|$$

Or,

$$\|nx\| \leq \|nx + y\| + \|y\| \leq 2\|y\|$$

En divisant par n et en passant à la limite, on obtient $\|x\| = 0$, donc $x = 0$.

On commence par le cas particulier où h_1 et h_2 commutent.

D'après le **lemme 1**, V est la somme directe $\mathrm{Inv}(h_1) \oplus S(h_1)$.

$\mathrm{Inv}(h_1)$ est stable par h_2 car ces endomorphismes commutent.

Soit h_2' l'endomorphisme induit sur $\mathrm{Inv}(h_1)$.

Alors, d'après le **lemme 1.**, $\mathrm{Inv}(h_1)$ est la somme directe $\mathrm{Inv}(h_2') \oplus S(h_2')$.

Or, $\mathrm{Inv}(h_2') = \mathrm{Inv}(h_1) \cap \mathrm{Inv}(h_2)$.

Finalement, V est la somme directe $\mathrm{Inv}(h_1) \cap \mathrm{Inv}(h_2) \oplus (S(h_2') + S(h_1))$. Le sous-espace supplémentaire $S(h_2') + S(h_1)$ est stable par h_1 et h_2, d'où le résultat.

Revenons à l'énoncé général. On suppose que h_1 et h_2 commutent avec leur commutateur $[h_1, h_2]$. Utilisons le **lemme** :

$$V = \mathrm{Inv}([h_1, h_2]) \oplus S([h_1, h_2])$$

$\mathrm{Inv}([h_1, h_2])$ est stable par h_1 et h_2. Considérons les endomorphismes induits h_1' et h_2'. Puisqu'ils commutent également avec $[h_1, h_2]$, ils commutent entre eux. On revient ainsi au cas particulier précédent, qui nous fournit un supplémentaire F stable par h_1' et h_2' tel que

$$\mathrm{Inv}([h_1, h_2]) = \mathrm{Inv}(h_1') \cap \mathrm{Inv}(h_2') + F = \mathrm{Inv}(h_1) \cap \mathrm{Inv}(h_2) + F$$

car, $\mathrm{Inv}(h_1) \cap \mathrm{Inv}(h_2) \subseteq \mathrm{Inv}([h_1, h_2])$.

Ainsi, $V = \mathrm{Inv}(h_1) \cap \mathrm{Inv}(h_2) + (F + S([h_1, h_2]))$

Ce qui conclut la démonstration.

✠✠✠✠✠✠✠

Cet exercice porte sur le théorème d'Hermite-Kakeya. Il demande de prouver une caractérisation des paires de polynômes qui s'entrelacent, c'est-à-dire dont les racines réelles sont simples et alternées. L'exercice fait appel à des notions de théorie des polynômes et d'analyse réelle.

Exercice 24. (Théorème d'Hermite–Kakeya)

Soient P et $Q \in \mathbb{R}[X]$ des polynômes non constants. On dit que P et Q *s'entrelacent* si :
(1) leurs racines sont réelles et simples,
(2) ils n'ont pas de racines réelles communes,
(3) entre deux racines consécutives de Q (resp. P), il y a une et une seule racine de P (resp. Q).
Montrer que si pour tout $(\lambda, \mu) \in \mathbb{R}^2 \setminus \{(0,0)\}$, les racines de $\lambda P + \mu Q$ sont toutes réelles et simples, alors P et Q s'entrelacent.
Montrer la réciproque.

Solution. (ETTOUSY Badr, ZINE Akram)

Méthode 1 : (ETTOUSY Badr)

Soit P et Q dans $\mathbb{R}[X]$.

On suppose que $\forall(\lambda, \mu) \in \mathbb{R}^2$, le polynôme $\lambda P(X) + \mu Q(X)$ a toutes ses racines réelles et simples. Montrons que les racines de P et Q sont intercalées (c'est-à-dire, entre deux racines de P il existe une racine de Q et réciproquement).

En utilisant les couples $(\lambda, \mu) = (1, 0)$ et $(\lambda, \mu) = (0, 1)$, on voit déjà que P et Q doivent avoir toutes leurs racines réelles. Les polynômes P et Q jouant des rôles symétriques, il suffit de montrer qu'entre deux racines de P, il existe au moins une racine de Q.

Soit a et b deux racines consécutives de P, et supposons que Q ne s'annule pas sur $[a, b]$. La fraction rationnelle $R(x) = \frac{P(x)}{Q(x)}$ est donc de classe C^1 sur $[a, b]$ avec $R(a) = R(b) = 0$.

D'après le théorème de Rolle, il existe $c \in]a, b[$ tel que $R'(c) = 0$. La fraction rationnelle $R(x) - R(c)$ admet donc c comme zéro de multiplicité au moins 2.

En vertu du lemme suivant, pour r assez petit, il existe sur la circonférence $|z - c| = r$ au moins quatre points tels que $\mathrm{Im}(R(z) - R(c)) = 0$, soit $\mathrm{Im}\, R(z) = 0$. L'un au moins de ces points z_0 n'est pas réel. Alors, $R(z_0) = \mu \in \mathbb{R}$. Le polynôme $P(x) - \mu Q(x)$ s'annule en un point z_0 non réel, ce qui contredit notre hypothèse.

Lemme 1.

Soit R une fraction rationnelle qui admet z_0 comme racine de multiplicité k. Alors, pour r assez petit, il existe au moins $2k$ points vérifiant $|z-z_0| = r$ et $\operatorname{Im} R(z) = 0$.

Preuve du lemme 1.

Posons $z - z_0 = re^{i\theta}$ et $\frac{1}{k!}R^{(k)}(z_0) = \rho e^{i\alpha}$.

La formule de Taylor Young nous dit alors que

$$R(z) = \rho r^k e^{i(\alpha+k\theta)}(1 + \varepsilon(z - z_0))$$

avec $\lim_{u\to 0}\varepsilon(u) = 0$. Soit $\eta > 0$ tel que $|u| < \eta$ et $|\varepsilon(u)| < 1$, et choisissons $r < \eta$.

Posons $f(\theta) = \operatorname{Im} R(z_0 + re^{i\theta})$, $\varepsilon(u) = \varepsilon_1(u) + i\varepsilon_2(u)$, avec $\varepsilon_1(u)$ et $\varepsilon_2(u)$ réels. On obtient :

$$f(\theta) = \operatorname{Im} R(z) = \rho r^k(\cos(\alpha + k\theta)\varepsilon_2(z - z_0) + \sin(\alpha + k\theta)(1 + \varepsilon_2(z - z_0)))$$

Définissons θ_m pour $m \in \{0, 1, \ldots, 2k\}$ par $\alpha + k\theta_m = m\pi + \frac{\pi}{2}$. On a alors :

$$f(\theta_m) = \rho r^k(-1)^m(1 + \beta_m)$$

avec $|\beta_m| < 1$. Donc $f(\theta_m)$ est du signe de $(-1)^m$. La fonction f change donc $2k+1$ fois de signe sur un intervalle de longueur 2π, et donc elle s'annule au moins $2k$ fois, ce qui achève la démonstration.

La réciproque

Soit (P, Q) un couple de polynômes réels simplement scindés tels qu'entre deux racines de l'un il y ait toujours au moins une racine de l'autre. Montrons que le polynôme $\lambda P + \mu Q$ reste scindé lorsque le couple (λ, μ) décrit $\mathbb{R}^2$.

Il est loisible de se ramener au cas où $\lambda \neq 0$ et où les deux polynômes sont de la forme :

$$P = \prod_{i=1}^{n}(X - a_i) \text{ and } Q = \prod_{j=1}^{m}(X - b_j)$$

avec $m = n$ ou $m = n - 1$. Nous supposerons de plus que :

$$a_1 < b_1 < a_2 < b_2 < \ldots < a_n < b_n \operatorname{si} m = n$$

cas que nous traiterons en premier.

Le signe des valeurs de la fonction rationnelle P/Q aux voisinages des infinis et des réels b_j, ainsi que son annulation en les réels a_i, montre que l'équation $\lambda P(x)+\mu Q(x) = 0$ possède au moins n racines réelles si $\lambda+\mu \neq 0$, à savoir une dans chaque intervalle $]b_j, b_{j+1}[$ et une autre dans l'un des deux intervalles $]-\infty, b_1[$ et $]b_n, +\infty[$, et au moins $n-1$ racines réelles dans le cas contraire – la dernière pouvant être alors considérée comme étant devenue infinie.

Ce nombre de racines étant toujours exactement égal au degré de $\lambda P + \mu Q$, ce dernier polynôme est donc (simplement) scindé.

Il en va tout de même si $m = n-1$ (ici d'ailleurs le degré de $\lambda P+\mu Q$ est toujours égal à n). Enfin $\lambda P + \mu Q$ est scindé (mais alors non simplement) dans le cas $\lambda = \mu = 0$.

Méthode 2 : (ZINE Akram)

Raisonnons par contraposée. Supposons que P et Q ne s'entrelacent pas. Cela signifie qu'il existe deux racines λ_1 et λ_2 de P telles qu'il n'y ait aucune racine de Q entre elles. Définissons alors la fonction $F = \frac{P}{Q}$. Puisque Q n'a pas de racine entre λ_1 et λ_2, F est bien définie sur cet intervalle. De plus, nous avons $F(\lambda_1) = F(\lambda_2) = 0$.

D'après le théorème de Rolle, il existe un point c situé entre λ_1 et λ_2 tel que $F'(c) = 0$.

Calculons alors $F'(x) = \left(\frac{P}{Q}\right)'$. En utilisant la formule de dérivation du quotient, on obtient :

$$F'(x) = \frac{P'(x)Q(x) - P(x)Q'(x)}{Q(x)^2}.$$

Comme $F'(c) = 0$, cela implique que $P'(c)Q(c)-P(c)Q'(c) = 0$. Puisque $Q(c) \neq 0$ (car Q n'a pas de racine entre λ_1 et λ_2), nous en déduisons que $P(c)Q'(c) = P'(c)Q(c)$.

Considérons alors le polynôme $T = P + \alpha Q$, où $\alpha = -F(c)$. Puisque $F'(c) = 0$, $c$est une racine double de T. Ceci contredit l'hypothèse que pour tout $(\lambda, \mu) \in \mathbb{R}^2 \setminus \{(0,0)\}$, les racines de $\lambda P + \mu Q$ sont toutes réelles et simples. Ainsi, nous avons montré par contraposée que P et Q doivent s'entrelacer.

Preuve du sens inverse

Supposons maintenant que P et Q s'entrelacent. Nous voulons montrer que pour tout $(\lambda, \mu) \in \mathbb{R}^2 \setminus \{(0,0)\}$, les racines de $R = \lambda P + \mu Q$ sont toutes réelles et simples. Supposons que λ et μ sont non nuls ; sinon, la conclusion est triviale.

Soit $n = \deg P$ et $m = \deg Q$.

On suppose, sans perte de généralité, que $n \geq m$ et que $p_1 < q_1$.

Traitons le cas $n > m$:

On a alors $m = n-1$. Pour tout $i \leq n-1$, $R(p_i) = \mu Q(p_i)$ et $R(p_{i+1}) = \mu Q(p_{i+1})$. Comme Q change de signe en q_i, R change également de signe sur $[p_i, p_{i+1}]$ et admet donc une racine sur cet intervalle. Ceci étant vrai pour tout i, R admet $n-1$ racines réelles distinctes.

Si n est pair, soit p et q les coefficients dominants de P et Q respectivement. On a $\frac{R}{\mu q}(p_1) < 0$ et $\lim\limits_{x \to -\infty} \frac{R}{\lambda p}(x) > 0$ ainsi que $\frac{R}{\mu q}(p_n) > 0$ et $\lim\limits_{x \to \infty} \frac{R}{\lambda p}(x) > 0$. Par conséquent, l'un des deux couples $(\lim\limits_{x \to -\infty} R(x), R(p_1))$ ou $(R(p_n), \lim\limits_{x \to \infty} R(x))$ possède deux éléments de signes opposés. Le théorème des valeurs intermédiaires implique alors l'existence d'une $n^{\text{ième}}$ racine.

Si n est impair, la conclusion reste la même.

Ainsi, R possède n racines réelles distinctes et son degré est n, d'où le résultat.

Le cas $n = m$ se traite de la même façon en prouvant que $n-1$ racines de R se trouvent dans les intervalles $[q_i, q_{i+1}]$. Pour la racine restante, on raisonne sur les couples $(\lim\limits_{x \to -\infty} R(x), R(q_1))$ et $(R(q_n), \lim\limits_{x \to \infty} R(x))$.

✠✠✠✠✠✠✠

L'exercice 25 s'intéresse à un groupe particulier de polynômes. Il demande de décrire le groupe des éléments inversibles dans un certain anneau de fractions rationnelles à coefficients dans $\mathbb{Z}/p^2\mathbb{Z}$, et de prouver que ce groupe n'est pas finiment engendré. L'exercice fait appel à des notions d'algèbre et de théorie des groupes.

Exercice 25. (Un groupe de polynômes)

Soit p un nombre premier. On considère l'anneau A des fractions rationnelles en X à coefficients dans $\mathbb{Z}/p^2\mathbb{Z}$ de la forme $X^{-k}P(X)$, avec P un polynôme. Décrire le groupe $A^\times$ des éléments inversibles (pour la multiplication) et montrer qu'il n'est pas engendré par un nombre fini d'éléments.

Solution. (ZINE Akram)

Lemme 1.

Soit $G = \langle g_1, g_2, \ldots, g_n \rangle$ un groupe abélien finiment engendré et soit N un sous-groupe de G. Alors, N est également finiment engendré.

Preuve du lemme 1.

Nous procédons par récurrence sur le nombre n de générateurs de G.

Le cas de base est trivial cas tout sous groupe d'un groupe cyclique est cyclique.

Supposons maintenant que le lemme est vrai pour tout groupe abélien finiment engendré avec $n-1$ générateurs.

Soit $G = \langle g_1, g_2, \ldots, g_n \rangle$ et soit N un sous-groupe de G. Considérons le sous-groupe

$$M = N \cap \langle g_2, \ldots, g_n \rangle.$$

Ce sous-groupe M est un sous-groupe de $\langle g_2, \ldots, g_n \rangle$, qui est un groupe abélien finiment engendré avec $n-1$ générateurs.

Par hypothèse de récurrence, M est donc finiment engendré.

Soit $M = \langle x_1, x_2, \ldots, x_m \rangle$ avec $x_i \in M$. Ensuite, considérons les éléments de N qui impliquent g_1. Définissons l'ensemble

$$A = \{a \in \mathbb{Z} \mid \exists b_2, \ldots, b_n \in \mathbb{Z}\text{tels que } g_1^a g_2^{b_2} \ldots g_n^{b_n} \in N\}.$$

Cet ensemble A est un sous-groupe de $\mathbb{Z}$, et tout sous-groupe de $\mathbb{Z}$ est de la forme $d\mathbb{Z}$ pour un certain entier d.

Par conséquent, il existe un entier d tel que $A = d\mathbb{Z}$. Cela signifie qu'il existe des entiers $b_2, \ldots, b_n$ tels que

$$x = g_1^d g_2^{b_2} \ldots g_n^{b_n} \in N.$$

Nous affirmons maintenant que $N = \langle x_1, \ldots, x_m, x \rangle$. Prenons un élément quelconque $g \in N$. Comme $g \in G$, il peut s'écrire sous la forme

$$g = g_1^{c_1} g_2^{c_2} \ldots g_n^{D_n}.$$

Par la définition de A, nous avons $c_1 \in A = d\mathbb{Z}$, donc il existe un entier h tel que $c_1 = dh$. Considérons alors

$$gx^{-h} = g_1^{c_1 - dh} g_2^{c_2} \ldots g_n^{D_n} = g_2^{c_2} \ldots g_n^{D_n}.$$

Cet élément appartient à M, qui est engendré par $x_1, \ldots, x_m$. Ainsi, nous avons

$$g = x^h (x_1^{e_1} x_2^{e_2} \ldots x_m^{e_m}),$$

où $e_i \in \mathbb{Z}$. Cela montre que chaque élément de N peut être écrit comme une combinaison des éléments $x_1, \ldots, x_m, x$.

Par conséquent, N est finiment engendré, ce qui conclut la preuve du lemme.

Revenons à l'exercice.

Pour caractériser les éléments inversibles de A, nous devons montrer que $X^{-k}P(X)$ est inversible si et seulement si P a exactement un coefficient non divisible par p. Supposons que $X^{-k}P(X)$ soit inversible : il existe alors un polynôme $Q(X)$ et un entier natuel l tels que

$$(X^{-k}P(X))(X^{-l}Q(X)) = 1_A.$$

Cela implique que tous les coefficients de $PQ - X^{k+l}$ sont des multiples de p^2. En réduisant modulo p, on trouve que $PQ = X^{k+l}$ dans $\mathbb{F}_p[X]$. Comme $\mathbb{F}_p$ est un corps et que X est irréductible dans $\mathbb{F}_p[X]$, cela signifie que $P = \alpha X^i$ pour un certain $\alpha \in \mathbb{F}_p \setminus \{0\}$. Ainsi, P possède exactement un coefficient non divisible par p.

Réciproquement, supposons que $P = \alpha X^i + pQ(X)$ avec α non divisible par p.

Soit b l'inverse de a modulo p^2. On trouve modulo p^2 que $P(X) = aX^i(1 + pbX^{-i}Q(X))$ En posant $y = bX^{k-i}(1 - pbX^{-i}Q(X))$. On trouve que $(X^{-k}P(X))y = 1_A$, prouvant que $X^{-k}P(X)$ est inversible.

Considérons maintenant le sous-groupe S de $A^\times$.

$$S = \{\alpha + pQ(X) \mid \alpha \in \mathbb{Z},\ \alpha \neq 0 \pmod p,\ Q(X) \in \mathbb{Z}[X]\}$$

Considérons maintenant que le sous-groupe S est généré par un ensemble fini d'éléments $s_1, s_2, \ldots, s_n$, où chaque s_i est de la forme :

$$s_i = \alpha_i + pQ_i(X)$$

avec $\alpha_i \in \mathbb{Z}$, $\alpha_i \neq 0 \pmod p$, et $Q_i(X) \in \mathbb{Z}[X]$. On suppose que ces s_i forment un système de générateurs de S.

Cependant, une contradiction émerge lorsque l'on examine le produit de deux générateurs s_i et s_j. Prenons deux éléments $s_i = \alpha_i + pQ_i(X)$ et $s_j = \alpha_j + pQ_j(X)$ dans S, et considérons leur produit :

$$s_i s_j = (\alpha_i + pQ_i(X))(\alpha_j + pQ_j(X)) = \alpha_i\alpha_j + p(\alpha_i Q_j(X) + \alpha_j Q_i(X)) + p^2 Q_i(X)Q_j(X)$$

Le terme $p^2 Q_i(X)Q_j(X)$ disparaît dans l'anneau $\mathbb{Z}/p^2\mathbb{Z}$. Ainsi, le produit devient :

$$s_i s_j = \alpha_i\alpha_j + p(\alpha_i Q_j(X) + \alpha_j Q_i(X))$$

Le degré du polynôme reste borné par $M = \max(\deg Q_i)_{1\leq i\leq n}$. Ceci est valable pour un produit aussi long que l'on souhaite.

En considérant le polynôme $1+pQ^{M+1}(X)$. Il est dans S mais ne peut être généré par un produit des générateurs de S. Et cela est une contradiction.

✠✠✠✠✠✠✠

Cet exercice comporte deux parties distinctes. La première traite des matrices de trace nulle dans $\mathrm{SL}_2(\mathbb{Z})$, demandant de prouver une propriété de conjugaison. La seconde partie concerne les sommes de deux carrés, demandant de prouver une condition suffisante pour qu'un entier soit la somme de deux carrés. L'exercice fait appel à des notions d'algèbre linéaire et de théorie des nombres.

Exercice 26. (Matrices de traces nulles et sommes de deux carrés)

Soient $A, B \in \mathrm{SL}_2(\mathbb{Z})$ (le groupe des matrices 2×2 à coefficients entiers et déterminant 1).

1. Montrer que si $\mathrm{Tr}(A) = \mathrm{Tr}(B) = 0$, alors A est conjuguée à B ou $-B$.

2. Montrer que si $n > 1$ et x sont des entiers tels que $x^2 \equiv -1 \pmod{n}$, alors il existe des entiers a et b tels que $n = a^2 + b^2$.

Solution. (ETTOUSY Badr - ZINE Akram)

1. Considérons $x, y, a, b, c, d \in \mathbb{Z}$, et définissons $\alpha_{x,y} := \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2$, et $A := \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Supposons que $b > 0$. On considère $M_{x,y} = (\alpha, A\alpha)$ et on souhaite démontrer que :

$$\det M_{x,y} bx^2 + (d-a)xy - cy^2 = 1$$

En utilisant la complétion du carré et par le fait que $a + d = 0$ et $a^2 + bc = -1$, que :

$$\det M_{x,y} = \frac{(bx - ay)^2 + y^2}{b}$$

Ainsi, $\det M_{x,y} > 0$ pour tout $(x, y) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

Détermination de e

Définissons $e = \inf_{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}} \det M_{x,y}$. Nous allons prouver le lemme suivant :

Lemme 1.

$e = \inf_{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\}} \det M_{x,y}$ est atteint et on a $3e^2 \leq -4(bc + a^2)$.

Preuve du lemme 1.

Notons $m = \inf_{(x,y)\in\mathbb{R}^2\setminus\{(0,0)\}} \det M_{x,y}$. Il est atteint car le cercle unité de

$\mathbb{R}^2$ est compact. Par homogénéité de la forme quadratique, on a

$$\det M_{x,y} \geq m(x^2+y^2)$$

Soit N un entier naturel tel que $N \geq \sqrt{\frac{e+1}{m}}$. D'après ce qui précède, si $(x,y) \in \mathbb{Z}^2$ et $|x| > N$ ou $|y| > N$, alors $\det M_{x,y} \geq e+1$.

Donc, $e = \inf_{\substack{(x,y)\in\mathbb{Z}^2\setminus\{(0,0)\} \\ |x|\leq N, |y|\leq N}} \det M_{x,y}$ est atteint car l'ensemble est fini.

Soit $(\alpha,\beta) \in \mathbb{Z}^2$ tel que $\det \mathrm{M}_{\alpha,\beta} = e$. Notons $d = \mathrm{pgcd}(\alpha,\beta)$ et α', β' les entiers tels que $\alpha = d\alpha'$ et $\beta = d\beta'$. On obtient

$$e = d^2 q(\alpha',\beta') \geq d^2 e$$

Ainsi, $d = 1$. D'après le théorème de Bézout, il existe (γ,δ) tel que $\alpha\delta + \beta\delta = 1$. Posons $v = (-\delta,\gamma)$.

$P = \begin{pmatrix} \alpha & -\delta \\ \beta & \gamma \end{pmatrix}$ et P^{-1} est la matrice de passage de (u,v) à (e_1,e_2) (base canonique de $\mathbb{R}^2$). Donc, $\mathbb{Z}^2 = \mathbb{Z}u + \mathbb{Z}v$.

Il existe (a',c') tels que, dans la base (u,v) on ait $q(x,y) = ex^2 + 2a'xy + c'y^2$. On a :

$$\begin{pmatrix} e & a' \\ a' & c' \end{pmatrix} = P^\top \begin{pmatrix} b & -a \\ -a & -c \end{pmatrix} P$$

et donc $c'e - a'^2 = (\det P)^2(-bc - a^2) = -bc - a^2$.

Pour tout $(x,y) \in \mathbb{Z}^2$, on obtient

$$q(xu+yv) = e\left(x + \frac{a'}{e}y\right)^2 + \left(c' - \frac{(a')^2}{e}\right)y^2$$

En prenant $y = 1$ et en choisissant $n \in \mathbb{Z}$ tel que $|n + \frac{a'}{e}| \leq \frac{1}{2}$, on a

$$e \leq q(nu+v) \leq \frac{e}{4} + c' - \frac{(a')^2}{e}$$

et donc $3e^2 \leq -4(bc+a^2)$.

Conclusion.

Ainsi, comme $e > 0$, on a $e = 1$. D'où il existe $\alpha \in \mathbb{R}$ tel que $\det M = 1$.

La matrice A dans la base $(\alpha, A\alpha)$ est sous la forme :

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

avec $m, n \in \mathbb{Z}$. Le déterminant et la trace sont conservés par conjugaison. Ainsi, on trouve que $n = 0$ et $m = -1$.

Si $b < 0$, on considère la base $(A\alpha, \alpha)$. Dans ce cas, $-b > 0$ et on introduit une forme quadratique de la même façon (avec pour coefficient dominant $-b$). On obtient ainsi que A est conjuguée à $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ ou $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Cela implique que pour toute matrice B sans $\mathrm{SL}_2(\mathbb{Z})$ telle que $\det B = 1$ et $\mathrm{Tr}(B) = 0$, A est conjuguée à B ou $-B$.

2. Si a et b sont somme de carrés $a = x^2 + y^2$ et $b = z^2 + t^2$ alors $ab = (xz - yt)^2 + (xt + yz)^2$ On va se réduire donc au cas où n est premier.

Lemme 2.

Soit p premier. Pour tout $a \in \mathbb{Z}$, $p \nmid a$. Il existe $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$ tels que $ax \equiv y \pmod p$ ou $ax \equiv -y \pmod p$.

Preuve du lemme 2.

Considérons $S = \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}^2$. On a $p < (\lfloor\sqrt{p}\rfloor + 1)^2$, et donc $\mathrm{card}(S) > p$. D'après le principe des tiroirs, il existe $(x_1, y_1) \neq (x_2, y_2)$ telles que $ax_1 - y_1 \equiv ax_2 - y_2 \pmod p$. On prouve facilement par l'absurde que x et y sont non nuls. D'où le résultat.

Conclusion.

Revenons à notre question, soit $x \in \mathbb{Z}$ tel que $x^2 \equiv -1 \pmod p$. On a $p \nmid x$. Il existe a, b d'après le lemme tels que $xa \equiv \pm b \pmod p$. On a $x^2a^2 + a^2 = b^2 + a^2 \equiv 0 \pmod p$, et donc $a^2 + b^2 = kp$ avec $k \in \mathbb{Z}$. On a $x^2 + y^2 \geq 2$. Ainsi $k > 0$.

Nous montrons que $k = 1$. $a, b \leq \lfloor\sqrt{p}\rfloor$, d'où $a^2 + b^2 < 2p$. Or, $p/a^2 + b^2$, d'où $p = a^2 + b^2$.

✠✠✠✠✠✠✠

L'exercice 27 porte sur le théorème d'Hermite-Sylvester. Il demande d'étudier les propriétés d'une matrice construite à partir des racines d'un polynôme, notamment son rang et sa positivité. L'exercice fait appel à des notions d'algèbre linéaire et de théorie des polynômes.

Exercice 27. (Théorème d'Hermite-Sylvester)

Soit $P \in \mathbb{R}[X]$ un polynôme de degré $n \geq 1$. Soit $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ ses racines, avec multiplicité. Soit $H \in \mathbb{C}^{n\times n}$ la matrice définie par

$$H_{i,j} = \sum_{k=1}^{n} \lambda_k^{i+j}.$$

Montrer que H est une matrice symétrique réelle. Montrer que le rang de H est égal au nombre de racines distincte, et que H est positive si et seulement si toutes les racines sont réelles.

Solution. (SABIR Ilyass)

Soit $P \in \mathbb{R}[X]$ de degré $n \geqslant 1$. Soient $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ ses racines, avec multiplicité.

Montrons que la matrice H est une matrice réelle symétrique,

Pour tout $i, j \in [\![1, n]\!]$, il est clair que $H_{i,j} = H_{j,i}$. Donc H est une matrice symétrique.

Notons $\alpha_1, \ldots, \alpha_r \in \mathbb{R}$ et $\beta_1, \overline{\beta_1}, \ldots, \beta_s, \overline{\beta_s} \in \mathbb{C}\backslash\mathbb{R}$ les racines de P, et notons pour tout $i \in [\![1, r]\!]$ et pour tout $j \in [\![1, s]\!]$ ζ_i l'ordre de multiplicité de α_i et ρ_j l'ordre de multiplicité de β_j et de $\overline{\beta_j}$.

On a alors, pour tout $i, j \in [\![1, n]\!]$

$$\begin{aligned} H_{i,j} &= \sum_{k=1}^{r} \zeta_k \lambda_k^{i+j} + \sum_{k=1}^{s} \rho_k (\beta_k^{i+j} + \overline{\beta_k}^{i+j}) \\ &= \sum_{k=1}^{r} \zeta_k \lambda_k^{i+j} + 2 \sum_{k=1}^{s} \rho_k \operatorname{Re}(\beta_k^{i+j}) \\ &\in \mathbb{R} \end{aligned}$$

Donc H est une matrice réelle. Montrons que le rang de H est égal au nombre de racines distincts.

Tout d'abord, observons que chaque racine λ_k (comptée avec multipli-

cité) définit un vecteur $v_k \in \mathbb{C}^n$ dont les composantes sont :

$$v_k = \begin{pmatrix} \lambda_k^1 \\ \lambda_k^2 \\ \vdots \\ \lambda_k^n \end{pmatrix}$$

Alors, H peut s'exprimer comme :

$$H = \sum_{k=1}^{n} v_k v_k^T$$

Comme P peut avoir des racines multiples, on peut regrouper les vecteurs correspondant aux racines identiques.

Soient $\lambda^{(1)}, \ldots, \lambda^{(m)}$ les racines distinctes de P, avec des multiplicités $n_1, \ldots, n_m$ (donc $\sum_{i=1}^{m} n_i = n$). Définissons :

$$w_i = \begin{pmatrix} (\lambda^{(i)})^1 \\ (\lambda^{(i)})^2 \\ \vdots \\ (\lambda^{(i)})^n \end{pmatrix}$$

Alors, H devient :

$$H = \sum_{i=1}^{m} n_i w_i w_i^T$$

Comme chaque $w_i w_i^T$ est une matrice de rang 1, et que les w_i correspondant aux racines distinctes sont linéairement indépendants (car des racines distinctes donnent des vecteurs de puissances linéairement indépendants), le rang de H est égal au nombre de racines distinctes :

$$\text{rang}(H) = m$$

où m est le nombre de racines distinctes de P.

Pour tout vecteur $x \in \mathbb{R}^n$, on a :

$$x^T H x = \sum_{k=1}^{n} (x^T v_k)^2 \geq 0$$

Cela montre que H est semi-définie positive.

— **Si toutes les racines sont réelles :**

Les vecteurs w_i sont réels et linéairement indépendants, donc H est définie positive :

$$x^T H x > 0 \quad \text{pour tout } x \in \mathbb{R}^n \setminus \{0\}$$

— **S'il y a des racines complexes :**

Les racines complexes apparaissent en paires conjuguées $\lambda, \bar{\lambda}$. Les vecteurs correspondants v_λ et $v_{\bar{\lambda}}$ vérifient :

$$v_{\bar{\lambda}} = \overline{v_\lambda}$$

La contribution à H d'une paire de conjugués complexes est :

$$v_\lambda v_\lambda^T + v_{\bar{\lambda}} v_{\bar{\lambda}}^T$$

Cette somme est réelle et symétrique, mais introduit une dépendance linéaire, ce qui fait que H est seulement semi-définie positive. Spécifiquement, il existe des vecteurs non nuls x tels que $x^T H x = 0$, indiquant que H n'est pas définie positive.

Commentaire.

Pour montrer que H est réelle, on peut utiliser aussi le résultat classique des formules de Newton :

Lemme 1. (Formules de Newton)

Soit $N \geqslant 2$ un entier, et K un corps commutatif, $x_1, \ldots, x_N$ des éléments de K. On considère, pour tout $p \in \mathbb{N}$:

$$S_p(x_1, \ldots, x_N) := \sum_{i=1}^{N} x_i^p$$

On note $\sigma_1, \ldots, \sigma_N$ les fonctions symétriques élémentaires de $x_1, \ldots, x_N$ définies par :

$$\sigma_k(x_1, \ldots, x_N) = \sum_{1 \leqslant j_1 < \cdots < j_k \leqslant N} \prod_{l=1}^{k} x_{j_l}, \forall k = 1, \ldots, n$$

Pour tout $p \geqslant N$, on a :

$$S_p(x_1, \ldots, x_N) + \sum_{i=1}^{N} (-1)^i \sigma_i(x_1, \ldots, x_N) S_{p-i}(x_1, \ldots, x_N) = 0$$

Et pour tout $p \in [\![1, N-1]\!]$, on a :

$$S_p(x_1, \ldots, x_N) + \sum_{i=1}^{p-1} (-1)^i \sigma_i(x_1, \ldots, x_N) S_{p-i}(x_1, \ldots, x_N) + (-1)^p p\sigma_p = 0$$

Preuve du lemme 1.

Soit $N \geqslant 2$ un entier, K un corps commutatif, $x_1, \ldots, x_N$ des éléments de K, et soit $p \in \mathbb{N}$.

Pour simplifier les notations, on note simplement $S_k$au lieu de $S_k(x_1, \ldots, x_N)$ (respectivement σ_k au lieu de $\sigma_k(x_1, \ldots, x_N)$) pour tout $k = 1, \ldots, N$.

Si $n \geqslant p$, on a :

$$\prod_{i=1}^{N} (X - x_i) = X^N + \sum_{i=1}^{N} (-1)^i \sigma_i X^{N-i}$$

Donc, pour tout $j \in [\![1, N]\!]$, on a :

$$x_j^N + \sum_{i=1}^{N} (-1)^i \sigma_i x_j^{N-i} = \prod_{i=1}^{N} (x_j - x_i) = 0$$

Par suite, en mutlipliant par x^{p-N}, on obtient :

$$x_j^p + \sum_{i=1}^{N} (-1)^i \sigma_i x_j^{p-i} = 0$$

Ainsi :

$$\begin{aligned} \sum_{j=1}^{N} \left(x_j^p + \sum_{i=1}^{N} (-1)^i \sigma_i x_j^{p-i} \right) &= \sum_{j=1}^{N} x_j^p + \sum_{i=1}^{N} (-1)^i \sigma_i \sum_{j=1}^{N} x_j^{p-i} \\ &= S_p + \sum_{i=1}^{N} (-1)^i \sigma_i S_{p-i} \end{aligned}$$

D'où :

$$S_p + \sum_{i=1}^{N} (-1)^i \sigma_i S_{p-i} = 0$$

Si $p \in [\![1, N-1]\!]$, on a, pour tout $k \in [\![1, p-1]\!]$:

$$\begin{aligned}
\sigma_k S_{p-k} &= \left(\sum_{1 \leqslant j_1 < \cdots < j_k \leqslant N} \prod_{l=1}^{k} x_{j_l} \right) S_{p-k} \\
&= \sum_{1 \leqslant j_1 < \cdots < j_k \leqslant N} \sum_{m=1}^{N} \prod_{l=1}^{k} x_{j_l} x_m^{p-k} \\
&= \sum_{\substack{1 \leqslant j_1 < \cdots < j_k \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_k}} \prod_{l=1}^{k} x_{j_l} x_m^{p-k} + \sum_{i=1}^{k} \sum_{\substack{1 \leqslant j_1 < \cdots < j_k \leqslant N \\ m = j_i}} \prod_{l=1}^{k} x_{j_l} x_m^{p-k} \\
&= \sum_{\substack{1 \leqslant j_1 < \cdots < j_k \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_k}} \prod_{l=1}^{k} x_{j_l} x_m^{p-k} + \sum_{1 \leqslant j_1 < \cdots < j_k \leqslant N} \sum_{i=1}^{k} \left(\prod_{\substack{l=1 \\ l \neq i}}^{k} x_{j_l} \right) x_{j_i}^{p-k+1} \\
&= \sum_{\substack{1 \leqslant j_1 < \cdots < j_k \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_k}} \prod_{l=1}^{k} x_{j_l} x_m^{p-k} + \sum_{\substack{1 \leqslant j_1 < \cdots < j_{k-1} \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_{k-1}}} \prod_{l=1}^{k-1} x_{j_l} x_m^{p-k+1}
\end{aligned}$$

Par suite :

$$(-1)^k \sigma_k S_{p-k} = (-1)^k \sum_{\substack{1 \leqslant j_1 < \cdots < j_k \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_k}} \prod_{l=1}^{k} x_{j_l} x_m^{p-k} - (-1)^{k-1} \sum_{\substack{1 \leqslant j_1 < \cdots < j_{k-1} \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_{k-1}}} \prod_{l=1}^{k-1} x_{j_l} x_m^{p-k+1}$$

Ainsi, par téléscopage, on a :

$$\begin{aligned}
\sum_{i=1}^{p-1} (-1)^i \sigma_i S_{p-i} &= (-1)^{p-1} \sum_{\substack{1 \leqslant j_1 < \cdots < j_{p-1} \leqslant N \\ 1 \leqslant m \leqslant N, m \neq j_1, \ldots, j_{p-1}}} \prod_{l=1}^{k} x_{j_l} x_m - S_p \\
&= (-1)^{p-1} p \sigma_p - S_p
\end{aligned}$$

D'où

$$S_p + \sum_{i=1}^{p-1} (-1)^i \sigma_i S_{p-i} + (-1)^p p \sigma_p = 0$$

Montrons par récurrance sur $p \in \mathbb{N}$ que $S_p(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}$.

On a $P = \prod_{i=1}^{n} (X - \lambda_i) \in \mathbb{R}[X]$, donc pour tout $k \in [\![1, n]\!]$, $\sigma_i(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}$.

On a pour $p = 0$, $S_0(\lambda_1, \ldots, \lambda_n) = n \in \mathbb{R}$.

Soit $p \in \mathbb{N}$, supposons que $S_0, \ldots, S_p \in \mathbb{R}$, et montrons que $S_{p+1} \in \mathbb{R}$.

Si $p+1 \geqslant n$, on a

$$S_{p+1} = \sum_{i=1}^{N} (-1)^{i-1} \sigma_i(\lambda_1, \ldots, \lambda_n) S_{p-i}(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}$$

Si $p+1 < n$, on a alors

$$S_p(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^{p-1} (-1)^{i-1} \sigma_i(\lambda_1, \ldots, \lambda_n) S_{p-i}(\lambda_1, \ldots, \lambda_n) + (-1)^{p-1} p\sigma_p \in \mathbb{R}$$

D'où $S_p(\lambda_1, \ldots, \lambda_n)$ pour tout $p \in \mathbb{N}$.

Ainsi, pour tout $i, j \in [\![1, n]\!]$ on a

$$H_{i,j} = S_{i+j} \in \mathbb{R}$$

Revenons à démontrer que H est réelle, On garde les mêmes notations que dans le lemme 1.

D'après le lemme, pour tout $p \in \mathbb{N}$:

$$\begin{cases} S_p(\lambda_1, \ldots, \lambda_n) + \sum\limits_{i=1}^{N} (-1)^i \sigma_i(\lambda_1, \ldots, \lambda_n) S_{p-i}(\lambda_1, \ldots, \lambda_n) = 0 & \text{si } p \geqslant n \\ S_p(\lambda_1, \ldots, \lambda_n) + \sum\limits_{i=1}^{p-1} (-1)^i \sigma_i(\lambda_1, \ldots, \lambda_n) S_{p-i}(\lambda_1, \ldots, \lambda_n) + (-1)^p p\sigma_p = 0 & \text{si } p < n \end{cases}$$

Remarque.

Pour plus de détails, vous pouvez consulter l'épreuve Math2 du concours Mines-Ponts, Filière PC, 2021.

✠✠✠✠✠✠✠

Deuxième partie

Les exercices posés à l'oral communs ULSR

L'épreuve orale ULSR propose une variété d'exercices couvrant un large éventail de sujets mathématiques. Les exercices abordent des domaines tels que les probabilités, l'algèbre linéaire, l'analyse, la théorie des nombres et les structures algébriques. On y trouve par exemple des problèmes sur l'ordre convexe de variables aléatoires, l'étude de suites récurrentes, les propriétés de matrices symétriques, les morphismes de groupes finis, les applications contractantes et non expansives, les séries entières de fractions rationnelles, et la construction d'arbres aléatoires. Les exercices sont conçus pour évaluer non seulement la maîtrise du programme, mais aussi la capacité des candidats à raisonner, à faire preuve d'initiative et à appliquer leurs connaissances dans des contextes nouveaux. Le niveau de difficulté est élevé, reflétant les attentes du concours d'entrée aux Écoles Normales Supérieures.

Vous trouvez l'énoncé des exercices à :
https ://www.ens.psl.eu/sites/default/files/23_mp_rap_omathulsr.pdf

✠✠✠✠✠✠✠

Cet exercice explore la notion d'ordre convexe en probabilités, testant la compréhension des candidats sur les propriétés des espérances conditionnelles et leur capacité à manipuler des inégalités impliquant des fonctions convexes.

Exercice 1.

Soient X, Y deux variables aléatoires discrètes ayant un support fini. On dit que X est plus petite que Y pour l'ordre convexe, ce qui sera noté $X \leqslant_{\text{cvx}} Y$ si et seulement si

$$\mathbb{E}[f(X)] \leqslant \mathbb{E}[f(Y)] \text{ pour toute fonction convexe } f : \mathbb{R} \to \mathbb{R}$$

1. Soit $f : \mathbb{R} \to \mathbb{R}$ une fonction convexe. Montrer que :

$$f(\mathbb{E}[X]) \leqslant \mathbb{E}[f(X)]$$

2. Montrer que si $X \leqslant_{\text{cvx}} Y$ alors $\mathbb{E}[X] = \mathbb{E}[Y]$ et $\text{var}[X] \leqslant \text{var}[Y]$.
3. Montrer que si $X \leqslant_{\text{cvx}} Y$ si et seulement si $\mathbb{E}[X] = \mathbb{E}[Y]$ et pour tout $a \in \mathbb{R}$,

$$\int_a^\infty \mathbb{P}[X \geqslant x]dx \leqslant \int_a^\infty \mathbb{P}[Y \geqslant x]dx$$

4. Montrer que $X + \mathbb{E}[X] \leqslant_{\text{cvx}} 2X$

Solution. (SABIR Ilyass)

1. Montrons que $f(\mathbb{E}[X]) \leqslant \mathbb{E}[f(X)]$.

On a

$$\begin{aligned} \mathbb{E}[f(X)] &= \sum_{k=1}^{n} \mathbb{P}[X = x_k] f(x_k) \\ &\geqslant f\left(\sum_{k=1}^{n} \mathbb{P}[X = x_k] x_k\right) \\ &= f(\mathbb{E}[X]) \end{aligned}$$

D'où le résultat.

2. Supposons que $X \leqslant_{\text{cvx}} Y$. Montrons que $\mathbb{E}[X] = \mathbb{E}[Y]$ et $\text{var}[X] \leqslant \text{var}[Y]$:

Les fonction $x \longmapsto x$ et $x \longmapsto -x$ sont convexes, alors $\mathbb{E}[X] \leqslant \mathbb{E}[Y]$ et $-\mathbb{E}[X] \leqslant -\mathbb{E}[Y]$.

D'où $\mathbb{E}[X] = \mathbb{E}[Y]$

D'autre part, la fonction $x \longmapsto (x - \mathbb{E}[X])^2$ est convexe, par conséquant :

$$\begin{aligned} \text{var}[X] &= \mathbb{E}[(X - \mathbb{E}[X])^2] \\ &\leqslant \mathbb{E}[(Y - \mathbb{E}[X])^2] \\ &= \mathbb{E}[(Y - \mathbb{E}[Y])^2] \\ &= \text{var}[Y] \end{aligned}$$

3. Montrons l'équivalence : $X \leqslant_{\text{cnv}} Y$ si et seulement si $\mathbb{E}[X] = \mathbb{E}[Y]$ et pour tout $a \in \mathbb{R}$,

$$\int_a^\infty \mathbb{P}[X \geqslant x]dx \leqslant \int_a^\infty \mathbb{P}[Y \geqslant x]dx$$

$\Rightarrow$) Supposons que $X \leqslant_{\text{cnv}} Y$, alors d'arpès la question 2, on a $\mathbb{E}[X] = \mathbb{E}[Y]$.

Montrons que :

$$\int_a^\infty \mathbb{P}[X \geqslant x]dx \leqslant \int_a^\infty \mathbb{P}[Y \geqslant x]dx, \text{pour tout } a \in \mathbb{R}$$

On peut justifier rapidement que ces intégrales sont bien définis.

Soit $a \in \mathbb{R}$, et soit $x \geqslant a$, la fonction $\varphi_x : \mathbb{R} \to \mathbb{R}$ définie pour tout $t \in \mathbb{R}$, par :

$$\varphi_x(t) = \begin{cases} 0 \text{ si } t < x \\ 1 \text{ si } t \geqslant x \end{cases}$$

La fontion φ_x est convexe, par conséquent $\mathbb{E}[\varphi_x(X)] \leqslant \mathbb{E}[\varphi_x(Y)]$. En appliquant le théorème de transfert, on obtient

$$\mathbb{P}[X \geqslant x] \leqslant \mathbb{P}[Y \geqslant x]$$

De plus, les fonctions $x \to \mathbb{P}[X \geqslant x]$ et $x \to \mathbb{P}[Y \geqslant x]$ sont des fonctions en escalier et à support compact (car X et Yont un support fini). En particulier, elles sont intégrables sur $\mathbb{R}$, par suite :

$$\int_a^\infty \mathbb{P}[X \geqslant x]dx \leqslant \int_a^\infty \mathbb{P}[Y \geqslant x]dx < +\infty$$

$\Leftarrow$) Supposons que $\mathbb{E}[X] = \mathbb{E}[Y]$ et pour tout $a \in \mathbb{R}$ on a

$$\int_a^\infty \mathbb{P}[X \geqslant x]dx \leqslant \int_a^\infty \mathbb{P}[Y \geqslant x]dx \tag{1}$$

Montrons que $X \leqslant_{\text{cnv}} Y$

La condition (1), signifie que pour tout $a \in \mathbb{R}$, on a

$$\mathbb{E}[\max(X - a, 0)] \leqslant \mathbb{E}[\max(Y - a, 0)]$$

Notons, dans toute la suite de cette question, $\{x_1, \ldots, x_N\}$ l'union des deux supports finis de Xet Y, avec $N \in \mathbb{N}^*$ et $x_1 < \cdots < x_N$.

Via le théorème de transfert, le problème pourrait être réécrit comme suit :

$$\begin{cases} \sum_{k=1}^N \mathbb{P}[X = x_k]x_k \leqslant \sum_{k=1}^N \mathbb{P}[Y = x_k]x_k \\ \sum_{k=1}^N \mathbb{P}[X = x_k]\max(x_k - a, 0) \leqslant \sum_{k=1}^N \mathbb{P}[Y = x_k]\max(x_k - a, 0) \quad \text{pour tout } a \in \mathbb{R} \end{cases}$$

Cela revient à montrer le lemme suivant :

Lemme 1. Soient $x_1, \ldots, x_N \in \mathbb{R}$, $\lambda_1, \ldots, \lambda_N \geqslant 0$ et $\beta_1, \ldots, \beta_N \geqslant 0$ tels que $\sum_{k=1}^N \lambda_k = \sum_{k=1}^N \beta_k = 1$ vérifiant :

$$\begin{cases} \sum_{k=1}^N \lambda_k x_k = \sum_{k=1}^n \beta_k x_k \\ \sum_{k=1}^N \lambda_k \max(x_k - a, 0) \leqslant \sum_{k=1}^N \beta_k \max(x_k - a, 0), \text{pour tout } a \in \mathbb{R} \end{cases} \tag{2}$$

Alors, pour toute fonction $f : \mathbb{R} \to \mathbb{R}$ convexe, on a :

$$\sum_{k=1}^N \lambda_k f(x_k) \leqslant \sum_{k=1}^N \beta_k f(x_k)$$

Preuve du lemme 1.

La première condition présentée dans (2) et $\sum_{k=1}^N \lambda_k = \sum_{k=1}^N \beta_k = 1$ impliquent que pour toute fonction affine g on a :

$$\sum_{k=1}^N \lambda_k g(x_k) = \sum_{k=1}^N \beta_k g(x_k)$$

Pour passer au cas d'une fonction convexe quelconque, on va essayer d'approximer toute fonction convexe par une suite de somme de fonctions affines et des fonctions $x \longmapsto \max(x - a, 0)$, $a \in \mathbb{R}$.

Pour ce faire, on va démontrer le lemme suivant :

Lemme 2. Soient $a < b$ deux réels et $f : [a, b] \to \mathbb{R}$ une fonction convexe, alors il existe une fonction affine φ, une suite de réels positifs $(\alpha_n)_{n\in\mathbb{N}}$ et une suite de réels $(a_n)_{n\in\mathbb{N}}$ tels que :

La suite de fonctions $\left(x \longmapsto \varphi(x) + \sum_{k=0}^{n} \alpha_n \max(x - a_k, 0)\right)_{n\in\mathbb{N}}$ converge simplement vers f

Preuve du lemme 2.

La fonction f est dérivable à droite en tout point de $[a, b]$, et $f'_+ : x \in [a, b] \longmapsto \lim\limits_{\substack{y\to x \\ y>x}} \frac{f(y)-f(x)}{y-x}$ est croissante.

Considérant la fonction affine $\varphi : x \longmapsto (f'_+(a)-1)(x-a)+f(a)$. Notons $g : [a, b] \to \mathbb{R}$ la fonction définie pour tout $x \in [a, b]$ par :

$$g(x) = f(x) - \varphi(x)$$

On a $g'_+ : x \in [a, b] \longmapsto \lim\limits_{\substack{y\to x \\ y>x}} \frac{g(y)-g(x)}{y-x}$ est strictement positive, ce qui implique que g est strictement croissante sur $[a, b]$.

La fonction g est convexe, alors elle est continue sur le segment $[a, b]$. Ainsi d'après le théorème de Heine, elle est uniformement continue sur $[a, b]$. Par conséquent, pour tout $\varepsilon > 0$, il existe $\mu > 0$ tel que pour tout $x, y \in [a, b]$ si $|x - y| \leqslant \mu$ alors $|g(x) - g(y)| < \varepsilon$.

Pour tout $n \in \mathbb{N}^*$, on a l'existance de $\mu_n > 0$ tel que tel que pour tout $x, y \in [a, b]$ si $|x - y| \leqslant \mu_n$ alors $|g(x) - g(y)| < \frac{1}{n}$.

Pour la subdivision $\left(x_k = a + k\frac{b-a}{\kappa_n}\right)_{k\in[\![0,\kappa_n]\!]}$ avec $\kappa_n = \left\lfloor \frac{1}{\mu_n} \right\rfloor + 1$. On a pour tout $k \in [\![0, \kappa_n - 1]\!]$ et pour tout $x, y \in [x_k, x_{k+1}]$:

$$|g(x) - g(y)| < \frac{1}{n}$$

En particulier pour tout $x \in [x_k, x_{k+1}]$, on a

$$|g(x) - g(x_k)| < \frac{1}{n}$$

Posons pour tout $k \in [\![0, \kappa_n - 1]\!]$,

$$\gamma_k : x \longmapsto \frac{g(x_{k+1}) - g(x_k)}{x_{k+1} - x_k}(x - x_k) + g(x_k)$$

On a

$$\begin{aligned} |g(x)-\gamma_k(x)| &\leqslant |g(x)-g(x_k)| + \frac{x-x_k}{x_{k+1}-x_k}|g(x_{k+1})-g(x_k)| \\ &\leqslant \frac{2}{n} \end{aligned}$$

Lemme 3.

Soit $k \in [\![0, \kappa_n - 2]\!]$ et $x \in \mathbb{R}$, on a

$$\gamma_{k+1}(x) - \gamma_k(x) \geqslant 0 \,\text{si and seulement si}\, x \geqslant x_{k+1}$$

Et

$$\gamma_0(x) \geqslant 0 \,\text{si and seulement si}\, x \geqslant a$$

Preuve du lemme 3.

Soient $k \in [\![0, \kappa_n - 2]\!]$ et $x \in \mathbb{R}$, alors :

$$\begin{aligned} & \gamma_{k+1}(x) - \gamma_k(x) \geqslant 0 \\ \Leftrightarrow \quad & \frac{g(x_{k+2})-g(x_{k+1})}{x_{k+2}-x_{k+1}}(x-x_{k+1}) + g(x_{k+1}) \geqslant \frac{g(x_{k+1})-g(x_k)}{x_{k+1}-x_k}(x-x_k) + g(x_k) \\ \Leftrightarrow \quad & x \geqslant \frac{b-a}{\kappa_n} + x_k = x_{k+1} \end{aligned}$$

Et

$$\begin{aligned} \gamma_0(x) \geqslant 0 \quad &\Leftrightarrow \quad \frac{g(x_1)-g(x_0)}{x_1-x_0}(x-x_0) + g(x_0) \geqslant 0 \\ &\Leftrightarrow \quad x \geqslant x_0 = a \quad (\text{car } g(x_0) = 0) \end{aligned}$$

Notons pour tout $k \in [\![0, \kappa_n - 1]\!]$,

$$\begin{cases} \alpha_k = \frac{g(x_{k+1})-g(x_k)}{x_{k+1}-x_k} - \frac{g(x_k)-g(x_{k-1})}{x_k-x_{k-1}} > 0 \quad \text{si } k \in [\![1, \kappa_n - 1]\!] \\ \alpha_0 = \frac{g(x_1)-g(x_0)}{x_1-x_0} > 0 \end{cases}$$

Et pour tout $k \in [\![1, \kappa_n - 1]\!]$:

$$a_k = \frac{1}{\alpha_k}\left(g(x_k) - g(x_{k-1}) - \frac{g(x_{k+1})-g(x_k)}{x_{k+1}-x_k}x_k + \frac{g(x_k)-g(x_{k-1})}{x_k-x_{k-1}}x_{k-1}\right)$$

De plus pour tout $k \in [\![0, \kappa_n - 1]\!]$ et pour tout $x \in [x_k, x_{k+1}]$, on a :

$$\begin{aligned}\left|g(x) - \sum_{j=0}^{\kappa_n-1} \alpha_j \max(x - a_j, 0)\right| &= \left|g(x) - \sum_{j=1}^{\kappa_n-1} \max(\gamma_j(x) - \gamma_{j-1}(x), 0) - \max(\gamma_0(x), 0)\right| \\ &= \left|g(x) - \sum_{j=1}^{k} (\gamma_j(x) - \gamma_{j-1}(x)) - \gamma_0(x)\right| \\ &= |g(x) - \gamma_k(x)| \\ &\leqslant \frac{2}{n}\end{aligned}$$

Et donc pour tout $x \in [a, b]$,

$$\left|g(x) - \sum_{j=0}^{\kappa_n-1} \alpha_j \max(x - a_j, 0)\right| \leqslant \frac{2}{n}$$

D'où le lemme 2.

Revenant au lemme 1, soit f une fonction convexe. L'objectif est de montrer que :

$$\sum_{k=1}^{N} \lambda_k f(x_k) \leqslant \sum_{k=1}^{N} \beta_k f(x_k)$$

D'après le lemme 2, il existe une fonction affine φ, une suite de réels positifs $(\alpha_n)_{n\in\mathbb{N}}$ et une suite de réels $(a_n)_{n\in\mathbb{N}}$ telles que :

La suite de fonctions $\left(x \longmapsto \varphi(x) + \sum_{k=0}^{n} \alpha_n \max(x - a_k, 0)\right)_{n\in\mathbb{N}}$ converge simplement vers f

Or Pour tout n, et pour tout $i \in [\![0, n]\!]$, on a :

$$\sum_{k=1}^{N} \lambda_k \max(x_k - a_i, 0) \leqslant \sum_{k=1}^{N} \beta_k \max(x_k - a_i, 0)$$

Ainsi :

$$\sum_{i=0}^{n} \alpha_i \sum_{k=1}^{N} \lambda_k \max(x_k - a_i, 0) \leqslant \sum_{i=0}^{n} \alpha_i \sum_{k=1}^{N} \beta_k \max(x_k - a_i, 0)$$

Ce qui est équivalent à :

$$\sum_{k=1}^{N} \lambda_k \left(\sum_{i=0}^{n} \alpha_i \max(x_k - a_i, 0)\right) \leqslant \sum_{k=1}^{N} \beta_k \left(\sum_{i=0}^{n} \alpha_i \max(x_k - a_i, 0)\right)$$

Or, $\sum_{i=0}^{n} \alpha_i \max(x_k - a_i, 0) \underset{n\to+\infty}{\to} f(x_k) - \varphi(x_k)$, alors :

$$\sum_{k=1}^{N} \lambda_k (f(x_k) - \varphi(x_k)) \leqslant \sum_{k=1}^{N} \beta_k (f(x_k) - \varphi(x_k))$$

Et puisque :

$$\begin{cases} \sum_{k=1}^{N} \lambda_k \varphi(x_k) = \varphi(\mathbb{E}[X]) \\ \sum_{k=1}^{N} \beta_k \varphi(x_k) = \varphi(\mathbb{E}[Y]) \end{cases}$$

Alors :

$$\sum_{k=1}^{N} \lambda_k f(x_k) \leqslant \sum_{k=1}^{N} \beta_k f(x_k)$$

D'où le résultat.

4. Montrons que $X + \mathbb{E}[X] \leqslant_{\text{cvx}} 2X$

D'après la question précédente, il suffit de montrer que :

$$\begin{cases} \mathbb{E}[X + \mathbb{E}[X]] = \mathbb{E}[2X] \\ \mathbb{E}[\max(X + \mathbb{E}[X] - a, 0)] \leqslant \mathbb{E}[\max(2X - a, 0)] \end{cases}$$

La première équation est immédiate grâce à la linéarité de l'espérance.

Notons $\{x_1, \ldots, x_n\}$ le support fini de X avec $x_1 < \cdots < x_n$, et pour $k = 1, \ldots, n$, $\lambda_k = \mathbb{P}[X = x_k]$

D'après le théorème de Transfert, il faut montrer que pour tout $a \in \mathbb{R}$:

$$\sum_{k=1}^{n} \lambda_k \max(x_k + \mathbb{E}[X] - a, 0) \leqslant \sum_{k=1}^{n} \lambda_k \max(2x_k - a, 0)$$

Cela équivaut à montrer que pour tout tout $a \in \mathbb{R}$:

$$\sum_{k=1}^{n} \lambda_k |x_k + \mathbb{E}[X] - a| \leqslant \sum_{k=1}^{n} \lambda_k |2x_k - a| \tag{3}$$

Posons pour tout $k \in [\![1, n]\!]$: $y_k = x_k - \frac{a}{2}$, Montrer (3) est équivalent à montrer que :

$$\sum_{k=1}^{n} \lambda_k \left| y_k + \sum_{j=1}^{n} \lambda_k y_k \right| \leqslant 2 \sum_{k=1}^{n} \lambda_k |y_k|$$

D'après l'inégalité triangulaire, on a :

$$\begin{aligned}\sum_{k=1}^{n}\lambda_k\left|y_k+\sum_{j=1}^{n}\lambda_k y_k\right| &\leqslant \sum_{k=1}^{n}\lambda_k\left(|y_k|+\sum_{j=1}^{n}\lambda_j|y_j|\right)\\ &= \sum_{j=1}^{n}\lambda_k|y_k|+\sum_{j=1}^{n}\left(\sum_{k=1}^{n}\lambda_k\right)\lambda_j|y_j|\\ &= \sum_{j=1}^{n}\lambda_k|y_k|+\sum_{j=1}^{n}\lambda_j|y_j|\\ &= 2\sum_{k=1}^{n}\lambda_k|y_k|\end{aligned}$$

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice porte sur l'étude asymptotique d'une suite récurrente linéaire d'ordre deux à coefficients variables.

Exercice 2.

On considère $(a_n),(b_n)$ deux suites telles que

$$a_n = 1+o(1), \quad b_n = 1+o(1)$$

et u_n une suite de nombres réels strictement positifs telle que

$$u_{n+1} = a_n u_n + b_n u_{n-1}$$

Montrer que les suites $v_n = \frac{u_{n+1}}{u_n}$ et $w_n = \frac{1}{n}\log u_n$ convergent.

Solution. (SABIR Ilyass, ZINE Akram)

Soient $(a_n),(b_n)$ deux suites telles que $a_n = 1+o(1), \quad b_n = 1+o(1)$ et u_n une suite de nombres réels strictement positifs telle que

$$u_{n+1} = a_n u_n + b_n u_{n-1}$$

Montrons que $v_n = \frac{u_{n+1}}{u_n}$ converge,
On a pour tout $n \in \mathbb{N}^*$,

$$v_n = a_n + \frac{b_n}{v_{n-1}}$$

Donc, pour tout $n \in \mathbb{N}$, on a

$$\begin{aligned}\sup_{k=1}^{n}(v_k) &= \sup_{k=1}^{n}(a_k) + \sup_{k=1}^{n}(b_k)\sup_{k=1}^{n}\left(\frac{1}{v_{k-1}}\right) \\ &= \sup_{k=1}^{n}(a_k) + \frac{\sup\limits_{k=1}^{n}(b_k)}{\inf\limits_{k=0}^{n-1}(v_k)}\end{aligned}$$

De même,

$$\inf_{k=1}^{n}(v_k) = \inf_{k=1}^{n}(a_k) + \frac{\inf\limits_{k=1}^{n}(b_k)}{\sup\limits_{k=0}^{n-1}(v_k)}$$

Or, les deux suites $\left(\sup\limits_{k=1}^{n}(v_k)\right)_{n\in\mathbb{N}}$ et $\left(\inf\limits_{k=1}^{n}(v_k)\right)_{n\in\mathbb{N}}$ sont monotones. En particulier, elles admettent une limite dans $\mathbb{R} \cup \{-\infty, +\infty\}$, notons $s$et l leurs limites respectivement.

On a par passage à la limite lorsque $n \to +\infty$

$$s = 1 + \frac{1}{l} \text{ and } l = 1 + \frac{1}{s}$$

Donc, par positivité de s et l, on a $s = l = \frac{1+\sqrt{5}}{2}$.

D'où $(v_n)_{n\in\mathbb{N}}$ est convergente et converge vers $\frac{1+\sqrt{5}}{2}$.

Lemme 1. (lemme de Césaro)

Soit $(z_n)_{n\in\mathbb{N}^*}$ une suite de nombres réels ou complexes qui converge vers l. Alors la suite $\left(\frac{1}{n}\sum\limits_{k=1}^{n} z_n\right)_{n\in\mathbb{N}^*}$ est convergente et converge vers la même limite l.

Preuve du lemme 1.

Soit $\varepsilon > 0$, on a l'existence de $N_1 \in \mathbb{N}^*$, tel que pout tout $n \geqslant N_1$, $|z_n - l| < \frac{\varepsilon}{2}$. Par suite, pour tout $n \geqslant N_1$

$$\begin{aligned}\left|\frac{1}{n}\sum_{k=1}^{n} z_k - l\right| &\leqslant \frac{1}{n}\sum_{k=1}^{n}|z_k - l| \\ &\leqslant \frac{1}{n}\sum_{k=1}^{N_1-1}|z_k - l| + \frac{n - N_1}{2n}\varepsilon\end{aligned}$$

Or, $\frac{1}{n}\sum_{k=1}^{N_1-1}|z_k-l| \underset{n\longrightarrow+\infty}{\longrightarrow} 0$, donc il existe $N_2 \in \mathbb{N}^*$ tel que pour tout $n \geqslant N_2$, on a

$$\frac{1}{n}\sum_{k=1}^{N_1-1}|z_k-l| < \frac{\varepsilon}{2}$$

Ainsi, pour tout $n \geqslant \max(N_1, N_2)$, on a

$$\left|\frac{1}{n}\sum_{k=1}^{n} z_k - l\right| < \varepsilon$$

D'où le lemme.

En appliquant ce lemme, on obtient alors $w_n \underset{n\longrightarrow+\infty}{\sim} \frac{1}{n}\sum_{k=1}^{n}\log(v_k) \underset{n\longrightarrow+\infty}{\longrightarrow} \log\left(\frac{1+\sqrt{5}}{2}\right)$.

✠✠✠✠✠✠✠

Ce problème examine les conditions sous lesquelles on peut déduire l'existence d'une limite pour une fonction à partir d'informations sur ses dérivées successives.

Exercice 3.

On considère un entier $k \geqslant 1$ et une fonction $f \in \mathcal{C}^k(\mathbb{R},\mathbb{R})$ telle que $\sum_{j=0}^{k} f^{(j)}(x)$ admet une limite pour $x \to +\infty$. Peut-on en déduire que f admet une limite en $x \to +\infty$, selon le valeur de k ?

Solution. (SABIR Ilyass)

Soient $k \geq 1$ et $f \in C^k(\mathbb{R},\mathbb{R})$ telle que

$$S(x) = \sum_{j=0}^{k} f^{(j)}(x)$$

admet une limite finie L lorsque $x \to +\infty$.

Cas $k = 1$:

On a

$$S(x) = f(x) + f'(x) \underset{x\to+\infty}{\to} L$$

Considérons l'équation différentielle :

$$f'(x) + f(x) = S(x).$$

C'est une équation différentielle linéaire du premier ordre. Son facteur intégrant est $\mu(x) = e^x$. En multipliant les deux membres par e^x, on obtient :

$$e^x f'(x) + e^x f(x) = e^x S(x),$$

ce qui équivaut à :

$$\frac{d}{dx}(e^x f(x)) = e^x S(x).$$

En intégrant entre un point x_0 et x, on obtient :

$$e^x f(x) = \int_{x_0}^{x} e^t S(t)\,dt + C.$$

Où C est une constante.

Comme $S(x) \to L$ lorsque $x \to +\infty$, nous pouvons écrire $S(x) = L+\varepsilon(x)$, avec $\varepsilon(x) \underset{x\to+\infty}{\to} 0$.

Ainsi,

$$\int_{x_0}^{x} e^t S(t)\,dt = Le^x - Le^{x_0} + \int_{x_0}^{x} e^t \varepsilon(t)\,dt.$$

Donc,

$$e^x f(x) = Le^x - Le^{x_0} + \int_{x_0}^{x} e^t \varepsilon(t)\,dt + C,$$

D'où

$$f(x) = L + e^{-x}(-Le^{x_0} + C) + e^{-x}\int_{x_0}^{x} e^t \varepsilon(t)\,dt$$

Or, $e^{-x}(-Le^{x_0} + C) \underset{x\to+\infty}{\to} 0$, et puisque $\varepsilon(x) \underset{x\to+\infty}{\to} 0$, alors pour tout $\kappa > 0$, il existe $M \in \mathbb{R}$ tel que pour tout $x \geqslant M$, on a

$$|\varepsilon(x)| \leqslant \frac{\kappa}{2}$$

Ainsi pour tout $x \geqslant \max(M, x_0)$, on a

$$\begin{aligned}
\left|e^{-x}\int_{x_0}^{x} e^t \varepsilon(t)\,dt\right| &\leqslant e^{-x}\int_{x_0}^{x} e^t |\varepsilon(t)|\,dt \\
&\leqslant e^{-x}\int_{x_0}^{M} e^t |\varepsilon(t)|\,dt + \frac{\kappa}{2}e^{-x}\int_{M}^{x} e^t\,dt \\
&= \frac{\kappa}{2} + e^{-x}\left(\int_{x_0}^{M} e^t |\varepsilon(t)|\,dt - \frac{\kappa}{2}e^M\right)
\end{aligned}$$

Avec, $e^{-x}\left(\int_{x_0}^{M} e^t|\varepsilon(t)|\,dt - \frac{\kappa}{2}e^M\right) \underset{x\to+\infty}{\to} 0$, alors il existe $M' \in \mathbb{R}$ tel que pour tout $x \geqslant M'$

$$e^{-x}\left(\int_{x_0}^{M} e^t|\varepsilon(t)|\,dt - \frac{\kappa}{2}e^M\right) \leqslant \frac{\kappa}{2}$$

Ainsi, pour tout $x \geqslant \max(M, M', x_0)$, on a

$$\left| e^{-x} \int_{x_0}^{x} e^t \varepsilon(t)\, dt \right| \leqslant \kappa$$

D'où $e^{-x} \int_{x_0}^{x} e^t \varepsilon(t)\, dt \underset{x\to+\infty}{\to} 0$ et par conséquent $f(x) \underset{x\to+\infty}{\to} L$.

D'où f admet une limite finie lorsque $x \to +\infty$.

Cas $k = 2$:

On a

$$S(x) = f(x) + f'(x) + f''(x) \underset{x\to+\infty}{\to} L$$

Notons $Y = \begin{pmatrix} f \\ f' \end{pmatrix}$, on a alors

$$Y' + \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} Y = \begin{pmatrix} 0 \\ S \end{pmatrix}$$

Posons $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$, on a alors

$$\frac{d}{dx}(e^{Ax} Y(x)) = e^{Ax} \begin{pmatrix} 0 \\ S(x) \end{pmatrix}$$

Par suite

$$Y(x) = e^{-Ax} \int e^{Ax} \begin{pmatrix} 0 \\ S(x) \end{pmatrix} dx + C$$

Par une approche similaire au cas $k = 1$, on peut montrer facilement que $Y(x) \underset{x\to+\infty}{\to} \begin{pmatrix} L \\ 0 \end{pmatrix}$

En particulier que $f(x) \underset{x\to+\infty}{\to} L$.

Cas $k \geq 3$:

Considérons l'équation différentielle

$$\sum_{j=0}^{k} f^{(j)}(x) = 0 \quad (✠)$$

Il s'agit d'une équation différentielle linéaire d'équation caractéristique

$$\sum_{j=0}^{k} r^j = 0$$

L'ensemble des solutions de l'équation caractéristique est

$$\left\{ \exp\left(2i\pi \frac{l}{k+1}\right) | l = 1, 2, \ldots, k+1 \right\}$$

En prenant $r = \exp\left(\frac{2i\pi}{k+1}\right)$, on a alors

$$h : x \longmapsto \mathcal{R}e(\exp(rx))$$

est une solution de (✠).

Or, pour tout $x \in \mathbb{R}$, on a

$$\begin{aligned} h(x) &= \mathcal{R}e\left(\exp\left(\exp\left(\frac{2i\pi}{k+1}\right)x\right)\right) \\ &= \mathcal{R}e\left(\exp\left(\cos\left(\frac{2\pi}{k+1}\right)x + i\sin\left(\frac{2\pi}{k+1}\right)x\right)\right) \\ &= \exp\left(\cos\left(\frac{2\pi}{k+1}\right)x\right)\cos\left(\sin\left(\frac{2\pi}{k+1}\right)x\right) \end{aligned}$$

Or, $k \geqslant 3$, alors $\cos\left(\frac{2\pi}{k+1}\right) > 0$ et $\sin\left(\frac{2\pi}{k+1}\right) > 0$, donc h n'admet pas de limite en $+\infty$.

✠✠✠✠✠✠✠

Cet exercice d'algèbre linéaire explore les propriétés spectrales d'une perturbation de rang 1 d'une matrice symétrique.

Exercice 4.

Soit $A \in \mathcal{M}_n(\mathbb{R})$ une matrice réelle symétrique, à valeurs propres toutes distinctes, et $v$un vecteur tel que la matrice $A + vv^T \in \mathcal{M}_n(\mathbb{R})$ n'ait aucune valeur propre en commun avec A. Montrer que les valeurs propres de $A+vv^T$ correspondent aux zéros de la fraction rationnelle :

$$F(X) = 1 + v^T(AXI_n)^{-1}v$$

En déduire que les valeurs propres de $A + vv^T$ et celles de A sont entrelacées.

Solution. (SABIR Ilyass)

Étant donné que A est symétrique avec des valeurs propres distinctes, elle est diagonalisable par une matrice orthogonale. Ses valeurs propres sont réelles et peuvent être ordonnées comme $\lambda_1 < \lambda_2 < \ldots < \lambda_n$.

La fonction $F(X)$ est bien définie et rationnelle sauf aux valeurs propres de A, où $(A - XI_n)^{-1}$ n'est pas définie.

Soit λ une valeur propre de $A + vv^T$, il existe donc un vecteur non nul x tel que :

$$(A + vv^T)x = \lambda x.$$

Réécrivons cette équation :

$$(A - \lambda I_n)x + vv^T x = 0.$$

Posons $\alpha = v^T x$ (un scalaire), alors :

$$(A - \lambda I_n)x = -\alpha v.$$

En supposant que $(A-\lambda I_n)$ est inversible (puisque λ n'est pas une valeur propre de A), on a :

$$x = -\alpha(A - \lambda I_n)^{-1}v.$$

En substituant dans α :

$$\alpha = v^T x = -\alpha v^T (A - \lambda I_n)^{-1} v.$$

En simplifiant (car $\alpha \neq 0$) :

$$1 + v^T (A - \lambda I_n)^{-1} v = 0.$$

Ainsi, λ est un zéro de $F(X)$.

Réciproquement, supposons que $F(\lambda) = 0$ et que λ n'est pas une valeur propre de A. Définissons :

$$x = (A - \lambda I_n)^{-1} v.$$

Alors :

$$(A - \lambda I_n)x = v.$$

Calculons $(A + vv^T - \lambda I_n)x$:

$$(A - \lambda I_n)x + vv^T x = v + v(v^T x) = v + v\alpha = v(1 + \alpha).$$

Comme $F(\lambda) = 1 + \alpha = 0$, il s'ensuit que :

$$(A + vv^T - \lambda I_n)x = 0$$

ce qui signifie que λ est une valeur propre de $A + vv^T$.

Considérons la fonction rationnelle :

$$F(X) = 1 + v^T(A - XI_n)^{-1}v.$$

Nous pouvons exprimer $F(X)$ en utilisant la décomposition en valeurs propres de A. Soit $A = PDP^T$, où $D = \text{diag}(\lambda_1, \ldots, \lambda_n)$ et P est orthogonale. Alors :

$$F(X) = 1 + \sum_{i=1}^{n} \frac{w_i^2}{\lambda_i - X},$$

où $w = (w_1, \ldots, w_n)^T = P^T v$.

Entre chaque paire de valeurs propres λ_i et λ_{i+1}, la fonction $F(X)$ a une asymptote verticale (due aux pôles en λ_i) et change de signe car les termes dans la somme passent de positif à négatif ou vice versa. Par conséquent, $F(X)$ a exactement un zéro dans chaque intervalle $(\lambda_i, \lambda_{i+1})$. Puisque $A + vv^T$ a n valeurs propres et qu'aucune ne coïncide avec celles de A, cela implique que les valeurs propres de $A + vv^T$ sont entrelacées avec celles de A.

✠✠✠✠✠✠✠

Ce problème d'algèbre et de théorie des groupes demande aux candidats de dénombrer les morphismes surjectifs entre groupes finis. Il évalue la compréhension des structures algébriques et la capacité à utiliser des outils comme le théorème des restes chinois.

Exercice 5.

Soient $m \geq 1$ et $r \geq 2$ des entiers et $H_{m,r}$ l'ensemble des morphismes de groupes $(\mathbb{Z}/m\mathbb{Z})^r \to \mathbb{Z}/m\mathbb{Z}$. Calculer la proportion dans $H_{m,r}$ des morphismes surjectifs

Solution. (SABIR Ilyass)

Commençons par étudier le cas où m **est une puissance d'un nombre premier**, puis on va utiliser le théorème des restes chinois pour généraliser au cas où m est quelconque.

Soit p un nombre premier, et $k \in \mathbb{N}^*$, tel que $m = p^k$.

Le groupe $(\mathbb{Z}/p^k\mathbb{Z})^r$ est engendré par les r éléments canoniques $e_1, e_2, \ldots, e_r$, où e_i a un 1 en position i et 0 ailleurs.

Un morphisme de groupes $\phi : (\mathbb{Z}/p^k\mathbb{Z})^r \to \mathbb{Z}/p^k\mathbb{Z}$ est entièrement déterminé par les images des générateurs e_i, c'est-à-dire par les éléments $a_i = \phi(e_i) \in \mathbb{Z}/p^k\mathbb{Z}$ pour $i = 1, 2, \ldots, r$.

Comme chaque a_i peut prendre p^k valeurs possibles, le nombre total de morphismes est $(p^k)^r$.

Un morphisme ϕ est surjectif si et seulement si son image est égale à $\mathbb{Z}/p^k\mathbb{Z}$.

Dans $\mathbb{Z}/p^k\mathbb{Z}$, un élément a engendre le groupe si et seulement si a est premier avec p.

Ainsi, le morphisme ϕ est surjectif si et seulement si les a_i engendrent $\mathbb{Z}/p^k\mathbb{Z}$, c'est-à-dire si $\text{pgcd}(a_1, a_2, \ldots, a_r, p) = 1$.

Dans ce contexte, puisque p est premier, $\text{pgcd}(a_1, \ldots, a_r, p) = 1$ si et seulement si au moins un des a_i n'est pas divisible par p.

Les morphismes non surjectifs sont ceux pour lesquels tous les a_i sont divisibles par p. Cela signifie que chaque a_i appartient à $p \times \mathbb{Z}/p^k\mathbb{Z}$.

Le nombre de choix possibles pour chaque a_i divisible par p est p^{k-1} (car les multiples de p dans $\mathbb{Z}/p^k\mathbb{Z}$ sont $0, p, 2p, \ldots, (p^k - p)$).

Donc, le nombre total de morphismes non surjectifs est $(p^{k-1})^r$.

Ainsi, le nombre de morphismes surjectifs est $(p^k)^r - (p^{k-1})^r$

La proportion des morphismes surjectifs est donnée par :

$$\frac{(p^k)^r - (p^{k-1})^r}{(p^k)^r} = 1 - \left(\frac{p^{k-1}}{p^k}\right)^r = 1 - \left(\frac{1}{p}\right)^r = 1 - \frac{1}{p^r}.$$

Cas général : Soit m un entier strictement positif, avec sa décomposition en facteurs premiers :

$$m = \prod_{i=1}^{n} p_i^{k_i},$$

où les p_i sont des nombres premiers distincts et les k_i des entiers positifs.

Par le théorème des restes chinois, on a les isomorphismes de groupes :

$$\mathbb{Z}/m\mathbb{Z} \simeq \prod_{i=1}^{n} \mathbb{Z}/p_i^{k_i}\mathbb{Z},$$

et

$$(\mathbb{Z}/m\mathbb{Z})^r \simeq \prod_{i=1}^{n} (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^r.$$

Un morphisme $\phi : (\mathbb{Z}/m\mathbb{Z})^r \to \mathbb{Z}/m\mathbb{Z}$ correspond à un n-uplet de morphismes :

$$\phi = (\phi_1, \phi_2, \ldots, \phi_n),$$

où chaque $\phi_i : (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^r \to \mathbb{Z}/p_i^{k_i}\mathbb{Z}$ est un morphisme de groupes.

Le morphisme ϕ est surjectif si et seulement si chaque ϕ_i est surjectif. En effet, l'isomorphisme fourni par le théorème des restes chinois est compatible avec les morphismes, et l'image de ϕ est le produit des images des ϕ_i.

Pour chaque i, d'après le résultat du cas particulier, la proportion des morphismes ϕ_i surjectifs est :

$$1 - \frac{1}{p_i^r}.$$

Comme les morphismes ϕ_i sont indépendants pour des premiers distincts, la proportion totale des morphismes surjectifs est le produit des proportions individuelles :

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

✠✠✠✠✠✠✠

Cet exercice traite d'une inégalité matricielle classique, connue sous le nom de théorème de Schur-Horn. Il teste la compréhension des candidats sur les propriétés des matrices symétriques et leur capacité à manipuler des inégalités impliquant des valeurs propres.

Exercice 6.

Soit $A = (a_{i,j})_{1 \leqslant i,j \leqslant n} \in S_n(\mathbb{R})$ une matrice réelle symétrique. On note $\lambda_1(A) \leqslant \cdots \leqslant \lambda_n(A)$ les valeurs propres de A. Montrer pour tout $k \in \{1, \ldots, n\}$ l'inégalité

$$\lambda_1(A) + \cdots + \lambda_k(A) \leqslant a_{1,1} + \cdots + a_{k,k} \leqslant \lambda_{n-k+1}(A) + \cdots + \lambda_n(A)$$

Solution. (SABIR Ilyass)

Pour tout $A \in S_n(\mathbb{R})$. Remarquons d'abord que si $\lambda_1(A) \leq \ldots \leq \lambda_n(A)$ sont les valeurs propres de A, alors les valeurs propres de $-A \in S_n(\mathbb{R})$ sont $-\lambda_n(A) \leq \ldots \leq -\lambda_1(A)$.

Donc, si

$$\lambda_1(A) + \ldots + \lambda_k(A) \leq a_{1,1} + \ldots + a_{k,k}$$

pour tout $k \in \{1, \ldots, n\}$ et pour toute matrice $A \in S_n(\mathbb{R})$, alors, puisque $-A \in S_n(\mathbb{R})$, on a pour tout $k \in \{1, \ldots, n\}$:

$$-\lambda_{n-k+1}(A) - \ldots - \lambda_n(A) \leq -a_{1,1} - \ldots - a_{k,k}.$$

Donc, il suffit de montrer que $\lambda_1(A) + \ldots + \lambda_k(A) \leq a_{1,1} + \ldots + a_{k,k}$ pour tout $k \in [\![1, n]\!]$

Définition 1.

Soit $m \in \mathbb{N}^*$ tel que $m \leq n$, et soit V un sous-espace vectoriel de $\mathbb{R}^n$ de dimension m. On définit $\mathrm{Tr}(A|_V)$ comme suit :

$$\mathrm{Tr}(A|_V) := \sum_{i=1}^{m} v_i^T A v_i$$

où $v_1, \ldots, v_m$ constituent une base orthonormée quelconque de V. Il est facile de voir que cette expression est indépendante du choix de la base orthonormée, et donc $\mathrm{Tr}(A|_V)$ est bien définie.

Lemme 1.

Pour tout $1 \leq k \leq n$, on a :

$$\lambda_1(A) + \ldots + \lambda_k(A) = \sup_{\substack{V \subset \mathbb{R}^n \\ \dim(V) = k}} \mathrm{Tr}(A|_V)$$

Preuve du lemme 1.

Soient $e_1, \ldots, e_n$ une base orthogonale formée par les vecteurs propres associés à $\lambda_1(A), \ldots, \lambda_n(A)$ respectivement (en appliquant le théorème spectral). On a :

$$\lambda_1(A) + \ldots + \lambda_k(A) = \mathrm{Tr}(A|_{\mathrm{vect}(e_1, \ldots, e_k)})$$

et

$$\lambda_1(A) + \ldots + \lambda_k(A) \leq \sup_{\substack{V \subset \mathbb{R}^n \\ \dim(V) = k}} \mathrm{Tr}(A|_V).$$

Il reste à montrer que $\lambda_1(A) + \ldots + \lambda_k(A) \geq \sup_{\substack{V \subset \mathbb{R}^n \\ \dim(V)=k}} \mathrm{Tr}(A|_V)$.

Montrons par récurrence sur $n \in \mathbb{N}^*$ que :

$$(\mathcal{P}_n) : \forall A \in S_n(\mathbb{R}), \forall k \in \{1, \ldots, n\}, \lambda_1(A) + \ldots + \lambda_k(A) \geq \sup_{\substack{V \subset \mathbb{R}^n \\ \dim(V)=k}} \mathrm{Tr}(A|_V).$$

C'est trivial pour $n = 1$. Supposons que $\mathcal{P}_n$ soit vraie et montrons $\mathcal{P}_{n+1}$.

Soit $A \in S_{n+1}(\mathbb{R})$ et $k \in \{1, \ldots, n+1\}$. Notons $(e_1, \ldots, e_{n+1})$ une base orthonormale formée par les vecteurs propres de A, associée aux valeurs propres $\lambda_1(A), \ldots, \lambda_{n+1}(A)$ respectivement.

Si $k = 1$, on a pour tous $\beta_1, \ldots, \beta_{n+1}$ non tous nuls, et pour $v = \frac{1}{\sqrt{\beta_1^2 + \ldots + \beta_{n+1}^2}} \sum_{k=1}^{n+1} \beta_k e_k$, on a :

$$\mathrm{Tr}(A|_{\mathrm{vect}(v)}) = v^T A v = \frac{1}{\beta_1^2 + \ldots + \beta_{n+1}^2} \sum_{k=1}^{n+1} \beta_k^2 \lambda_k(A)$$

et

$$\mathrm{Tr}(A|_{\mathrm{vect}(v)}) \leq \frac{1}{\beta_1^2 + \ldots + \beta_{n+1}^2} \sum_{k=1}^{n+1} \beta_k^2 \lambda_1(A) = \lambda_1(A).$$

Donc,

$$\lambda_1(A) \geq \sup_{\substack{V \subset \mathbb{R}^{n+1} \\ \dim(V) = 1}} \mathrm{Tr}(A|_V).$$

Si $k > 1$, soit V un sous-espace vectoriel de $\mathbb{R}^{n+1}$ de dimension k. Alors V contient un sous-espace V' de dimension $k-1$ inclus dans $\mathrm{vect}(e_2, \ldots, e_{n+1})$. En appliquant l'hypothèse de récurrence à la restriction de A à $\mathrm{vect}(e_2, \ldots, e_{n+1})$, qui a pour valeurs propres $\lambda_2(A), \ldots, \lambda_{n+1}(A)$, on obtient :

$$\lambda_2(A) + \ldots + \lambda_k(A) \geq \mathrm{Tr}(A|_{V'}).$$

D'autre part, si v est un vecteur unitaire dans le complément orthogonal de V' dans V, on voit à partir du cas $k = 1$ que :

$$\lambda_1(A) \geq v^T A v.$$

Par suite, on a :

$$\lambda_1(A) + \ldots + \lambda_k(A) \geq \mathrm{Tr}(A|_V).$$

D'où :

$$\lambda_1(A) + \ldots + \lambda_k(A) \geq \sup_{\substack{V \subset \mathbb{R}^n \\ \dim(V)=k}} \mathrm{Tr}(A|_V).$$

Cela conclut la preuve par récurrence sur $n \in \mathbb{N}^*$.

En appliquant ce lemme à $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)^T$,où 1est à la i-ème position pour tout $i = 1, \ldots, n$, on obtient :

$$\begin{aligned} \lambda_1(A) + \ldots + \lambda_k(A) &= \sup_{\substack{V \subset \mathbb{R}^n \\ \dim(V)=k}} \mathrm{Tr}(A|_V) \\ &\geqslant \mathrm{Tr}(A|_{\{e_i\}_{1 \leqslant i \leqslant n}}) \\ &= \sum_{i=1}^{k} e_i^T A e_i \\ &= a_{1,1} + \cdots + a_{k,k} \end{aligned}$$

D'où le résultat.

✠✠✠✠✠✠✠

Ce problème explore différentes versions du théorème du point fixe pour des applications contractantes et non expansives dans $\mathbb{R}^n$.

Exercice 7.

On considère l'espace vectoriel $\mathbb{R}^n$ équipé de la norme euclidienne $\|.\|$. Une application $A : \mathbb{R}^n \to \mathbb{R}^n$ est dite contractante s'il existe $k < 1$ tel que, pour tous $x, y \in \mathbb{R}^n$, $\|A(x) - A(y)\| \leqslant k\|x - y\|$, et non expansive si $\|A(x) - A(y)\| \leqslant \|x - y\|$ pour tous $x, y \in \mathbb{R}^n$.

1. Montrer qu'une application contractante admet un unique point fixe.

2. Soient $A : \mathbb{R}^n \to \mathbb{R}^n$ une application non expansive et $K \subset \mathbb{R}^n$ un sous-ensemble convexe, fermé et borné tel que $A(K) \subseteq K$. Montrer que A admet un point fixe.

3. Soit $A : \mathbb{R}^n \to \mathbb{R}^n$ une application non expansive. Montrer que pour tout $R > 0$, l'application

$$\tilde{A}(x) = \min(1, R \parallel A(x) \parallel^{-1}) A(x)$$

est non expansive et admet un point fixe.

4. Soit $A : \mathbb{R}^n \to \mathbb{R}^n$ une application non expansive. On suppose que l'ensemble

$S := \{x \in \mathbb{R}^n : \exists \lambda \in [0, 1], x = \lambda A(x)\}$ est borné. Montrer que A admet un point fixe.

Solution. (SABIR Ilyass)

1. Soit $x_0 \in \mathbb{R}^n$ un point arbitraire, et définissons la suite (x_n) par récurrence :

$$x_{n+1} = A(x_n).$$

Montrons que la suite $(x_n)_{n\in\mathbb{N}}$ converge.

On a pour tout $n \geqslant 1$,

$$\begin{aligned} \|x_{n+1} - x_n\| &= \|A(x_n) - A(x_{n-1})\| \\ &\leqslant k\|x_n - x_{n-1}\| \end{aligned}$$

Par récurrence, on obtient pour tout $n \in \mathbb{N}$:

$$\|x_{n+1} - x_n\| \leq k^n \|x_1 - x_0\|$$

Pour tout $p > n$, considérons $\|x_p - x_n\|$:

$$\begin{aligned}\|x_p - x_n\| &\leqslant \sum_{i=n}^{p-1} \|x_{i+1} - x_i\| \\ &\leqslant \|x_1 - x_0\| \sum_{i=n}^{p-1} k^i \\ &= \|x_1 - x_0\| \frac{k^n - k^p}{1-k} \\ &\leqslant \frac{k^n}{1-k} \|x_1 - x_0\|\end{aligned}$$

Comme $k \in [0,1[$, $k^n \underset{n\to\infty}{\to} 0$. Donc, la suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy. Puisque $\mathbb{R}^n$ est complet, la suite $(x_n)_{n\in\mathbb{N}}$ converge vers un point $x^* \in \mathbb{R}^n$.

Par continuité de A (car elle est lipschitzienne), on a :

$$x^* = \lim_{n\to\infty} x_n = \lim_{n\to\infty} A(x_{n-1}) = A\left(\lim_{n\to\infty} x_{n-1}\right) = A(x^*).$$

Donc, x^* est un point fixe de A.

Unicité du point fixe :

Supposons qu'il existe un autre point fixe y^* tel que $A(y^*) = y^*$. Alors :

$$\|x^* - y^*\| = \|A(x^*) - A(y^*)\| \leq k\|x^* - y^*\|.$$

Ainsi,

$$(1-k)\|x^* - y^*\| \leq 0.$$

Comme $k < 1$, on a $\|x^* - y^*\| = 0$, donc $x^* = y^*$.

En conclusion, l'application A admet un unique point fixe dans $\mathbb{R}^n$.

2. Soient $A : \mathbb{R}^n \to \mathbb{R}^n$ une application non expansive et $K \subset \mathbb{R}^n$ un sous-ensemble convexe, fermé et borné tel que $A(K) \subset K$. Montrer que A admet un point fixe.

Comme K est un sous-ensemble fermé et borné de $\mathbb{R}^n$. Il est donc compact d'après le théorème de Heine-Borel.

Or, A est une application non expansive, c'est-à-dire que pour tous $x, y \in \mathbb{R}^n$, on a :

$$\|A(x) - A(y)\| \leq \|x - y\|.$$

Cela implique que A est lipschitzienne. Par conséquent, A est continue sur $\mathbb{R}^n$, et en particulier sur K.

Le théorème du point fixe de Brouwer (voir le lemme 1) affirme que toute application continue d'un compact convexe non vide de $\mathbb{R}^n$ dans lui-même possède au moins un point fixe.

Comme K est compact, convexe et non vide (puisque tout compact dans $\mathbb{R}^n$ est non vide), et que $A(K) \subset K$, on peut appliquer le théorème de Brouwer à l'application A restreinte à K.

Lemme 1. (Théorème du point fixe de Brouwer)

Soit $K \subset \mathbb{R}^n$ un compact convexe non vide. Toute application continue $f : K \to K$ admet au moins un point fixe.

Preuve du lemme 1.

Supposons par l'absurde que f n'a pas de point fixe sur K. Alors, pour tout $x \in K$, $f(x) \neq x$.

Définissons l'application $g : K \to \partial K$ (où ∂K désigne le bord de K) par :

$$g(x) = x + \lambda(x)[f(x) - x],$$

où $\lambda(x) > 0$ est choisi de sorte que $g(x) \in \partial K$.

Puisque K est convexe, le segment $[x, f(x)]$ est contenu dans K. Comme $f(x) \neq x$, le vecteur $f(x) - x$ est non nul. En prolongeant ce segment au-delà de $f(x)$, nous sortons de K car K est compact. Donc, il existe un scalaire $\lambda(x) > 0$ tel que $g(x) = x + \lambda(x)[f(x) - x]$ appartient à ∂K.

L'application g est continue car elle composée de fonctions continues. Elle envoie K dans ∂K.

Il est connu qu'il n'existe pas de rétraction continue d'un compact convexe K de $\mathbb{R}^n$ sur son bord ∂K (c'est une propriété topologique des espaces contractiles). En effet, cela violerait les propriétés homologiques ou homotopiques de K.

Donc, l'application f admet au moins un point fixe dans K.

3. Soit $R > 0$, montrons que

$$\tilde{A}(x) = \min\left(1, \frac{R}{\|A(x)\|}\right) A(x)$$

est non expansive

Soient $x, y \in \mathbb{R}^n$,

Cas 1 : Si $\|A(x)\| < R$ et $\|A(y)\| < R$, on a alors

$$\begin{aligned}\|\tilde{A}(x) - \tilde{A}(y)\| &= \|A(x) - A(y)\| \\ &= \|x - y\|\end{aligned}$$

Cas 2 : Si $\|A(x)\| \geq R$ et $\|A(y)\| \geq R$, on a alors

$$\begin{aligned}\frac{1}{R^2}\|\tilde{A}(x) - \tilde{A}(y)\|^2 &= \|\frac{1}{\|A(x)\|}A(x) - \frac{1}{\|A(y)\|}A(y)\|^2 \\ &= 2 - \frac{2}{\|A(x)\|\|A(y)\|}\langle A(x), A(y)\rangle\end{aligned}$$

Pour conclure, il suffit de montrer que :

$$2 - \frac{2}{\|A(x)\|\|A(y)\|}\langle A(x), A(y)\rangle \leqslant \frac{1}{R^2}\|A(x) - A(y)\|^2 \quad (1)$$

En posant $\alpha = \|A(x)\| \geq R$, $\beta = \|A(y)\| \geq R$ et $\cos(\theta) = \frac{\langle A(x), A(y)\rangle}{\|A(x)\|\|A(y)\|}$, pour montrer (1), cela revient à montrer que

$$\frac{\alpha^2}{R^2} + \frac{\beta^2}{R^2} + 2\cos(\theta)\left(1 - \frac{\alpha\beta}{R^2}\right) \geqslant 2$$

Puisque $1 - \frac{\alpha\beta}{R^2} < 0$, il suffit de montrer que

$$\frac{\alpha^2}{R^2} + \frac{\beta^2}{R^2} - 2\left(1 - \frac{\alpha\beta}{R^2}\right) \geqslant 2$$

Ce qui est équivalent à $(\alpha + \beta)^2 \geqslant 4R^2$ et ceci est vrai car $\alpha, \beta \geqslant R$.

Cas 3 : Si $\|A(x)\| \geq R$ et $\|A(y)\| < R$ (respectivement si $\|A(x)\| < R$ et $\|A(y)\| \geqslant R$), par symétrie, on peut supposer sans perte de généralité que $\|A(x)\| \geq R$ et $\|A(y)\| < R$, on a alors

$$\begin{aligned}\|\tilde{A}(x) - \tilde{A}(y)\|^2 &= \|\frac{R}{\|A(x)\|}A(x) - A(y)\|^2 \\ &= R^2 + \|A(y)\|^2 - 2\frac{R}{\|A(x)\|}\langle A(x), A(y)\rangle\end{aligned}$$

En posant $\alpha = \|A(x)\| \geq R$, $\beta = \|A(y)\| < R$ et $\cos(\theta) = \frac{\langle A(x), A(y)\rangle}{\|A(x)\|\|A(y)\|}$, pour montrer que

$$R^2 + \|A(y)\|^2 - 2\frac{R}{\|A(x)\|}\langle A(x), A(y)\rangle \leqslant \|A(x) - A(y)\|^2$$

Il suffit de montrer que

$$R^2 + 2\beta(\alpha - R)\cos(\theta) \leqslant \alpha^2$$

Puisque $\alpha - R > 0$ et $\beta < R$, il suffit de montrer que

$$R^2 + 2R(\alpha - R) \leqslant \alpha^2$$

Cette inégalité est équivalente à $(\alpha - R)^2 \geqslant 0$.

D'où pour tout $x, y \in \mathbb{R}^n$, on a

$$\|\tilde{A}(x) - \tilde{A}(y)\| \leqslant \|x - y\|$$

Ainsi $\tilde{A}$ est non expansive.

L'application $\tilde{A}$ est continue (car combinaison de fonctions continues) et à valeurs dans la boule fermée $B(0, R)$ de $\mathbb{R}^n$, c'est-à-dire $\|\tilde{A}(x)\| \leq R$ pour tout $x \in \mathbb{R}^n$.

Or, $B(0, R)$est sous-ensemble de $\mathbb{R}^n$ convexe, fermé et borné, donc d'après la question précédente, $\tilde{A}$ admet un point fixe.

4. Pour chaque $\lambda \in [0, 1[$, définissons l'application $T_\lambda : \mathbb{R}^n \to \mathbb{R}^n$ par :

$$T_\lambda(x) = \lambda A(x).$$

Pour tout $x, y \in \mathbb{R}^n$,

$$\begin{aligned} \|T_\lambda(x) - T_\lambda(y)\| &= \|\lambda A(x) - \lambda A(y)\| \\ &= \lambda \|A(x) - A(y)\| \\ &\leq \lambda \|x - y\|. \end{aligned}$$

Puisque $\lambda \in [0, 1[$, alors T_λ est une application contractante avec une constante de contraction $\lambda < 1$.

Ainsi, d'après la question 1, T_λ admet un unique point fixe x_λ tel que

$$x_\lambda = T_\lambda(x_\lambda) = \lambda A(x_\lambda)$$

Ainsi, pout tout $\lambda \in [0, 1[$, il existe $x_\lambda \in \mathbb{R}^n$ tel que $x_\lambda = \lambda A(x_\lambda)$.

En particulier, pour tout $n \in \mathbb{N}^*$, il existe $x_n \in \mathbb{R}^n$, tel que $x_n = \left(1 - \frac{1}{n}\right) A(x_n)$.

Puisque pour tout $n \in \mathbb{N}$, $x_n \in S$ et que S est borné, alors $(x_n)_{n\in\mathbb{N}}$ est bornée,

D'après le théorème de Bolzano-Weierstrass, la suite bornée (x_n) possède une sous-suite convergente $(x_{\varphi(n)})_{n\in\mathbb{N}}$. Notons x sa limite. (où $\varphi : \mathbb{N} \to \mathbb{N}$ strictement croissante).

Ainsi, pour tout $n \in \mathbb{N}$

$$x_{\varphi(n)} = \left(1 - \frac{1}{\varphi(n)}\right) A(x_{\varphi(n)})$$

Puisque A est non expensive, elle est lipschitizienne, en particulier elle esr continue sur $\mathbb{R}^n$. Par passage à la limite $n \to +\infty$, on trouve

$$x = A(x)$$

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice d'analyse complexe et de combinatoire demande aux candidats d'étudier le développement en série entière d'une fraction rationnelle particulière. Il teste leur capacité à manipuler des séries formelles et à extraire des informations sur les coefficients de ces séries.

Exercice 8.

Soient $p, q \geq 2$ des entiers premiers entre eux. Calculer le développement en série entière $\sum_{k=0}^{\infty} c_k z^k$ de la fraction rationnelle

$$\frac{1 - z^{pq}}{(1 - z^p)(1 - z^q)}$$

en $z = 0$. Déterminer le plus grand entier k tel que $c_k = 0$.

Solution. (SABIR Ilyass)

On a, pour tout $|z| < 1$, puisque p et q sont premiers entre eux, p et q jouent un rôle symétrique, et donc sans perte de généralité, on peut supposer

que q est impair. On a alors

$$\begin{aligned}
\frac{1-z^{pq}}{(1-z^p)(1-z^q)} &= \frac{(1-z^p)\sum_{k=0}^{q-1} z^{kp}}{(1-z^p)(1-z^q)} \\
&= \frac{1}{1-z^q}\sum_{k=0}^{q-1} z^{kp} \\
&= \left(\sum_{k=0}^{q-1} z^{kp}\right)\left(\sum_{n=0}^{+\infty} z^{qn}\right) \\
&= \left(\sum_{k=0}^{+\infty} \mathbf{1}_{[0,q[}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{k}{p}\right) z^k\right)\left(\sum_{n=0}^{+\infty} \mathbf{1}_{\mathbb{N}}\left(\frac{k}{q}\right) z^n\right) \\
&= \sum_{n=0}^{+\infty}\left(\sum_{k=0}^{n} \mathbf{1}_{[0,q[}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{n-k}{q}\right)\right) z^n
\end{aligned}$$

Posons,

$$c_n = \sum_{k=0}^{n} \mathbf{1}_{[0,q[}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{n-k}{q}\right)$$

On a pour tout $n \in \mathbb{N}$, $c_n = 0$ si, et seulement si, pour tout $k \in [\![0, n]\!]$, on a

$$\mathbf{1}_{[0,q[}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{n-k}{q}\right) = 0$$

Ainsi, pour un $n \in \mathbb{N}$, $c_n \neq 0$ si et seulement s'il existe $k \in [\![0, n]\!]$ tel que

$$\mathbf{1}_{[0,q[}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{k}{p}\right)\mathbf{1}_{\mathbb{N}}\left(\frac{n-k}{q}\right) = 1$$

Ce qui est équivalent à l'existence de $s, t \in \mathbb{N}$ tels que

$$k \leqslant pq, k = ps \text{ and } n = k + tq$$

Donc,

$$k = ps + tq \text{ and } k \leqslant \min(pq, n)$$

En vertu des deux lemmes suivants, un tel $k$existe si et seulement si $n > pq - p - q$.

Ainsi, le plus grand entier n tel que $c_n = 0$ est $n = pq - p - q$.

Lemme 1. (Chicken McNugget Theorem)

Soient a et b deux entiers positifs premiers entre eux. Alors le plus grand entier qui ne peut pas s'exprimer comme une combinaison linéaire non négative de a et b (c'est-à-dire de la forme $ma + nb$ avec $m, n \in \mathbb{N}$) est :

$$N = ab - a - b.$$

Preuve du Lemme 1.

Puisque a et b sont premiers entre eux, il existe des entiers relatifs u et v tels que :

$$au + bv = 1.$$

Ceci est une conséquence de l'identité de Bézout.

Considérons les résidus modulo b des multiples de a. Puisque $\text{pgcd}(a, b) = 1$, les multiples de a mod b parcourent tous les résidus de 0 à $b - 1$.

Pour chaque entier r tel que $0 \leq r \leq b - 1$, il existe un entier k tel que :

$$ka \equiv r \bmod b.$$

Pour tout entier $n \geq N + 1 = ab - a - b + 1$, on peut écrire :

$$n = ak + b\left(\frac{n - ak}{b}\right).$$

Puisque $n - ak \equiv 0 \bmod b$, le second terme est un entier. Il nous suffit de montrer que le coefficient du second terme est non négatif.

Comme $n \geq ab - a - b + 1$, on a :

$$n \geq ab - a - b + 1.$$

En choisissant judicieusement k pour chaque n, on peut assurer que les coefficients sont non négatifs.

Lemme 2 :

L'entier $N = pq - p - q$ ne peut pas être exprimé comme une combinaison linéaire non négative de p et q.

Preuve du Lemme 2 :

Supposons par l'absurde que N puisse être exprimé comme une combinaison linéaire non négative de p et q :

$$N = ap + bq, \quad \text{avec} \quad a, b \in \mathbb{N}.$$

Alors :

$$ap + bq = pq - p - q.$$

Réarrangeons l'équation :

$$ap + p + bq + q = pq.$$

Ce qui donne :

$$p(a+1)+q(b+1)=pq.$$

Comme p et q sont premiers entre eux, p ne divise pas q et vice versa. Ainsi, pour que la somme $p(a+1)+q(b+1)$ soit égale à pq, il faut que $a+1$ soit multiple de q et $b+1$ soit multiple de p. Donc, il existe des entiers $m,n\in\mathbb{N}$ tels que :

$$a+1=qn,\quad b+1=pm.$$

Substituons dans l'équation :

$$p(qn)+q(pm)=pq.$$

Ce qui simplifie à :

$$pq(n+m)=pq.$$

Donc :

$$n+m=1.$$

Cela implique que soit $n=1$ et $m=0$, soit $n=0$ et $m=1$.

- Si $n=1$ et $m=0$, alors $a+1=q$ donc $a=q-1$, et $b+1=0$ donc $b=-1$, ce qui est impossible puisque $b\in\mathbb{N}$.

- Si $n=0$ et $m=1$, alors $a+1=0$ donc $a=-1$, impossible car $a\in\mathbb{N}$.

Dans les deux cas, nous obtenons une contradiction. Par conséquent, N ne peut pas être exprimé comme une combinaison linéaire non négative de p et q.

✠✠✠✠✠✠✠

Ce problème de probabilités porte sur l'étude d'un processus aléatoire générant un sous-ensemble de $[\![1,N]\!]$. Il évalue la compréhension des candidats sur les concepts de probabilité conditionnelle et leur aptitude à calculer des espérances et des variances pour des variables aléatoires discrètes.

Exercice 9.

Soit un entier $N \geqslant 1$. On considère la suite aléatoire suivante : on choisit u_1 uniformément dans $[\![1, N]\!]$; puis à chaque étape, on choisit u_{n+1} uniformément dans $[\![1, u_n]\!]$. On considère ensuite l'ensemble aléatoire $E_N := \{u_i\}_{i\geqslant 1} \subset [\![1, N]\!]$.

1. Pour tout $k \in [\![1, N]\!]$, déterminer la probabilité que $k \in E_N$. 2. Quelle est la probabilité que $2 \in E_N$ sachant que $3 \notin E_N$?

3. Calculer l'espérance de $|E_N|$ et en donner un équivalent lorsque $N \to \infty$.

4. Calculer la variance de $|E_N|$ et en donner un équivalent lorsque $N \to \infty$.

Solution. (SABIR Ilyass)

1. Soit $N \geqslant 1$, et $k \in [\![1, N]\!]$, calculons la probabilité que $k \in E_N$.

Pour tout $n \geqslant 1$, notons $\mathbb{P}(k \in E_n)$ la probabilité que $k \in E_n$.

On a pour tout $n \geqslant 2$, si $n < k$: $\mathbb{P}(k \in E_n) = 0$, sinon

$$\begin{aligned}
\mathbb{P}(k \in E_n) &= \sum_{j=1}^{n} \mathbb{P}(k \in E_n, u_1 = j) \\
&= \sum_{j=k}^{n} \mathbb{P}(k \in E_n, u_1 = j) \\
&= \frac{1}{n} + \sum_{j=k+1}^{n} \mathbb{P}(u_1 = j)\mathbb{P}(k \in E_j) \\
&= \frac{1}{n} + \frac{1}{n} \sum_{j=k+1}^{n} \mathbb{P}(k \in E_j)
\end{aligned}$$

Par suite,

$$\mathbb{P}(k \in E_n) = \frac{1}{n-1} + \frac{1}{n-1} \sum_{j=k+1}^{n-1} \mathbb{P}(k \in E_j)$$

Ainsi,

$$\frac{1}{n} \sum_{j=k+1}^{n} \mathbb{P}(k \in E_j) = \frac{1}{n(n-1)} + \frac{1}{n-1} \sum_{j=k+1}^{n-1} \mathbb{P}(k \in E_j)$$

Par suite,

$$\sum_{n=k+1}^{N}\left(\frac{1}{n}\sum_{j=k+1}^{n}\mathbb{P}(k\in E_j)-\frac{1}{n-1}\sum_{j=k+1}^{n-1}\mathbb{P}(k\in E_j)\right)=\sum_{n=k+1}^{N}\frac{1}{n(n-1)}$$

Par téléscopage, on a

$$\sum_{j=k+1}^{N}\mathbb{P}(k\in E_j)=\frac{N}{k}-1$$

Par suite

$$\begin{aligned}\mathbb{P}(k\in E_N) &= 1+\frac{1}{N}\sum_{j=k+1}^{N}\mathbb{P}(k\in E_j)\\ &= \frac{1}{N}+\frac{1}{N}\left(\frac{N}{k}-1\right)\\ &= \frac{1}{k}\end{aligned}$$

2. Il est clair que pour tous $i<j\in[\![1,n]\!]$, on a $\mathbb{P}(i\in E_N|j\in E_N)=\mathbb{P}(i\in E_j)$

$$\begin{aligned}\mathbb{P}\left(2\in E_N|3\not\in E_N\right) &= \frac{\mathbb{P}\left(3\not\in E_N|2\in E_N\right)\mathbb{P}(2\in E_N)}{\mathbb{P}\left(3\not\in E_N\right)}\\ &= \frac{(1-\mathbb{P}(3\in E_N|2\in E_N))}{1-\mathbb{P}(3\in E_N)}\mathbb{P}(2\in E_N)\\ &= \frac{\mathbb{P}(2\in E_N)}{1-\mathbb{P}(3\in E_N)}\left(1-\frac{\mathbb{P}(3\in E_N)}{\mathbb{P}(2\in E_N)}\mathbb{P}(2\in E_N|3\in E_N)\right)\\ &= \frac{\mathbb{P}(2\in E_N)}{1-\mathbb{P}(3\in E_N)}\left(1-\frac{\mathbb{P}(3\in E_N)}{\mathbb{P}(2\in E_N)}\mathbb{P}(2\in E_3)\right)\\ &= \frac{\frac{1}{2}}{1-\frac{1}{3}}\left(1-\frac{\frac{1}{3}}{\frac{1}{2}}\times\frac{1}{2}\right)\\ &= \frac{1}{2}\end{aligned}$$

3. Pour tout $N\geqslant 1$, notons $E_N=\{u_1,\dots,u_l\}$ avec $l\leqslant N$ et $u_1<\dots<u_l$.

On a pour tout $k \in [\![1, n]\!]$

$$\begin{aligned}\mathbb{E}[|E_N|] &= \mathbb{E}\left(\sum_{k=1}^{N} \mathbb{1}_{k\in E_N}\right)\\ &= \sum_{k=1}^{N} \mathbb{P}(k \in E_N)\\ &= \sum_{k=1}^{N} \frac{1}{k}\end{aligned}$$

On a alors :

$$\mathbb{E}[|E_N|] \underset{n\longrightarrow+\infty}{\sim} \ln(N)$$

4. On a

$$\begin{aligned}\mathbb{E}[|E_N|^2] &= \sum_{k=1}^{N}\sum_{j=1}^{N} \mathbb{P}(k \in E_N, j \in E_N)\\ &= \sum_{k=1}^{N} \mathbb{P}(k \in E_N) + 2 \sum_{1\leqslant j<k\leqslant N} \mathbb{P}(k \in E_N, j \in E_N)\\ &= \sum_{k=1}^{N} \frac{1}{k} + 2 \sum_{1\leqslant j<k\leqslant N} \mathbb{P}(k \in E_N, j \in E_k)\\ &= \sum_{k=1}^{N} \frac{1}{k} + 2 \sum_{1\leqslant j<k\leqslant N} \mathbb{P}(k \in E_N)\mathbb{P}(j \in E_k)\\ &= \sum_{k=1}^{N} \frac{1}{k} + 2 \sum_{1\leqslant j<k\leqslant N} \frac{1}{kj}\end{aligned}$$

Par suite,

$$\begin{aligned}\mathrm{Var}(|E_N|) &= \mathbb{E}[|E_N|^2] - \mathbb{E}[|E_N|]^2\\ &= \sum_{k=1}^{N} \frac{1}{k} + 2 \sum_{1\leqslant j<k\leqslant N} \frac{1}{kj} - \left(\sum_{k=1}^{N} \frac{1}{k}\right)^2\\ &= \sum_{k=1}^{N} \frac{1}{k} - \sum_{k=1}^{N} \frac{1}{k^2}\end{aligned}$$

D'où

$$\mathrm{Var}(|E_N|) \underset{n\longrightarrow+\infty}{\sim} \ln(N)$$

✠✠✠✠✠✠✠

Cet exercice traite de la construction et de l'analyse d'un arbre aléatoire croissant. Il teste la capacité des candidats à modéliser un processus stochastique, à calculer des probabilités conditionnelles et à déterminer les caractéristiques statistiques (espérance, variance) de certaines propriétés de l'arbre.

Exercice 10.

On construit un arbre aléatoire de la manière suivante : on commence par une racine S_1 ; on lui ajoute un premier descendant direct S_2. Puis, à l'étape $N+1$, on choisit un sommet S_i uniformément (avec $i \in [\![1, N]\!]$) et on lui ajoute un descendant direct S_{N+1}.

1. Calculer l'espérance et la variance du nombre de descendants directs de S_1 à l'étape N.

2. Calculer la probabilité que S_2 ait k descendants (directs ou non) à l'issue de l'étape N.

3. Calculer l'epsérance et la variance du nombre de feuilles (sommets sans descendants) de l'arbre à l'étape N.

Solution. (SABIR Ilyass, ZINE Akram)

1. À chaque étape k (de 2 à N), le sommet S_1 a une probabilité de $\frac{1}{k-1}$ d'être choisi pour recevoir un nouveau descendant direct. On définit pour tout $k = 2, \ldots, N$, la variable aléatoire X_k par :

$$X_k = \begin{cases} 1 \text{ si } S_1 \text{ est choisi à} l'\text{étape } k \\ 0 \text{ sinon} \end{cases}$$

L'espérance du nombre de descendants directs de S_1 à l'étape N :

$$\begin{aligned} \mathbb{E}\left[\sum_{k=2}^{N} X_k\right] &= \sum_{k=2}^{N} \mathbb{E}[X_k] \\ &= \sum_{k=2}^{N} \frac{1}{k-1} \\ &= H_{N-1} \end{aligned}$$

où H_{N-1} est le $(N-1)$-ième nombre harmonique.

La variance du nombre de descendants directs de S_1 à l'étape N :

On a par indépendance entre $X_2, X_3, \ldots, X_N$

$$\begin{aligned}\operatorname{Var}\left[\sum_{k=2}^{N} X_k\right] &= \sum_{k=2}^{N} \operatorname{Var}[X_k] \\ &= \sum_{k=2}^{N} \left(\frac{1}{k-1}\left(1-\frac{1}{k-1}\right)\right) \\ &= H_{N-1} - \sum_{k=2}^{N} \frac{1}{(k-1)^2}\end{aligned}$$

2. Le nombre total de sommets est N. On a la racine S_1, qui n'est pas un descendant de S_2. S_2 lui-même ne doit pas être compté comme son propre descendant.

Les sommets $S_3, S_4, \ldots, S_N$ sont les $N-2$ sommets restants qui peuvent potentiellement être des descendants de S_2.

Le nombre total d'arbres que l'on peut construire est : $(N-1)!$

Le nombre de façons de choisir les k descendants de S_2 parmi les $N-2$ sommets est : $\binom{N-2}{k}$

Le nombre de façons de construire un arbre récursif avec $k+1$ sommets (incluant S_2) est :

$$T_{\text{sous-arbre}} = k!$$

puisque S_2 est la racine fixe du sous-arbre.

Les $N-k-2$ sommets restants (qui ne sont pas descendants de S_2) forment un autre arbre récursif enraciné en S_1. Le nombre de façons de construire cet arbre est :

$$T_{\text{complément}} = (N-k-2)!$$

Le nombre total d'arbres favorables est :

$$\text{Nombre d'arbres favorables} = \binom{N-2}{k} \times T_{\text{sous-arbre}} \times T_{\text{complément}}$$

D'où, la probabilité que S_2 ait exactement k descendants (directs ou

indirects), est :

$$\begin{aligned} P &:= \frac{\binom{N-2}{k} \times k! \times (N-k-2)!}{(N-1)!} \\ &= \frac{(N-2)!}{(N-1)!} \\ &= \frac{1}{N-1} \end{aligned}$$

3. Notons L_N le nombre de feuilles dans un arbre aléatoire de N sommets.

Soit $\sigma = (\sigma_1, \ldots, \sigma_{N-1})$ une permutation sur $\{2, \ldots, N\}$. On peut construire un arbre récursif avec les nœuds $1, 2, \ldots, N$ en prenant 1 comme racine, et en attachant le nœud $i \geq 2$ au nœud le plus à droite j de σ qui précède i et qui est inférieur à i. S'il n'existe pas un tel élément j, alors on définit la racine 1 comme le parent de i.

De la construction de l'arbre ci-dessus, L_N peut être défini par :

$$L_N = \sum_{i=1}^{N-2} I\{\sigma_i > \sigma_{i+1}\} + 1. \tag{4}$$

Ceci est obtenu en observant que chaque apparition de descentes dans σ signifie qu'une feuille sera ajoutée à l'arbre T_n. De plus, le dernier élément σ_{n-1} de σ est toujours une feuille.

$\mathbb{E}[L_N] = N/2$ découle du fait que $\mathbb{P}(I\{\sigma_i > \sigma_{i+1}\} = 1) = 1/2$.

De plus,

$$\begin{aligned} \mathbb{E}[L_N^2] &= \mathbb{E}\left[\left(\sum_{i=1}^{N-2} I\{\sigma_i > \sigma_{i+1}\} + 1\right)^2\right] \\ &= \mathbb{E}\left[3\sum_{i=1}^{N-2} I\{\sigma_i > \sigma_{i+1}\} + \sum_{1 \leqslant i \neq j \leqslant N-2} I\{\sigma_i > \sigma_{i+1}\} I\{\sigma_j > \sigma_{j+1}\} + 1\right] \end{aligned}$$

Or, pour tout $i, j \in [\![1, N-2]\!]$, on a :

$$\mathbb{P}(I\{\sigma_i > \sigma_{i+1}\} | I\{\sigma_j > \sigma_{j+1}\} = 1) = \begin{cases} 1/6 & \text{si } |i-j| = 1, \\ 1/4 & \text{si } |i-j| > 1 \end{cases}$$

Ainsi, on obtient :

$$\begin{aligned}\mathbb{E}[L_N^2] &= \frac{3(N-2)}{2} + \frac{(N-3)(N-4)}{4} + \frac{2(N-3)}{6} + 1 \\ &= \frac{N^2}{4} + \frac{N}{12}\end{aligned}$$

Par conséquent,

$$\mathrm{Var}[L_N^2] = \frac{N}{12}$$

✠✠✠✠✠✠✠

Troisième partie

Exercices additionnels

Dans les pages qui suivent, nous plongerons au cœur des défis mathématiques les plus stimulants. Nous explorerons une sélection soigneusement choisie d'exercices issus des oraux de l'École Polytechnique et de l'École Normale Supérieure. Notre parcours s'enrichira également de problèmes fascinants tirés des Olympiades de mathématiques, ainsi que d'autres sujets d'étude captivants. Cette section vise à aiguiser votre esprit analytique, à développer votre créativité mathématique et à vous préparer aux plus hauts niveaux de réflexion scientifique.

✠✠✠✠✠✠✠

L'exercice suivant s'intéresse aux polynômes et au comportement de leurs racines réelles. Il s'agit de déterminer s'il est possible de construire une suite particulière de coefficients permettant d'obtenir un nombre précis de racines réelles distinctes pour chaque polynôme considéré.

Exercice 1. (Oral ULM)

Existe-il une suite $(a_n)_{n\in\mathbb{N}}$ de réels telle que pour tout entier $n \in \mathbb{N}$, le polynôme $\sum_{k=0}^{n} a_k X^k$ ait exactement n racines réelles distinctes ?

Solution. (SABIR Ilyass)

Commençons par construire une suite de polynômes $\left(P_n := \sum_{k=0}^{n} a_k X^k\right)_{n\in\mathbb{N}}$ scindés sur $\mathbb{R}$à racines simples.

Initialisons la suite par $P_0 = 1$, $P_1 = X + 1$, puis l'idée est de supposer pour un $n \in \mathbb{N}$ donné, qu'il existe $a_0, \ldots, a_n$ tels que $P_n := \sum_{k=0}^{n} a_k X^k$ soit scindé sur $\mathbb{R}$ à racines simples. Nous allons chercher un $a_{n+1} \in \mathbb{R}$ tel que $P_{n+1} = \sum_{k=0}^{n+1} a_k X^k$ soit également scindé sur $\mathbb{R}$à racines simples.

Puisque P_n est scindé à racines simples, alors il existe $\lambda_1 < \ldots < \lambda_n \in \mathbb{R}$ tels que $P_n = \prod_{k=1}^{n} (X - \lambda_k)$

Soient $\beta_0, \ldots, \beta_n \in \mathbb{R}$ vérifiant $\beta_{k-1} < \lambda_k < \beta_k$ pour tout$k = 1, \ldots, n$.

Par ailleurs, pour tout $k \in [\![0, n-1]\!]$ P_n change de signe sur les intervalles $]\lambda_k, \lambda_{k+1}[$ et $]\lambda_{k+1}, \lambda_{k+2}[$ avec $\lambda_0 = -\infty$ et $\lambda_{n+1} = +\infty$. En particulier, pour tout $k \in [\![0, n-1]\!]$ $P_n(\beta_k)P_n(\beta_{k+1}) < 0$ et $P_n(\beta_n) > 0$.

Soit φ la fonction définie sur $\mathbb{R}^2$ par $\varphi(x, y) = P_n(x) + yx^{n+1}$ pour tout $(x, y) \in \mathbb{R}^2$.

On a $\varphi(\beta_k, 0)\varphi(\beta_{k+1}, 0) = P_n(\beta_k)P_n(\beta_{k+1}) < 0$ et $\varphi(\beta_n, 0)$=$P_n(\beta_n) > 0$.

Donc par continuité de $(x, y, z) \longmapsto \varphi(x, z)\varphi(y, z)$ sur $\mathbb{R}^2$, pour tout $k \in [\![0, n-1]\!]$ il existe $\varepsilon_k > 0$ tel que pour tout $t \in \mathbb{R}$ tel que $|t| < \varepsilon_k$ on a $\varphi(\beta_k, t)\varphi(\beta_{k+1}, t) < 0$ pour tout $k = 1, \ldots, n$.

Par continuité de φ, il existe $\varepsilon_n > 0$ tel que pour tout $t \in \mathbb{R}$ vérifiant $|t| < \varepsilon_n$, on a $\varphi(\beta_n, t) > 0$.

En particulier pour $a_{n+1} := -\frac{1}{2}\min_{k=0}^{n}(\varepsilon_k)$, on obtient pour tout $k \in [\![0, n-1]\!]$ $\varphi(\beta_k, a_{n+1})\varphi(\beta_{k+1}, a_{n+1}) < 0$ et $\varphi(\beta_n, a_{n+1}) > 0$.

Via le théorème des valeurs intermédiaires, pour tout $k \in [\![0, n-1]\!]$, il existe $\gamma_k \in]\beta_k, \beta_{k+1}[$ tel que $\varphi(\gamma_k, a_{n+1}) = 0$.

D'autre part, $\lim\limits_{x \to +\infty} \varphi(x, a_{n+1}) = -\infty$ et $\varphi(\beta_n, a_{n+1}) > 0$, d'après le même théorème il existe $\gamma_n \in]\beta_n, +\infty[$ tel que $\varphi(\gamma_n, a_{n+1}) = 0$.

En conclusion, $x \longmapsto \varphi(x, a_{n+1}) = \sum\limits_{k=0}^{n+1} a_k X^k$ admet exactement $n+1$ racines simples $\gamma_0 < \cdots < \gamma_n$.

D'où le résultat par récurrence.

✠✠✠✠✠✠✠

Dans cet exercice, nous allons explorer la convergence d'une suite de polynômes vers un polynôme donné, en utilisant les notions de normes dans l'espace des polynômes $\mathbb{R}[X]$. L'objectif est de construire une norme appropriée pour laquelle une suite de polynômes de degré croissant converge vers le polynôme cible. Cette approche permet de mieux comprendre les comportements asymptotiques des polynômes et les propriétés des espaces normés en analyse.

Exercice 2. (Oral ULM)

Soit Q un pôlynome de $\mathbb{R}[X]$, et $(P_n)_{n\in\mathbb{N}}$ une suite de pôlynomes vérifiant, pour tout
$n \in \mathbb{N}, \deg(P_n) = n$.
Construire une norme sur $\mathbb{R}[X]$ telle que le suite $(P_n)_{n\in\mathbb{N}}$ tende vers Qau sens de cette norme.

Solution. (SABIR Ilyass)

Notons $n_0 = \deg(Q)$.

Posons, pour tout $n \in \mathbb{N}$: $R_n = 2^n(P_n - Q)$

Pour tout norme $\|.\|$ de $\mathbb{R}[X]$,et pour tout $n \in \mathbb{N}$ on a : $\|P_n - Q\| = \frac{1}{2^n}\|R_n\|$

Pour avoir la convergence de $(P_n)_{n\in\mathbb{N}}$ vers Q, il suffit de choisir une norme $\|\cdot\|$ telle que :

pour tout $n \in \mathbb{N}$: $\|R_n\| = 1$

une petite modification des premiers termes de R_n ne change pas le rèsultat.

En prenant $R_n = X^n$ pour $n = 1, 2, \ldots, n_0$

Alors pour tout $n \in \mathbb{N}$, on a $\deg(R_n) = n$, donc $(R_n)_{n\in\mathbb{N}}$ forme une base de $\mathbb{R}[X]$.

On définie sur $\mathbb{R}[X]$, la norme $\|.\|$ par : pour tout $P = \sum_{i=0}^{r} a_i R_i \in \mathbb{R}[X]$, on pose :

$$\|P\| = \max_{i=0}^{r} |a_i|$$

$\|.\|$ est clairement une norme sur $\mathbb{R}[X]$,et pour tout $n \in \mathbb{N}$, $\|R_n\| = 1$

Parsuite :

$$\forall n \geq n_0, \quad \|P_n - Q\| = \frac{1}{2^n} \underset{n\to+\infty}{\longrightarrow} 0$$

D'où le résultat.

✠✠✠✠✠✠✠

Dans cet exercice, nous explorons une expression de la somme des puissances d'entiers copremiers avec un nombre donné, en utilisant l'indicatrice d'Euler et des techniques combinatoires.

Exercice 3.

Pour tous $n, r \in \mathbb{N}$ tel que $n \geqslant 2$, on définit :

$$T_{n,r} := \sum_{\substack{1\leqslant i\leqslant n \\ i\wedge n=1}} i^r$$

Montrer que :

$$T_{n,r} = n^r \varphi(n) + \sum_{j=0}^{r-1} \binom{r}{j} \sum_{k=0}^{j} (-1)^{j+k} T_{n,k} - \varphi(n) \sum_{j=0}^{r-1} \binom{r}{j} \sum_{k=0}^{j} (-1)^{j+k} n^k$$

Où φ désigne l'indicatrice d'Euler.

Solution. (SABIR Ilyass)

On définit l'application ψ pour tout $(l,m) \in \mathbb{N}^\star \times \mathbb{N}$ par :

$$\psi(l,m) = \#\{1 \leqslant i \leqslant m | i \wedge l = 1\}$$

On a

$$\begin{aligned} T_{n,r} &= \sum_{i=1}^{n} i^r(\psi(n,i) - \psi(n,i-1)) \\ &= \sum_{i=1}^{n} i^r\psi(n,i) - \sum_{i=1}^{n} i^r\psi(n,i-1) \\ &= n^r\psi(n,n) + \sum_{i=1}^{n-1}(i^r - (i+1)^r)\psi(n,i) \\ &= n^r\varphi(n) - \sum_{i=1}^{n-1}\sum_{j=0}^{r-1}\left(\begin{array}{c} r \\ j \end{array}\right) i^j\psi(n,i) \end{aligned}$$

Donc,

$$n^r\varphi(n) - T_{n,r} = \sum_{j=0}^{r-1}\left(\begin{array}{c} r \\ j \end{array}\right)\left(\sum_{i=1}^{n-1} i^j\psi(n,i)\right)$$

D'après la formule d'inversion de Pascal, on peut écrire pour tout $j \in [\![0, r-1]\!]$:

$$\sum_{i=1}^{n-1} i^j\psi(n,i) = (-1)^j\sum_{k=0}^{j}(-1)^k(n^k\varphi(n) - T_{n,k})$$

Ainsi,

$$\begin{aligned} n^r\varphi(n) - T_{n,r} &= \sum_{j=0}^{r-1}\left(\begin{array}{c} r \\ j \end{array}\right)(-1)^j\sum_{k=0}^{j}(-1)^k(n^k\varphi(n) - T_{n,k}) \\ &= \sum_{j=0}^{r-1}\sum_{k=0}^{j}\left(\begin{array}{c} r \\ j \end{array}\right)(-1)^{j+k}(n^k\varphi(n) - T_{n,k}) \\ &= \sum_{j=0}^{r-1}\sum_{k=0}^{j}\left(\begin{array}{c} r \\ j \end{array}\right)(-1)^{j+k}n^k\varphi(n) - \sum_{j=0}^{r-1}\sum_{k=0}^{j}\left(\begin{array}{c} r \\ j \end{array}\right)(-1)^{j+k}T_{n,k} \end{aligned}$$

D'où

$$T_{n,r} = n^r\varphi(n) + \sum_{j=0}^{r-1}\left(\begin{array}{c} r \\ j \end{array}\right)\sum_{k=0}^{j}(-1)^{j+k}T_{n,k} - \varphi(n)\sum_{j=0}^{r-1}\left(\begin{array}{c} r \\ j \end{array}\right)\sum_{k=0}^{j}(-1)^{j+k}n^k$$

✠✠✠✠✠✠✠

Cet exercice illustre le théorème de Cayley-Hamilton, qui affirme qu'une matrice carrée annule son propre polynôme caractéristique, en exploitant une preuve analytique.

Exercice 4. (Théorème de Cayley-Hamilton)

Soit K un corps commutatif quelconque, et $n \in \mathbb{N}^\star$.
Pour tout matrice $M \in M_n(K)$, notons $\chi_A(X) = \det(X.I_n - A)$ le polynôme caractéristique de M.
On a alors $\chi_M(M) = 0$

Solution. (SABIR Ilyass)

Soit $A \in \mathcal{M}_n(K)$, et soit $\|.\|$ une norme sur $\mathcal{M}_n(K)$.

Notons $\lambda_1, \ldots, \lambda_l$ les racines complexes de $\det(X.I_n - A)$ et $R(A) = \max\limits_{j=1}^{l} |\lambda_j|$.

Pour tout réel $r > R(A)$ et pour tout $t \in \mathbb{R}$, on a $\det(r.e^{\mathrm{i}t} I_n - A) \neq 0$, donc $r.e^{\mathrm{i}t} I_n - A \in \mathrm{GL}_n(K)$.

On écrit alors :

$$r.e^{\mathrm{i}t} I_n - A = r.e^{\mathrm{i}t} \left(I_n - \frac{1}{r} e^{-\mathrm{i}t} A \right)$$

On pose $R = \max(R(A), \|A\|)$. Pour tout $r > R$ et pour tout $t \in \mathbb{R}$, on a :

$$\left\| \frac{1}{r} e^{-\mathrm{i}t} A \right\| = \frac{\|A\|}{r} < 1$$

Ainsi, la série $\sum\limits_{p \geqslant 0} \left(\frac{1}{r} e^{-it} A \right)^p$ converge absolument, donc converge dans $\mathcal{M}_n(K)$.

De plus :

$$\sum_{p=0}^{+\infty} \left(\frac{1}{r} e^{-\mathrm{i}t} A \right)^p = \left(I_n - \frac{1}{r} e^{-it} A \right)^{-1}$$

Ainsi :

$$\begin{aligned}(r.e^{it}I_n - A)^{-1} &= \frac{1}{r}e^{-it}\left(I_n - \frac{1}{r}e^{-it}A\right)^{-1} \\ &= \frac{1}{r}e^{-it}\sum_{p=0}^{+\infty}\left(\frac{1}{r}e^{-it}A\right)^p \\ &= \sum_{p=1}^{+\infty}\left(\frac{1}{r}e^{-it}\right)^p A^{p-1}\end{aligned}$$

Par suite, pour tout $k \in \mathbb{N}^\star$, on a :

$$\int_0^{2\pi}(re^{it})^k(r.e^{it}I_n - A)^{-1}dt = \int_0^{2\pi}\sum_{p=1}^{+\infty}\left(\frac{1}{r}e^{-it}\right)^{p-k}A^{p-1}dt$$

Il est possible d'intervertir l'integrale et la sommation en série, puisque la convergence de la série est normale sur $[0, 2\pi]$, on obtient alors :

$$\begin{aligned}\int_0^{2\pi}(re^{it})^k(r.e^{it}I_n - A)^{-1}dt &= \sum_{p=1}^{+\infty}r^{k-p}\int_0^{2\pi}e^{-i(p-k)t}A^{p-1}dt \\ &= \sum_{p=1}^{+\infty}r^{k-p}(2\pi\delta_{k,p})A^{p-1}\end{aligned}$$

avec $\forall p, k \in \mathbb{N}^\star, \delta_{k,p} = \begin{cases} 0 \text{ si } p \neq k \\ 1 \text{ si } p = k \end{cases}$

D'où

$$\int_0^{2\pi}(re^{it})^k(r.e^{it}I_n - A)^{-1}dt = 2\pi A^{k-1}$$

On en déduit que pour tout $k \in \mathbb{N}^\star$:

$$A^{k-1} = \frac{1}{2\pi}\int_0^{2\pi}(re^{it})^k(re^{it}I_n - A)^{-1}dt$$

Posons $\chi_A(X) = \det(X.I_n - A) = \sum_{k=0}^{n} a_k X^k$, où $a_0, \ldots, a_n \in \mathbb{C}$ (le polynôme caractéristique de A).

On a :

$$\begin{aligned}\chi_A(A) &= \sum_{k=1}^{n+1}a_{k-1}A^{k-1} \\ &= \frac{1}{2\pi}\sum_{k=1}^{n+1}a_{k-1}\int_0^{2\pi}(re^{it})^k(re^{it}I_n - A)^{-1}dt\end{aligned}$$

Par suite

$$\chi_A(A) = \frac{1}{2\pi}\int_0^{2\pi} \chi_A(re^{it})re^{it}(\mathrm{re}^{it}\, I_n - A)^{-1}\,\mathrm{dt}$$

Or, d'après la formule fondamentale vérifiée par la comatrice, on a :

$${}^t\,\mathrm{Com}(X.I_n - A)(X.I_n - A) = \chi_A(X)I_n$$

En évaluant çela en re^{it}, on obtient pour tout $r > R$ et pour tout $t \in [0, 2\pi]$:

$$\chi_A(re^{it})re^{it}(re^{it}I_n - A)^{-1} = {}^t\,\mathrm{Com}(re^{it}.I_n - A)$$

Par suite

$$\chi_A(A) = \frac{1}{2\pi}\int_0^{2\pi} re^{it\,t}\,\mathrm{Com}(re^{it}I_n - A)\,\mathrm{dt} = 0$$

car les coefficients de la matrice sous le signe intégral sont des polynômes trigonométriques de valeurs moyennes nulles.

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice montre que l'ensemble des valeurs d'adhérence d'une suite bornée dont les différences entre termes successifs tendent vers zéro forme un segment dans $\mathbb{R}$.

Exercice 5.

Soit $(u_n)_{n\in\mathbb{N}}$ une suite bornée vérifiant $\lim(u_{n+1} - u_n) = 0$.
Montrer que X_u : l'ensemble des valeurs d'adhérence de la suite $(u_n)_{n\in\mathbb{N}}$ est un segment.

Solution. (SABIR Ilyass)

Selon le théorème de Bolzano-Weiestrass, $(u_n)_{n\in\mathbb{N}}$ admet au moins une valeur d'adhérence.

Si $(u_n)_{n\in\mathbb{N}}$ admet une et une seule valeur d'adhérence alors $(u_n)_{n\in\mathbb{N}}$ est convergente (puisqu'elle est bornée), et dans ce cas X_u est réduit à un singleton.

Si $(u_n)_{n\in\mathbb{N}}$ admet au mois deux valeurs d'dhérence, on va essayer dans un premier temps de montrer que X_u est un intervalle de $\mathbb{R}$, puis qu'il est fermée bornée afin d'atteindre le résultat souhaité.

Soient $\alpha < \beta \in X_u$. Nous allons montrer que pour tout $x \in]\alpha, \beta[$, x est aussi une valeur d'adhérence de $(u_n)_{n\in\mathbb{N}}$.

Soit $\varepsilon > 0$, et $N \in \mathbb{N}$. L'objectif est de trouver $M \geqslant N$ tel que $|u_M - x| \leqslant \varepsilon$. Quitte à diminuer ε, on peut supposer qu'on a $\alpha < x - \varepsilon < x + \varepsilon < \beta$

Puisque $\lim(u_{n+1} - u_n) = 0$, il existe $n_1 \in \mathbb{N}$ tel que pour tout $n \geqslant n_1$ on a $|u_{n+1} - u_n| \leqslant \varepsilon$.

Puisque $\alpha \in X_u$, alors il existe $n_2 \geqslant \max(N, n_1)$ tel que $u_{n_2} \in]-\infty, x-\varepsilon[$. De même, $\beta \in X_u$, alors il existe $n_3 \geqslant n_2$ tel que $u_{n_3} \in]x + \varepsilon, +\infty[$

Notons

$$n_{\max} = \max\{n \in [\![n_2, n_3]\!] | u_n < x - \varepsilon\}$$

$\{n \in [\![n_2, n_3]\!] | u_n < x - \varepsilon\}$ est non vide (il contient n_2), et majoré par n_3, donc $n_{\max}$est bien défini, de plus $n_{\max} \leqslant n_3$. On a donc $u_{n_{\max}+1} \geqslant x - \varepsilon$, mais aussi

$$u_{n_{\max}+1} \leqslant u_{n_{\max}} + |u_{n_{\max}+1} - u_{n_{\max}}| \leqslant u_{n_{\max}} + \varepsilon \leqslant x$$

Et donc on a trouvé $M := n_{\max} + 1 \geqslant N$ tel que $u_{n_{\max}+1} \in [x - \varepsilon, x]$. Ceci montre que $x \in X_u$.

Ainsi, $X_u$est un intervalle de $\mathbb{R}$, il est borné car $(u_n)_{n\in\mathbb{N}}$ est bornée (X_u est majoré par $\max\limits_{n\in\mathbb{N}}(u_n)$, et minoré par $-\max\limits_{n\in\mathbb{N}}(u_n)$). De plus X_u peut être écrit sous la forme :

$$X_u = \bigcap_{N\in\mathbb{N}} \mathrm{Adh}\{u_n | n \geqslant N\}$$

Où $\mathrm{Adh}(A)$ désigne l'adhérence de A pour la norme usuelle de $\mathbb{R}$, pour tout $A \subset \mathbb{R}$.

Ainsi, X_u est férmée. En conclusion X_u est un intervalle fermé et borné de $\mathbb{R}$, donc il s'agit bien d'un segment de $\mathbb{R}$

✠✠✠✠✠✠✠

Dans cet exercice, nous étudions le comportement asymptotique de la suite $(u_n)_{n\in\mathbb{N}}$ définie par récurrence, en analysant sa croissance et en obtenant les deux premiers termes de son développement asymptotique.

Exercice 6.

Soit $(u_n)_{n\in\mathbb{N}}$ définie par $u_0 \in \mathbb{R}$, et la relation : $u_{n+1} = u_n + e^{-u_n}$ pour tout $n \in \mathbb{N}$.

Donner les deux premiers termes du développement asymptotique de u_n.

Solution. (SABIR Ilyass)

La suite $(u_n)_{n\in\mathbb{N}}$ est croissante. Si elle convergeait vers $l \in \mathbb{R}$, on aurait, par continuité de l'exponentielle, $\lim\limits_{n\longrightarrow+\infty} e^{-u_n} = e^{-l} = 0$, ce qui est impossible. Donc, la suite $(u_n)_{n\in\mathbb{N}}$ tend vers $+\infty$.

Posons, pour tout entier naturel n, $v_n = e^{u_n}$. On obtient :

$$v_{n+1} = e^{u_{n+1}} = e^{u_n + \frac{1}{v_n}} = v_n e^{\frac{1}{v_n}}$$

La suite $(v_n)_{n\in\mathbb{N}}$ est à termes strictement positifs, croît, et diverge vers $+\infty$. On a :

$$v_{n+1} = v_n\left(1 + \frac{1}{v_n} + \frac{1}{2v_n^2} + o\left(\frac{1}{v_n^2}\right)\right) = v_n + 1 + \frac{1}{2v_n} + o\left(\frac{1}{v_n}\right)$$

On en déduit que : $\lim\limits_{n\longrightarrow+\infty}(v_{n+1} - v_n) = 1$. Donc :

$$v_n - v_0 \underset{n\longrightarrow+\infty}{\sim} n \text{ and donc } v_n \underset{n\longrightarrow+\infty}{\sim} n$$

et :

$$v_{n+1} - v_n - 1 = \frac{1}{2v_n} + o\left(\frac{1}{v_n}\right) \underset{n\longrightarrow+\infty}{\sim} \frac{1}{2v_n} \underset{n\longrightarrow+\infty}{\sim} \frac{1}{2n}$$

On obtient :

$$v_n - v_1 - (n-1) \underset{n\longrightarrow+\infty}{\sim} \sum_{k=1}^{n-1} \frac{1}{2k} \underset{n\longrightarrow+\infty}{\sim} \frac{1}{2}\ln(n-1) \underset{n\longrightarrow+\infty}{\sim} \frac{1}{2}\ln(n)$$

Ainsi :

$$v_n = n + \frac{1}{2}\ln(n) + o(\ln(n))$$

En conséquence :

$$\begin{aligned} u_n &= \ln(v_n) \\ &= \ln\left(n + \frac{1}{2}\ln(n) + o(\ln(n))\right) \\ &= \ln\left(n\left(1 + \frac{1}{2}\frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)\right)\right) \end{aligned}$$

On développe alors :

$$u_n = \ln(n) + \ln\left(1 + \frac{1}{2}\frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)\right)$$

Enfin :

$$u_n = \ln(n) + \frac{1}{2}\frac{\ln(n)}{n} + o\left(\frac{\ln(n)}{n}\right)$$

✠✠✠✠✠✠✠

Cet exercice vise à montrer que, parmi 13 nombres réels distincts, on peut toujours en choisir deux, a et b, tels que le rapport $\frac{a-b}{1+a.b}$ soit compris entre 0 et $2-\sqrt{3}$.

Exercice 7. (Oral de l'X)

Montrer que parmi les 13 réels distincts ,on peut toujours en choisir deux ,disons a et b tels que :

$$0 < \frac{a-b}{1+a.b} < 2-\sqrt{3}$$

Solution. (SABIR Ilyass)

Soient $a_1 < a_2 < \cdots < a_{13}$des réels ,l'expression $\frac{a-b}{1+a.b}$ rappelle le développement de $\tan(x-y)$

Considérons $\theta_i = \arctan(a_i)$, pour tout $i \in [\![1, 13]\!]$,on a la fonction arctan est strictement croissante

Alors :

$$\theta_1 < \theta_2 < \cdots < \theta_{13}$$

et ils sont dans $]-\frac{\pi}{2}, \frac{\pi}{2}[$,

Donc, il existe $k_0 \in [\![1, 12]\!]$ tel que $\theta_{k_0+1} - \theta_{k_0} < \frac{\pi}{12}$, (car sinon, c-à-d si $\forall k \in [\![1, 12]\!]$ $\theta_{k+1} - \theta_k > \frac{\pi}{12}$, on aurait $\theta_{13} - \theta_0 = \sum_{k=1}^{12} \theta_{k+1} - \theta_k \geqslant \pi$, ce qui est absurde avec : $\theta_{13}, \theta_0 \in]-\frac{\pi}{2}, \frac{\pi}{2}[$ et la longueur de $]-\frac{\pi}{2}, \frac{\pi}{2}[$ est égale à π).

Comme la fonction tan est strictement croissante sur $[0, \frac{\pi}{2}[$, alors

$$0 < \tan(\theta_{k_0+1} - \theta_{k_0}) < \tan\left(\frac{\pi}{12}\right)$$

Or,

$$\tan(\theta_{k_0+1} - \theta_{k_0}) = \frac{\tan(\theta_{k_0+1}) - \tan(\theta_{k_0})}{1 + \tan(\theta_{k_0}) \tan(\theta_{k_0+1})} = \frac{a_{k_0+1} - a_{k_0}}{1 + a_{k_0} a_{k_0+1}}$$

le réel $x = \tan\left(\frac{\pi}{12}\right)$ vérifie l'équation :

$$\frac{2x}{1 - x^2} = \tan\left(\frac{\pi}{6}\right) = \frac{1}{\sqrt{3}}$$

En résolvant cette équation, on obtient $x = -\sqrt{3} \pm 2$, avec $\tan\left(\frac{\pi}{12}\right) > 0$, on a $x = \tan\left(\frac{\pi}{12}\right) = 2 - \sqrt{3}$

Par conséquent :

$$0 < \frac{a_{k_0+1} - a_{k_0}}{1 + a_{k_0} a_{k_0+1}} < 2 - \sqrt{3}$$

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice explore une inégalité mathématique impliquant une somme pondérée de puissances de variables positives.

Exercice 8.

Soient $a_1, \ldots, a_m > 0$, $n \in \mathbb{N}^*$. Montrer que le maximum de $K = K(a_1, \ldots, a_n)$ vérifiant pour tout $x_1, \ldots, x_m > 0$

$$\sum_{k=1}^{m} a_k x_k^n \geqslant K \left(\sum_{k=1}^{m} x_k\right)^n$$

est :

$$K = \frac{1}{\left(\frac{1}{\sqrt[n-1]{a_1}} + \cdots + \frac{1}{\sqrt[n-1]{a_m}}\right)^{n-1}}$$

Solution. (SABIR Ilyass)

Soit $x_1, \ldots, x_m > 0$

Soient $y_1, \ldots, y_m$ des nombres réels non-négatifs tels que $y_1 + \cdots + y_m = x_1 + \cdots + x_m$

Selon l'**inégalité de Hölder**, on a

$$\left(\sum_{k=1}^{m} a_k x_k^n\right)\left(\sum_{k=1}^{m} a_k y_k^n\right)^{n-1} \geqslant \left(\sum_{k=1}^{m} a_k x_k y_k^{n-1}\right)^n$$

Par conséquent,

$$\sum_{k=1}^{m} a_k x_k^n \geqslant \frac{\left(\sum\limits_{k=1}^{m} a_k x_k y_k^{n-1}\right)^n}{\left(\sum\limits_{k=1}^{m} a_k y_k^n\right)^{n-1}}$$

Nous choisirons $y_1, \ldots, y_m$ de sorte que $a_1 y_1^{n-1} = \cdots = a_m y_m^{n-1} = C$, Si c'est le cas alors

$$\sum_{k=1}^{m} a_k x_k^n \geqslant \frac{C^n \left(\sum\limits_{k=1}^{m} x_k\right)^n}{C^{n-1}\left(\sum\limits_{k=1}^{m} y_k\right)^{n-1}} = C\sum_{k=1}^{m} x_{1k}$$

On a pour tout $k = 1, \ldots, m$

$$y_k = \sqrt[n-1]{\frac{C}{a_k}}$$

Par conséquent,

$$\sqrt[n-1]{C}\left(\frac{1}{\sqrt[n-1]{a_1}} + \cdots + \frac{1}{\sqrt[n-1]{a_m}}\right) = x_1 + \cdots + x_m$$

Ainsi,

$$C = \frac{(x_1 + \cdots + x_m)^{n-1}}{\left(\frac{1}{\sqrt[n-1]{a_1}} + \cdots + \frac{1}{\sqrt[n-1]{a_m}}\right)^{n-1}}$$

On en déduit que

$$\sum_{k=1}^{m} a_k x_k^n \geqslant \frac{(x_1 + \cdots + x_m)^n}{\left(\frac{1}{\sqrt[n-1]{a_1}} + \cdots + \frac{1}{\sqrt[n-1]{a_m}}\right)^{n-1}}$$

Et l'égalité est atteinte pour $x_k = \frac{1}{\sqrt[n-1]{a_k}\left(\frac{1}{\sqrt[n-1]{a_1}}+\cdots+\frac{1}{\sqrt[n-1]{a_m}}\right)}$, $k = 1, \ldots, m$

D'où le résultat.

✠✠✠✠✠✠✠

Dans cet exercice, nous étudions une inégalité impliquant des sommes doubles de racines carrées. Elle compare deux expressions similaires, l'une faisant intervenir des différences de nombres réels, l'autre leurs sommes.

Exercice 9. (IMO 2021)

Montrer que pour tout $x_1, \ldots, x_n \in \mathbb{R}$, on a :

$$\sum_{i=1}^{n}\sum_{j=1}^{n}\sqrt{|x_i - x_j|} \leqslant \sum_{i=1}^{n}\sum_{j=1}^{n}\sqrt{|x_i + x_j|}$$

Solution. (SABIR Ilyass)

Sans perte de généralité, on peut supposer que $x_1, \ldots, x_n \neq 0$. On a :

$$\begin{aligned}
H(x_1, \ldots, x_n) &:= \sum_{i=1}^{n}\sum_{j=1}^{n}\sqrt{|x_i + x_j|} - \sum_{i=1}^{n}\sum_{j=1}^{n}\sqrt{|x_i - x_j|} \\
&= \sum_{i=1}^{n}\sum_{j=1}^{n}\frac{|x_i + x_j| - |x_i - x_j|}{\sqrt{|x_i + x_j|} + \sqrt{|x_i - x_j|}} \\
&= 2\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{\operatorname{sgn}(x_i)\operatorname{sgn}(x_j)\min(|x_i|, |x_j|)}{\sqrt{|x_i + x_j|} + \sqrt{|x_i - x_j|}} \\
&\geqslant \frac{2}{\max\limits_{1\leqslant i,j\leqslant n}\left(\sqrt{|x_i + x_j|} + \sqrt{|x_i - x_j|}\right)}\sum_{i=1}^{n}\sum_{j=1}^{n}\operatorname{sgn}(x_i)\operatorname{sgn}(x_j)\min(|x_i|, |x_j|) \\
&= \frac{2}{\max\limits_{1\leqslant i,j\leqslant n}\left(\sqrt{|x_i + x_j|} + \sqrt{|x_i - x_j|}\right)}\int_0^{+\infty}\left(\sum_{i=1}^{n}\operatorname{sgn}(x_i)\mathbf{1}_{[\mathbf{0},|\boldsymbol{x_i}|]}(x)\right)^2 dx \\
&\geqslant 0
\end{aligned}$$

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice explore des propriétés de congruences binomiales et des puissances modulo un nombre premier p, en combinatoire et arithmétique modu-

laire, avec des démonstrations utiles pour les concours d'entrée aux grandes écoles scientifiques.

Exercice 10. (Oral Paris-Lyon-Cachan-Rennes 98)

Soit p un nombre premier.

1- Montrer que pour tout $x \in \mathbb{Z}$,

$$(1+x)^p \equiv 1 + x^p \pmod{p}$$

Soit m et n deux entiers naturels, on écrit m et n en base p :

$$m = \sum_{i=0}^{+\infty} a_i p^i \text{et } n = \sum_{i=0}^{+\infty} b_i p^i$$

2- Montrer que :

$$\binom{m}{n} \equiv \prod_{i=0}^{+\infty} \binom{a_i}{b_i} \pmod{p}$$

3- Avec les notations précédentes, montrer que :

$$\binom{pm}{pn} \equiv \binom{m}{n} \pmod{p}$$

Solution. (SABIR Ilyass)

1- Soit $x \in \mathbb{Z}$, on a :

$$(1+x)^p = \sum_{i=0}^{p} \binom{p}{i} x^i = 1 + x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i$$

Pour tout $i \in [\![1, p-1]\!]$ on a :

$$i! \binom{p}{i} = p(p-1) \times \cdots \times (p-i+1)$$

Ainsi, $p | i! \binom{p}{i}$, puisque p est premier, donc pour tout $k \in [\![1, i]\!]$, p ne divise pas k. En particulier p ne divise par $i\,!$. Via le lemme de Gauss $p | \binom{p}{i}$.

D'où

$$\sum_{i=1}^{p-1} \binom{p}{i} x^i \equiv 0 \pmod{p}$$

Par conséquent,

$$(1+x)^p \equiv 1 + x^p \pmod{p}$$

2- Soit N_0 (respectivement N_1) le plus petit entier tel que pour tout $i \geqslant N_0 + 1$, $b_i = 0$ (respectivement pour tout $i \geqslant N_1 + 1$, $a_i = 0$).

Si $n > m$, alors

$$\binom{m}{n} = 0$$

D'autre part, vu que $n > m$, alors ou bien $N_0 > N_1$ ou bien $N_0 = N_1$ et $b_{N_0} > a_{N_0}$.

Dans les deux cas, on a

$$\binom{a_{N_0}}{b_{N_0}} = \binom{0}{b_{N_0}} = 0 (\text{carb}_{N_0} \neq 0)$$

Donc :

$$\prod_{i=0}^{+\infty} \binom{a_i}{b_i} = \binom{a_{N_0}}{b_{N_0}} \prod_{i=0 i \neq N_0}^{+\infty} \binom{a_i}{b_i} = 0$$

Si $n \leqslant m$, alors dans $\mathbb{Z}/p\mathbb{Z}[X]$:

$$\begin{aligned} (X+1)^m &= (X+1)^{\sum_{i=0}^{+\infty} a_i p^i} \\ &= \prod_{i=0}^{+\infty} ((X+1)^{p^i})^{a_i} \end{aligned}$$

Or, pour tout $r \in \mathbb{N}^*$, d'après la question 1, pour tout $j \in [\![1, r]\!]$, on a

$$\begin{aligned} (X^{p^{r-j}} + 1)^{p^j} &= ((X^{p^{r-j}} + 1)^p)^{p^{j-1}} \\ &= (X^{p^{r-(j-1)}} + 1)^{p^{j-1}} \end{aligned}$$

En particulier, pour tout $r \in \mathbb{N}^*$

$$(X+1)^{p^r} = 1 + X^{p^r} (\text{modp})$$

Ce résultat reste vrai pour $r = 0$, donc pour tout $r \in \mathbb{N}$

$$(X+1)^{p^r} = 1 + X^{p^r} (\text{modp})$$

Ainsi, dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a

$$\begin{aligned}(1+X)^m &= \prod_{i=0}^{N_1}(1+X^{p^i})^{a_i} \\ &= \prod_{i=0}^{N_1}\sum_{j_i=0}^{a_i}\binom{a_i}{j_i}X^{j_i p^i} \\ &= \sum_{j_0=0}^{a_0}\sum_{j_1=0}^{a_1}\cdots\sum_{j_{N_1}=0}^{a_{N_1}}\prod_{i=0}^{N_1}\binom{a_i}{j_i}X^{\sum_{i=0}^{N_1}j_i p^i}\end{aligned}$$

D'autre part,

$$(1+X)^m = \sum_{j=0}^{m}\binom{m}{j}X^j$$

Pour $n \in [\![0, m]\!]$, le coefficient du monôme de degré n à gauche est $\binom{m}{n}$ et celui de droite est $\prod_{i=0}^{N_1}\binom{a_i}{b_i}$.

Par unicité des coefficients d'un polynôme, on a :

$$\binom{m}{n} \equiv \prod_{i=0}^{+\infty}\binom{a_i}{b_i} \pmod{p}$$

3- Montrons que

$$\binom{pm}{pn} \equiv \binom{m}{n} \pmod{p}$$

On a

$$m = \sum_{i=0}^{+\infty} a_i p^i \text{et } n = \sum_{i=0}^{+\infty} b_i p^i$$

Alors

$$pm = \sum_{i=1}^{+\infty} a_{i-1} p^i \text{et } pn = \sum_{i=1}^{+\infty} b_{i-1} p^i$$

Donc, d'après la question précédente,

$$\begin{aligned}\binom{pm}{pn} &\equiv \binom{0}{0}\prod_{i=1}^{+\infty}\binom{a_i}{b_i} \pmod{p} \\ &\equiv \prod_{i=1}^{+\infty}\binom{a_i}{b_i} \pmod{p} \\ &\equiv \binom{m}{n} \pmod{p}\end{aligned}$$

D'où le résultat.

✠✠✠✠✠✠✠

1- Soit $x \in \mathbb{Z}$, on a :

$$(1+x)^p = \sum_{i=0}^{p} \binom{p}{i} x^i = 1 + x^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i$$

Pour tout $i \in [\![1, p-1]\!]$ on a :

$$i! \binom{p}{i} = p(p-1) \times \cdots \times (p-i+1)$$

Ainsi, $p | i! \binom{p}{i}$, puisque p est premier, donc pour tout $k \in [\![1, i]\!]$, p ne divise pas k. En particulier p ne divise par $i\,!$. Via le lemme de Gauss $p | \binom{p}{i}$.

D'où

$$\sum_{i=1}^{p-1} \binom{p}{i} x^i \equiv 0 \pmod{p}$$

Par conséquent,

$$(1+x)^p \equiv 1 + x^p \pmod{p}$$

2- Soit N_0 (respectivement N_1) le plus petit entier tel que pour tout $i \geqslant N_0 + 1$, $b_i = 0$ (respectivement pour tout $i \geqslant N_1 + 1$, $a_i = 0$).

Si $n > m$, alors

$$\binom{m}{n} = 0$$

D'autre part, vu que $n > m$, alors ou bien $N_0 > N_1$ ou bien $N_0 = N_1$ et $b_{N_0} > a_{N_0}$.

Dans les deux cas, on a

$$\binom{a_{N_0}}{b_{N_0}} = \binom{0}{b_{N_0}} = 0 (\text{carb}_{N_0} \neq 0)$$

Donc :

$$\prod_{i=0}^{+\infty} \binom{a_i}{b_i} = \binom{a_{N_0}}{b_{N_0}} \prod_{i=0 i \neq N_0}^{+\infty} \binom{a_i}{b_i} = 0$$

Si $n \leqslant m$, alors dans $\mathbb{Z}/p\mathbb{Z}[X]$:

$$\begin{aligned} (X+1)^m &= (X+1)^{\sum_{i=0}^{+\infty} a_i p^i} \\ &= \prod_{i=0}^{+\infty} ((X+1)^{p^i})^{a_i} \end{aligned}$$

Or, pour tout $r \in \mathbb{N}^*$, d'après la question 1, pour tout $j \in [\![1, r]\!]$, on a

$$\begin{aligned}(X^{p^{r-j}}+1)^{p^j} &= ((X^{p^{r-j}}+1)^p)^{p^{j-1}} \\ &= (X^{p^{r-(j-1)}}+1)^{p^{j-1}}\end{aligned}$$

En particulier, pour tout $r \in \mathbb{N}^*$

$$(X+1)^{p^r} = 1 + X^{p^r} (\text{modp})$$

Ce résultat reste vrai pour $r = 0$, donc pour tout $r \in \mathbb{N}$

$$(X+1)^{p^r} = 1 + X^{p^r} (\text{modp})$$

Ainsi, dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a

$$\begin{aligned}(1+X)^m &= \prod_{i=0}^{N_1} (1+X^{p^i})^{a_i} \\ &= \prod_{i=0}^{N_1} \sum_{j_i=0}^{a_i} \binom{a_i}{j_i} X^{j_i p^i} \\ &= \sum_{j_0=0}^{a_0} \sum_{j_1=0}^{a_1} \cdots \sum_{j_{N_1}=0}^{a_{N_1}} \prod_{i=0}^{N_1} \binom{a_i}{j_i} X^{\sum_{i=0}^{N_1} j_i p^i}\end{aligned}$$

D'autre part,

$$(1+X)^m = \sum_{j=0}^{m} \binom{m}{j} X^j$$

Pour $n \in [\![0, m]\!]$, le coefficient du monôme de degré n à gauche est $\binom{m}{n}$ et celui de droite est $\prod_{i=0}^{N_1} \binom{a_i}{b_i}$.

Par unicité des coefficients d'un polynôme, on a :

$$\binom{m}{n} \equiv \prod_{i=0}^{+\infty} \binom{a_i}{b_i} \pmod{p}$$

3- Montrons que

$$\binom{pm}{pn} \equiv \binom{m}{n} \pmod{p}$$

On a

$$m = \sum_{i=0}^{+\infty} a_i p^i \text{et } n = \sum_{i=0}^{+\infty} b_i p^i$$

Alors

$$pm = \sum_{i=1}^{+\infty} a_{i-1}p^i \text{et } pn = \sum_{i=1}^{+\infty} b_{i-1}p^i$$

Donc, d'après la question précédente,

$$\begin{aligned}\binom{pm}{pn} &\equiv \binom{0}{0}\prod_{i=1}^{+\infty}\binom{a_i}{b_i} \pmod p \\ &\equiv \prod_{i=1}^{+\infty}\binom{a_i}{b_i} \pmod p \\ &\equiv \binom{m}{n} \pmod p\end{aligned}$$

D'où le résultat.

✠✠✠✠✠✠✠

Les inégalités entre moyennes sont au cœur de l'étude des inégalités en général. Cet exercice nous propose d'étudier une inégalité faisant intervenir des puissances et qui généralise les inégalités entre moyennes.

Exercice 11.

Soient $a, b, c > 0$. Montrer que pour tout $k \in \mathbb{N}$,

$$\frac{a^{k+1}}{b^k} + \frac{b^{k+1}}{c^k} + \frac{c^{k+1}}{a^k} \geqslant a + b + c$$

Solution. (SABIR Ilyass)

Méthode 1.

En utilisant l'inégalité arithmético-géométrique (AM-GM), on a :

$$\frac{a^{k+1}}{b^k} + kb = \frac{a^{k+1}}{b^k} + \sum_{j=1}^{k} b \geqslant (k+1)a$$

Par symétrie, on obtient :

$$\frac{a^{k+1}}{b^k} + \frac{b^{k+1}}{c^k} + \frac{c^{k+1}}{a^k} + k(b+c+a) \geqslant (k+1)(a+b+c)$$

D'où le résultat.

Méthode 2.

Montrons le resultat par récurrence forte sur $k \in \mathbb{N}$.

Pour $k = 0$, ona :

$$\begin{aligned} \frac{a^{k+1}}{b^k} + \frac{b^{k+1}}{c^k} + \frac{c^{k+1}}{a^k} &= a+b+c \\ &\geqslant a+b+c \end{aligned}$$

Soit $k \in \mathbb{N}$, supposons que pour tout $j \in [\![0, k]\!]$, on ait :

$$\frac{a^{j+1}}{b^j} + \frac{b^{j+1}}{c^j} + \frac{c^{j+1}}{a^j} \geqslant a+b+c$$

Et montrons que :

$$\frac{a^{k+2}}{b^{k+1}} + \frac{b^{k+2}}{c^{k+1}} + \frac{c^{k+2}}{a^{k+1}} \geqslant a+b+c$$

Si k est pair, alors il existe un $l \in \mathbb{N}$ tel que $k = 2l$. Ainsi,

$$\begin{aligned} \frac{a^{k+2}}{b^{k+1}} + b &= \frac{a^{2l+2}}{b^{2l+1}} + b \\ &\geqslant 2\frac{a^{l+1}}{b^l} \end{aligned}$$

Par symétrie, on a alors :

$$\frac{a^{k+2}}{b^{k+1}} + b + \frac{b^{k+2}}{c^{k+1}} + c + \frac{c^{k+2}}{a^{k+1}} + a \geqslant 2\left(\frac{a^{l+1}}{b^l} + \frac{b^{l+1}}{c^l} + \frac{c^{l+1}}{a^l}\right)$$

Or,

$$\frac{a^{l+1}}{b^l} + \frac{b^{l+1}}{c^l} + \frac{c^{l+1}}{a^l} \geqslant a+b+c$$

Ainsi,

$$\frac{a^{k+2}}{b^{k+1}} + b + \frac{b^{k+2}}{c^{k+1}} + c + \frac{c^{k+2}}{a^{k+1}} + a \geqslant 2(a+b+c)$$

D'où

$$\frac{a^{k+2}}{b^{k+1}} + \frac{b^{k+2}}{c^{k+1}} + \frac{c^{k+2}}{a^{k+1}} \geqslant a+b+c$$

De même, on montre le résultat dans le cas où k est impair.

Méthode 3. (Hors programme)

Via l'inégalité de Hölder, on a

$$\left(\frac{a^{k+1}}{b^k} + \frac{b^{k+1}}{c^k} + \frac{c^{k+1}}{a^k}\right)(b+c+a)^k \geqslant (a+b+c)^{k+1}$$

D'où le résultat.

✠✠✠✠✠✠✠

L'algèbre linéaire nous réserve parfois des surprises en liant commutateurs de matrices et nilpotence. Cet exercice propose d'établir un résultat remarquable sur la nilpotence d'une matrice vérifiant une relation particulière avec son commutateur.

Exercice 12. (Oral ULM Lyon Cachan Rennes 2016)

Soit A et B dans $M_n(\mathbb{R})$ telles que :

$$AB - BA = A$$

1. Montrer que A est nilpotente
2. Même question en remplaçant $\mathbb{R}$ par $\mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, et en supposant $p > n$.

Solution. (SABIR Ilyass)

1. On remarque tout d'abord qu'on a :

$$A^2B - ABA = A^2 \text{ et } ABA - BA^2 = A^2$$

Donc,

$$A^2B - BA^2 = 2A^2$$

et

$$A^3B - A^2BA = 2A^3 \text{et } ABA^2 - BA^3 = A^3$$

Ainsi,

$$A^3B - BA^3 = 3A^3$$

Par récurrence, on établit que, pour tout $k \in \mathbb{N}$

$$A^kB - BA^k = kA^k \quad (1)$$

Méthode 1 :

Par (1), on a pour tout $k \in \mathbb{N}^*$:

$$\mathrm{tr}(kA^k) = \mathrm{tr}(A^kB - BA^k) = \mathrm{tr}(A^kB) - \mathrm{tr}(BA^k) = 0$$

Donc

$$k \cdot \mathrm{tr}(A^k) = 0$$

Par suite, opour tout $k \in \mathbb{N}^*$

$$\mathrm{tr}(A^k) = 0$$

C'est très classique, les seules matrices qui vérifient cette propriété sont les matrices nilpotentes.

Méthode 2 :

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

Pour tout $k \in [\![0, n]\!]$, on a

$$\sum_{k=0}^{n} a_k (A^k B - B A^k) = \sum_{k=0}^{n} a_k k A^k$$

Donc

$$\left(\sum_{k=0}^{n} a_k A^k\right) B - B \left(\sum_{k=0}^{n} a_k A^k\right) = A \sum_{k=1}^{n} a_k k A^{k-1}$$

Ainsi

$$P(A)B - BP(A) = AP'(A)$$

Notons Π_A le polynôme minimal de A. On a

$$X\Pi'_A(A) = \Pi_A(A)B - B\Pi_A(A) = 0$$

Donc $Q = X\Pi'_A$ annule A, et par conséquent Π_A divise Q.

Or, $\deg(Q) = 1 + \deg(\Pi'_A) = \deg(\Pi_A)$, donc Q et Π_A sont associés, ce qui implique qu'il existe $r \in \mathbb{R}$ tel que

$$X\Pi'_A = r\Pi_A$$

Par suite, il existe $k \in \mathbb{N}$ tel que $\Pi_A = X^k$.

D'où A est niplotante.

Remarque.

Voir aussi la partie II, CCP(MP 2012) - exercice 2.

Ce résultat de la question 1 reste valable pour tout anneau de caractéristique nulle, on va voir dans la question 2 que le résultat est également vrai sur $\mathbb{Z}/p\mathbb{Z}$, avec $p > n$.

2. Même raisonnement.

Etant donné que $\mathbb{Z}/p\mathbb{Z}$ est intègre, et que $p > n$, Le raisonnement précédent s'applique ici.

Ce résultat reste vrai pour tout anneau intègre de caractéristique nulle ou de caractéristique r avec $r > n$.

✠✠✠✠✠✠✠

Cet exercice propose de démontrer une inégalité entre la somme de termes positifs et l'inverse de la moyenne harmonique, qui est majorée par le double de la somme arithmétique des termes.

Exercice 13.

Soient $a_1, \ldots, a_n > 0$, Montrer que :

$$a_1 + \frac{2}{\frac{1}{a_1} + \frac{1}{a_2}} + \cdots + \frac{n}{\frac{1}{a_1} + \cdots + \frac{1}{a_n}} < 2(a_1 + \cdots + a_n)$$

Solution. (SABIR Ilyass)

Posons, pour tout $k \in [\![1, n]\!]$: $y_k = \frac{1}{a_k}$, et montrons que :

$$\frac{1}{y_1} + \frac{2}{y_1 + y_2} + \cdots + \frac{n}{y_1 + \cdots + y_n} < 2\left(\frac{1}{y_1} + \cdots + \frac{1}{y_n}\right)$$

Considérons $x_1, \ldots, x_n > 0$. D'après l'inégalité de Cauchy-Schwarz, pour tout $k \in [\![1, n]\!]$:

$$(y_1 + \cdots + y_k)\left(\frac{x_1^2}{y_1} + \cdots + \frac{x_k^2}{y_k}\right) \geqslant (x_1 + \cdots + x_k)^2$$

Ainsi, pour tout $k \in [\![1, n]\!]$, on obtient :

$$\frac{k}{y_1 + \cdots + y_k} \leqslant \frac{k}{(x_1 + \cdots + x_k)^2}\left(\frac{x_1^2}{y_1} + \cdots + \frac{x_k^2}{y_k}\right)$$

En sommant, on a :

$$\sum_{k=1}^{n} \frac{k}{y_1 + \cdots + y_k} \leqslant \sum_{k=1}^{n} \frac{k}{(x_1 + \cdots + x_k)^2} \left(\frac{x_1^2}{y_1} + \cdots + \frac{x_k^2}{y_k} \right)$$

En développant l'expression, on obtient :

$$\begin{aligned} \sum_{k=1}^{n} \frac{k}{(x_1 + \cdots + x_k)^2} \left(\frac{x_1^2}{y_1} + \cdots + \frac{x_k^2}{y_k} \right) &= \sum_{k=1}^{n} \sum_{j=1}^{k} \frac{k}{(x_1 + \cdots + x_k)^2} \times \frac{x_j^2}{y_j} \\ &= \sum_{j=1}^{n} \sum_{k=j}^{n} \frac{k}{(x_1 + \cdots + x_k)^2} \times \frac{x_j^2}{y_j} \end{aligned}$$

On en déduit :

$$\sum_{k=1}^{n} \frac{k}{y_1 + \cdots + y_k} \leqslant \sum_{j=1}^{n} \left(\sum_{k=j}^{n} \frac{k.x_j^2}{(x_1 + \cdots + x_k)^2} \right) \times \frac{1}{y_j}$$

Pour tout $j \in [\![1, n]\!]$, si on pose $x_j = j$, on a :

$$\begin{aligned} \sum_{k=j}^{n} \frac{k.x_j^2}{(x_1 + \cdots + x_k)^2} &= \sum_{k=j}^{n} \frac{k.j^2}{(1 + \cdots + k)^2} \\ &= 4j^2 \sum_{k=j}^{n} \frac{1}{k(k+1)^2} \\ &\leqslant 2j^2 \sum_{k=j}^{n} \frac{2k+1}{k(k+1)^2} \\ &= 2j^2 \sum_{k=j}^{n} \left(\frac{1}{k^2} - \frac{1}{(k+1)^2} \right) \end{aligned}$$

Donc :

$$\sum_{k=j}^{n} \frac{k.x_j^2}{(x_1 + \cdots + x_k)^2} \leqslant 2j^2 \left(\frac{1}{j^2} - \frac{1}{(n+1)^2} \right) < 2$$

Finalement, on obtient :

$$\frac{1}{y_1} + \frac{2}{y_1 + y_2} + \cdots + \frac{n}{y_1 + \cdots + y_n} < 2 \left(\frac{1}{y_1} + \cdots + \frac{1}{y_n} \right)$$

✠✠✠✠✠✠✠

Les propriétés arithmétiques des puissances de 2 et leur développement décimal recèlent des surprises fascinantes. Cet exercice propose d'utiliser

des outils de théorie des nombres pour établir un résultat contre-intuitif sur les premiers chiffres de ces puissances.

Exercice 14. (Oral ULM 2008)

Montrer qu'il existe une infinité de puissances de 2 dont le développement décimal commence par 7.

Solution. (SABIR Ilyass)

Le résultat, énoncé ici en base 10, et pour les puissances de 2 qui commence par 7, est en fait valable pour tout base $b \geq 2$ et pour les puissances de $a \geq 2$ tel qu'il existe au moins un nombre premier p qui divise a et ne divise pas b ou divise b et ne divise pas a, et en remplaçant 7 par n'importe quelle nombre $r \in [\![1, b-1]\!]$.

Nous traiterons le cas général, et on souhaite démontrer qu'il existe une infinité de puissances de $a \geq 2$ dont le développement dans la base $b \geq 2$ commence par r où $(a, b, r) \in \mathbb{N}^{*3}$ tel que $a, b \geq 2$, et qu'il existe au moins un nombre premier p qui divise a et ne divise pas b ou qui divise b et ne divise pas a et $r \in [\![1, b-1]\!]$.

Avec les notations précédentes, il suffit de montrer qu'il existe une infinité de couple $(n, k) \in \mathbb{N}^2$ tels que

$$r \leq \frac{a^n}{b^k} < r + 1$$

c'est-à-dire :

$$\ln r \leq n \ln a - k \ln b < \ln(r+1)$$

Montrons que $\ln a\mathbb{Z} + \ln b\mathbb{Z}$ est dense dans $\mathbb{R}$. Puisque les sous-groupes de $\mathbb{R}$ sont soit dense sur $\mathbb{R}$ ou de la forme $\alpha\mathbb{Z}$ où $\alpha \in \mathbb{R}^+$ (résultat classique).

Puisque $\ln a\mathbb{Z} + \ln b\mathbb{Z}$ est un sous-groupe de $\mathbb{R}$, il suffit de montrer que $\ln a\mathbb{Z} + \ln b\mathbb{Z}$ ne s'écrit pas sous la forme $\alpha\mathbb{Z}$ avec $\alpha > 0$. Cela revient à montrer que $\frac{\ln a}{\ln b} \notin \mathbb{Q}$.

Supposons par l'absurde que $\frac{\ln a}{\ln b} \in \mathbb{Q}$, alors il existe $P, Q \in \mathbb{N}^*$ tels que $\frac{\ln a}{\ln b} = \frac{P}{Q}$ donc $a^Q = b^P$, ce qui est contradictoire avec l'existence de p premier

qui divise a et ne divise pas b ou divise b et ne divise pas a.

Ainsi, $\ln a\mathbb{Z} + \ln b\mathbb{Z}$ dense dans $\mathbb{R}$.

Par conséquent, $(\ln a\mathbb{Z} + \ln b\mathbb{Z}) \cap [\ln r, \ln(r+1)]$ dense dans $[\ln r, \ln r + 1]$, donc il existe une infinité de couples $(n, k) \in \mathbb{Z}^2$ tels que :

$$\ln r \leq n \ln a - k \ln b < \ln(r+1)$$

Pour finir, il ne reste à montrer que l'ensemble :

$$\{(n,k) \in (\mathbb{Z}_-^* \times \mathbb{Z}_-^*) \cup (\mathbb{Z}_-^* \times \mathbb{N}) \cup (\mathbb{N} \times \mathbb{Z}_-^*) \mid \ln r \leq n \ln a - k \ln b < \ln(r+1)\}$$

est fini.

Tout d'abord, il n'existe aucun couple $(n, k) \in \mathbb{Z}_-^* \times \mathbb{N}$ tel que

$$\ln r \leq n \ln a - k \ln b < \ln(r+1)$$

La suite $(n \ln a + k \ln b)_{n\in\mathbb{N}}$ est strictement croissante, puisque $\ln b > 0$ avec $\lim\limits_{n\to+\infty}(n \ln a + k \ln b) = +\infty$

Ainsi, il existe $n_0 \in \mathbb{N}$, tel que pour tout $k \geqslant n_0$

$$n \ln a + k \ln b \geq \ln(r+1)$$

Donc pour que $n \ln a - k \ln b \leq \ln(r+1)$, il faut $k \leq n_0$. Ainsi $k \in \mathbb{Z}_-^* \cap]-n_0, +\infty[$

Par conséquent, $k \in [\![1 - n_0, 0]\!]$ et comme $\ln r \leq n \ln a - k \ln b \leq \ln(r+1)$ alors

$$\frac{\ln r + k \ln b}{\ln a} \leq n \leq \frac{\ln(r+1) + k \ln b}{\ln a}$$

Donc

$$n \in \left[\!\!\left[\left\lceil \frac{\ln r + k \ln b}{\ln a} \right\rceil, \left\lfloor \frac{\ln(r+1) + k \ln b}{\ln a} \right\rfloor \right]\!\!\right]$$

D'où

$$(n,k) \in [\![1 - n_0, 0]\!] \times \bigcup_{k=1-n_0}^{0} \left[\!\!\left[\left\lceil \frac{\ln r + k \ln b}{\ln a} \right\rceil, \left\lfloor \frac{\ln(r+1) + k \ln b}{\ln a} \right\rfloor \right]\!\!\right]$$

est fini

De même, on montre que l'ensemble des couples $(n, k) \in \mathbb{N} \times \mathbb{Z}_-^*$ tel que

$$\ln r \leq n \ln a - k \ln b \leq \ln(r+1)$$

est de cardinal fini.

Ce qui montre qu'il existe une infinité de couples $(n,k) \in \mathbb{N}^2$ tels que $\ln r \leq n \ln a - k \ln b \leq \ln(r+1)$

D'où le résultat.

✠✠✠✠✠✠✠

Les suites de nombres harmoniques sont riches en propriétés intéressantes et cet exercice nous propose d'étudier la partie entière de leur somme partielle. C'est une belle occasion d'explorer les liens entre l'analyse et l'arithmétique.

Exercice 15.

Montrer que $f : \begin{cases} \mathbb{N}^* \to \mathbb{N}^* \\ n \mapsto \left\lfloor 1 + \frac{1}{2} + \cdots + \frac{1}{n} \right\rfloor \end{cases}$ est surjective.

Solution. (SABIR Ilyass)

Montrons que $f : \begin{cases} \mathbb{N}^* \to \mathbb{N}^* \\ n \mapsto \left\lfloor 1 + \frac{1}{2} + \cdots + \frac{1}{n} \right\rfloor \end{cases}$ est surjective.

Notons :

$$A = \{f(n) - 1 | n \in \mathbb{N}^*\}$$

On a f est croissante et $f(1) = 1$, donc $0 \in A$.

Montrons que $\lim\limits_{n \to +\infty} f(n) = +\infty$

On a $t \mapsto \frac{1}{t}$ est décroissante sur $]0, +\infty[$, donc pour tout $k \in \mathbb{N}^*$, on a :

$$\frac{1}{k+1} \leqslant \int_k^{k+1} \frac{dt}{t} \leqslant \frac{1}{k}$$

Donc :

$$\ln(n+1) \leqslant 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

Ainsi, $\lim\limits_{n \to +\infty} f(n) = +\infty$, et pour tout $n \in \mathbb{N}^*$, on a :

$$\begin{aligned} f(n+1) - f(n) &= \left\lfloor 1 + \frac{1}{2} + \cdots + \frac{1}{n+1} \right\rfloor - \left\lfloor 1 + \frac{1}{2} + \cdots + \frac{1}{n} \right\rfloor \\ &\leqslant \left(1 + \frac{1}{2} + \cdots + \frac{1}{n+1} \right) - \left[\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} \right) - 1 \right] \\ &= \frac{1}{n+1} + 1 \end{aligned}$$

Donc :

$$0 \leqslant f(n+1) - f(n) \leqslant \left\lfloor \frac{1}{n+1} + 1 \right\rfloor = 1$$

Soit $k \in A$, donc il existe un $n_0 \in \mathbb{N}^*$ tel que $k+1 = f(n_0)$.

Notons :

$$A_k = \{j \in \mathbb{N} \mid j \geqslant k \text{et } f(j) = k+1\}$$

Si A_k est non bornée, on aurait par croissance de f, pour tout $j \geqslant k$ $f(j) = k+1$, ce qui est absurde avec $\lim\limits_{n \to +\infty} f(n) = +\infty$

Donc, A_k est fini, et admet un plus grand élément noté j_0.

On a alors $f(j_0) = k+1$ et $f(j_0+1) \neq k+1$, et par croissance de f, on a $f(j_0+1) > k+1$

Or :

$$0 \leqslant f(j_0+1) - f(j_0) \leqslant 1$$

Donc, $f(j_0+1) = k+2$, ainsi $k+1 = f(j_0+1) - 1 \in A$

Conclusion

$$\begin{cases} 0 \in A \\ \text{si } k \in A \text{alors } k+1 \in A \end{cases}$$

Par l'axiome de Peano, $A = \mathbb{N}$.

D'où

$$f(\mathbb{N}^*) = A + 1 = \mathbb{N}^*$$

✠✠✠✠✠✠✠

L'étude des fonctions infiniment dérivables satisfaisant des équations fonctionnelles est un domaine fascinant de l'analyse. Cet exercice propose d'étudier une fonction vérifiant une relation linéaire particulière et invite à utiliser les propriétés de dérivation pour conclure.

Exercice 16. (Généralisation de l'oral ULM 2007)

Soient $a_1, a_2, \ldots, a_n > 0$, deux à deux distincts, et $f \in \mathcal{C}^\infty(\mathbb{R}, \mathbb{R})$ vérifiant :

$$\forall x \in \mathbb{R}, f(a_1 x) + f(a_2 x) + \cdots + f(a_n x) = 0$$

Montrer que $f = 0$.

Solution. (SABIR Ilyass)

On a, pour tout $x \in \mathbb{R}$:

$$f(a_1x) + f(a_2x) + \cdots + f(a_nx) = 0$$

Donc, pour tout $r \in \mathbb{N}$ et pour tout $x \in \mathbb{R}$, on obtient :

$$\sum_{k=1}^{n} a_k^r \times f^{(r)}(a_kx) = 0 \quad (1)$$

En particulier, pour tout $r \in \mathbb{N}$, on a :

$$f^{(r)}(0) = 0 \quad (2)$$

On peut supposer sans perte de généralité que $0 < a_1 < a_2 < \cdots < a_n$
Soit $a > 0$, pour tout $x \in [-a, a]$, et pour tout $r \in \mathbb{N}$, on a d'après (1) :

$$f^{(r)}(x) = -\sum_{k=1}^{n-1} \left(\frac{a_k}{a_n}\right)^r \times f^{(r)}\left(\frac{a_kx}{a_n}\right)$$

Notons $M_r = \sup_{x\in[-a,a]} |f^{(r)}(x)|$. On a alors, pour tout $r \in \mathbb{N}$:

$$|f^{(r)}(x)| \leqslant M_r \times \sum_{k=1}^{n-1} \left(\frac{a_k}{a_n}\right)^r$$

Donc :

$$M_r \leqslant M_r \times \sum_{k=1}^{n-1} \left(\frac{a_k}{a_n}\right)^r$$

Or, pour tout $k \in [\![1, n-1]\!]$, on a :

$$0 < \frac{a_k}{a_n} < 1$$

Donc $\left(\frac{a_k}{a_n}\right)^r \xrightarrow[r\to+\infty]{} 0$. Ainsi,

$$\sum_{k=1}^{n-1} \left(\frac{a_k}{a_n}\right)^r \xrightarrow[r\to+\infty]{} 0 < 1$$

Donc, il existe un $r_0 \in \mathbb{N}$, tel que pour tout $r \geq r_0$

$$\sum_{k=1}^{n-1} \left(\frac{a_k}{a_n}\right)^r < 1$$

En particulier, pour tout $r \geq r_0$

$$M_r \leqslant M_r \times \sum_{k=1}^{n-1} \left(\frac{a_k}{a_n}\right)^r < M_r$$

Cela implique que, pour tout $r \geq r_0$, $M_r = 0$, d'où pour tout $r \geq r_0$ et pour tout $x \in [-a, a]$, $f^{(r)}(x) = 0$, et ceci pour tout $a > 0$.

Donc, pour tout $r \geq r_0$ et pour tout $x \in \mathbb{R}$, $f^{(r)}(x) = 0$

Ainsi, f est polynômiale de degré inférieur ou égal à $r_0 - 1$, et on a pour tout $x \in \mathbb{R}$

$$f(x) = \sum_{k=0}^{r_0-1} \frac{f^{(k)}(0)}{k!} x^k = 0$$

Finalement, $f = 0$. (d'après (2)).

✠✠✠✠✠✠✠

Les propriétés des suites de la forme $\{nx\}$ (partie fractionnaire) sont riches en applications dans l'étude de la répartition des nombres. Cet exercice propose d'établir un résultat sur l'existence d'un terme de cette suite dans un intervalle donné.

Exercice 17.

Soit $x \in]0, \frac{2}{3}[$, montrer qu'il existe $n \in \mathbb{N}$ tel que $\{nx\} \in [\frac{1}{3}, \frac{2}{3}[$.

Solution. (SABIR Ilyass)

Soit $x \in]0, \frac{2}{3}[$. On sait que pour tout $b \in \mathbb{N}$ tel que $b \geq 2$, il existe une suite $(a_n)_{n\in\mathbb{N}}$ telle que :

$$\forall n \in \mathbb{N}^\star \quad a_n \in [\![0, b-1]\!]$$

et $(a_n)_{n\in\mathbb{N}}$ n'est pas stationnaire en 0.

On a également :

$$x = \sum_{k=1}^{+\infty} \frac{a_k}{b^k}$$

En particulier, il existe une suite $(a_n)_{n\in\mathbb{N}}$ d'éléments dans $\{0, 1, 2\}$, non stationnaire en 2 telle que :

$$x = \sum_{k=1}^{+\infty} \frac{a_k}{3^k}$$

Puisque $x \in]0, \frac{2}{3}[$, alors forcément $a_1 \in \{0, 1\}$, et la suite $(a_n)_{n\in\mathbb{N}}$ est non identiquement nulle.

Pour tout $n \in \mathbb{N}$, on a :

$$3^n x = \sum_{k=1}^{+\infty} \frac{a_k}{3^{k-n}} = \sum_{k=1}^{n} a_k 3^{n-k} + \sum_{k=n+1}^{+\infty} \frac{a_k}{3^{k-n}}$$

Avec $\sum_{k=1}^{n} a_k 3^{n-k} \in \mathbb{N}$, et $\sum_{k=n+1}^{+\infty} \frac{a_k}{3^{k-n}} \in [0, 1[$, alors pour tout $l \in \mathbb{N}$, on a :

$$\{3^l x\} = \sum_{k=l+1}^{+\infty} \frac{a_k}{3^{k-l}} = \sum_{k=1}^{+\infty} \frac{a_{k+l}}{3^k}$$

S'il existe $n_0 \in \mathbb{N}^\star$ tel que $a_{n_0} = 1$, alors on a :

$$\{3^{n_0-1} x\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{a_{k+n_0-1}}{3^k}$$

Par positivité, on a :

$$\{3^{n_0-1} x\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{a_{k+n_0-1}}{3^k} \geq \frac{1}{3}$$

D'autre part, puisque $(a_n)_{n\in\mathbb{N}}$ n'est pas stationnaire en 2, on a :

$$\{3^{n_0-1} x\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{a_{k+n_0-1}}{3^k} < \frac{1}{3} + 2\sum_{k=2}^{+\infty} \frac{1}{3^k} < \frac{2}{3}$$

Donc, on a bien :

$$\{3^{n_0-1} x\} \in \left[\frac{1}{3}, \frac{2}{3}\right[$$

Sinon, c'est-à-dire, si la suite $(a_n)_{n\in\mathbb{N}}$ prend des valeurs seulement dans $\{0, 2\}$, par la non-stationnarité de $(a_n)_{n\in\mathbb{N}}$ en 2, il existe $r_0 \geq 3$ tel que $a_{r_0} = 0$. On a alors (facile à vérifier !) :

$$\{2\times 3^{r_0-1} x\} = 2\times\sum_{k=1}^{+\infty} \frac{a_{k+r_0-1}}{3^k} = \frac{4}{3^2} + 2\times\sum_{k=3}^{+\infty} \frac{a_{k+r_0-1}}{3^k} = \frac{1}{3} + \frac{1}{3^2} + 2\times\sum_{k=3}^{+\infty} \frac{a_{k+r_0-1}}{3^k}$$

Avec :

$$\frac{1}{3^2} + 2 \times \sum_{k=3}^{+\infty} \frac{a_{k+r_0-1}}{3^k} \leq \frac{2}{3^2}$$

Par l'unicité de la décomposition dans la base de 3, il existe une suite $(a'_n)_{n\in\mathbb{N}}$ à valeurs dans $\{0, 1, 2\}$ telle que :

$$\{2 \times 3^{r_0-1} x\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{a'_{k+r_0-1}}{3^k}$$

En conclusion, dans tous les cas, il existe $n \in \mathbb{N}$, tel qu'il existe une suite $(c_n)_{n\in\mathbb{N}}$ d'éléments dans $\{0,1,2\}$, non stationnaire en 2 telle que :

$$\{nx\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{c_k}{3^k}$$

Par positivité, on a :

$$\{nx\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{c_k}{3^k} \geq \frac{1}{3}$$

Et par non stationnarité en 2, on a :

$$\{nx\} = \frac{1}{3} + \sum_{k=2}^{+\infty} \frac{c_k}{3^k} < \frac{1}{3} + 2 \times \frac{1}{3^2} \frac{1}{1-\frac{1}{3}} = \frac{2}{3}$$

On en déduit que :

$$\{nx\} \in [\frac{1}{3}, \frac{2}{3}[$$

D'où le résultat.

✠✠✠✠✠✠✠

La caractérisation des boules unités fermées en dimension finie fait appel à des propriétés géométriques et topologiques fondamentales. Cet exercice établit un pont élégant entre la théorie des espaces normés et les propriétés géométriques des ensembles convexes.

Exercice 18.

Soit E un espace vectoriel de dimension finie muni de sa topologie d'espace vectoriel, et B une partie de E. Montrer l'équivalence :
il existe une norme N sur E telle que B est la boule unité fermée de (E,N) si, et seulement si, B est convexe, compacte, symétrique par rapport à l'origine, et d'intérieur non vide.

Solution. (SABIR Ilyass)

$\Longrightarrow$) Supposons qu'il existe une norme N sur E telle que B est la boule fermée unité de (E,N).

Alors, B est convexe. En effet, pour tout $\lambda \in [0,1]$ et pour tout $x, y \in B$, on a :

$$N((1-\lambda)x + \lambda y) \leq (1-\lambda)N(x) + \lambda N(y) \leq 1$$

Ainsi, $(1-\lambda)x + \lambda y \in B$, d'où B est convexe.

B est compacte, car elle est fermée et bornée (en dimension finie).

De plus, pour tout $x \in B$, on a $N(-x) = N(x) \leq 1$, donc $-x \in B$. D'où B est symétrique par rapport à 0.

Il reste à montrer que B est d'intérieur non vide. En effet, pour $x \neq 0$, on a $\frac{1}{2N(x)}x \in B^\circ$. Donc B est d'intérieur non vide.

$\Longleftarrow$) Supposons maintenant que B est convexe, compacte, symétrique par rapport à l'origine, et d'intérieur non vide, et montrons qu'il existe une norme N sur E telle que B est la boule unité fermée de (E, N).

Pour cela, l'idée est d'utiliser l'homogénéité. Pour x vecteur non nul de E, posons :

$$T_x = \{\lambda > 0 \mid \frac{x}{\lambda} \in B\}$$

Montrons d'abord que cet ensemble est non vide. En effet, l'origine est forcément un point intérieur à B, car comme B est d'intérieur non vide, on peut trouver $y \in B$ et $r > 0$, tel que $B(y, r) \subset B$.

Par symétrie par rapport à l'origine, on a également $B(-y, r) \subset B$. Par convexité, il en découle que $B(0, r) \in B$.

Ainsi, comme B est convexe, et contient l'origine, si $\lambda \in T_x$, alors $[\lambda, +\infty[\subset T_x$. Donc T_x est un intervalle non majoré de $\mathbb{R}_+^*$.

Comme B est compacte, elle est bornée. Soit $M > 0$ tel que $\|a\| \leq M$ pour tout $a \in B$. (Pour une norme quelconque $\|\cdot\|$, puisque toutes les normes sont équivalentes en dimension finie). Si $\lambda \in T_x$, on a $\lambda \geq \frac{\|x\|}{M} > 0$. Posons alors :

$$N(x) = \inf T_x$$

On pose aussi $N(0) = 0$

On vient de prouver qu'il s'agit d'un réel strictement positif. Comme B est fermée, l'intervalle T_x est aussi fermé et il est donc égal à $[N(x), +\infty[$.

Il reste à montrer que N est une norme et que B en est la boule unité fermée.

L'application N est positive car pour tout $x \in E$ non nul, on a :

$$T_x \subset]0, +\infty[$$

Donc :

$$N(x) = \inf(T_x) \geq \inf(]0, +\infty[) = 0$$

Et :

$$N(0) = 0$$

De plus, d'après ce qui précède, on a pour tout $x \in E$ non nul :

$$\forall \lambda \in T_x, \lambda \geq \frac{\|x\|}{M}$$

Donc, pour tout $x \in E$ non nul, on a :

$$N(x) \geq \frac{\|x\|}{M} > 0$$

Donc l'axiome de séparation est vérifié.

Si $x \in E$ est non nul et si $\mu > 0$, on a pour tout $\lambda > 0$:

$$\lambda \in T_{\mu x} \iff \frac{\mu x}{\lambda} \in B \iff \frac{\mu}{\lambda} x \in B \iff \frac{\lambda}{\mu} \in T_x \iff \lambda \in \mu T_x$$

Donc :

$$T_{\mu x} = \frac{1}{\mu} T_x$$

Ainsi :

$$N(\mu x) = \inf T_{\mu x} = \inf \mu T_x = \mu \inf T_x = \mu N(x)$$

Par symétrie de B, on a pour tout $x \in E$ non nul $T_{-x} = T_x$, donc $N(-x) = N(x)$. Cela reste vrai pour $x = 0$. Donc N est homogène.

Il ne reste qu'à montrer que N vérifie l'inégalité triangulaire. Pour cela, on va montrer d'abord le lemme suivant :

Lemme 1.

Soit $\Phi : E \to \mathbb{R}_+$ vérifiant pour tout $x \in E$ et pour tout $\lambda \in \mathbb{R}$:

$$\Phi(x) = 0 \iff x = 0 \text{et } \Phi(\lambda x) = |\lambda| \Phi(x)$$

On a : Φ est une norme si, et seulement si, l'ensemble $\{x \in E, \Phi(x) \leq 1\}$ est convexe.

Preuve du lemme 1.

Si Φ est une norme, il est clair que B est convexe. En effet, si $(x, y) \in B^2$ et $t \in [0, 1]$, on a :

$$\Phi((1-t)x + ty) \leq (1-t)\Phi(x) + t\Phi(y) \leq (1-t) + t = 1$$

Donc :

$$(1-t)x + ty \in B$$

D'où B est convexe.

Réciproquement, supposons que B est convexe, considérons x et y dans E. On veut prouver que :

$$\Phi(x+y) \leq \Phi(x) + \Phi(y)$$

On peut supposer que x et y non nuls, sans quoi l'inégalité est triviale.

Par homogénéité, les vecteurs $\frac{x}{\Phi(x)}$ et $\frac{y}{\Phi(y)}$ sont dans B. Il en est donc de même de leur barycentre z affecté des masses positives $\Phi(x)$ et $\Phi(y)$. On a :

$$z = \frac{x+y}{\Phi(x)+\Phi(y)}$$

Le fait que $\Phi(z) \leq 1$ conduit à $\Phi(x+y) \leq \Phi(x) + \Phi(y)$.

D'où l'équivalence.

Pour tout $x \in E$, on a $N(x) \leq 1$ si, et seulement si, $1 \in T_x$, donc si, et seulement si, $x \in B$. Ainsi :

$$\{x \in E \mid N(x) \leq 1\} = B$$

Comme B est convexe, on en déduit d'après le lemme que N vérifie l'inégalité triangulaire.

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice étudie le rayon de convergence d'une série entière dont le terme général fait intervenir une fonction trigonométrique de la racine carrée de l'indice. La singularité de ce terme général nécessite une analyse fine du comportement asymptotique.

Exercice 19. (Généralisation d'un exercice posé à l'oral de l'ENS Cachan)

Soit n_0 un entier strictement positif tel que $\sqrt{n_0} \notin \mathbb{Q}$. Déterminer le rayon de convergence de

$$\sum_{n \geqslant 1} \frac{z^n}{\sin(\sqrt{n_0}\pi n)}$$

Solution. (SABIR Ilyass)

Notons $\alpha = \sqrt{n_0}$. L'irrationalité de α assure que pour tout $n \in \mathbb{N}^*$,

$$\sin(\alpha\pi n) \neq 0$$

Pour $z = 1$, la série $\sum_{n\geqslant 1} \frac{1}{\sin(\alpha\pi n)}$ diverge, puisque pour tout $n \in \mathbb{N}^*$

$$|\sin(\alpha\pi n)| \leq 1$$

Donc, le rayon de convergence R vérifie $R \leq 1$.

Pour obtenir une minoration de R, on va majorer $\frac{1}{\sin(\alpha\pi n)}$, donc minorer $\sin(\alpha\pi n)$.

On note pour tout $n \in \mathbb{N}^*$

$$A_n = \{r \in \mathbb{N} : r \leq nd + \frac{1}{2}\}$$

Pour tout $n \in \mathbb{N}^*$, A_n est une partie non vide de $\mathbb{N}$ (puisque $0 \in A_n$) et majorée, donc A_n admet un plus grand élément. Notons $P_n = \max A_n$

On a donc, pour tout $n \in \mathbb{N}^*$,

$$P_n \leqslant n\alpha + \frac{1}{2} \text{ and } P_n + 1 > n\alpha + \frac{1}{2}$$

Ainsi,

$$P_n - \frac{1}{2} \leqslant n\alpha < P_n + \frac{1}{2}$$

Posons pour tout $n \in \mathbb{N}^*$,

$$\varepsilon_n = n\alpha - P_n \in \left[-\frac{1}{2}, \frac{1}{2}\right[$$

Par suite, pour tout $n \in \mathbb{N}^*$,

$$\sin(\alpha\pi n) \quad = \quad \sin(\pi\varepsilon_n)$$

Avec la fonction sin est concave sur $[0, \frac{\pi}{2}]$, donc pour tout $x \in [0, \frac{\pi}{2}]$,

$$\sin(x) \geq \frac{2}{\pi}x$$

Ainsi, pour tout $x \in [-\frac{\pi}{2}, \frac{\pi}{2}]$,

$$|\sin(x)| \geqslant \frac{2}{\pi}|x|$$

Par conséquent, pour tout $n \in \mathbb{N}^*$,

Ce dernier terme est en $O(n)$. Il en résulte que pour tout nombre complexe z vérifiant $|z| < 1$, la série $\sum_{n\geqslant 1} \frac{z^n}{\sin(d\pi n)}$

converge, d'où $R = 1$.

✠✠✠✠✠✠✠

Cet exercice traite d'un déterminant de Vandermonde généralisé faisant intervenir des polynômes. On cherche à calculer ce déterminant en exploitant les propriétés des déterminants et la structure particulière des polynômes P_k.

Exercice 20. (Classique niveau de l'X - Mines-Ponts)

Soit $n \geq 2$ un entier. Pour tout $k \in [\![1, n-1]\!]$, on considère un polynôme

$$P_k = X^k + a_{k,1}X^{k-1} + \cdots + a_{k,k} \in \mathbb{R}[X]$$

si $x_1, \ldots, x_n \in \mathbb{R}$. Calculer le déterminant

$$\Delta = \begin{vmatrix} 1 & P_1(x_1) & \cdots & P_{n-1}(x_1) \\ 1 & P_1(x_2) & \cdots & P_{n-1}(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ 1 & P_1(x_n) & \cdots & P_{n-1}(x_n) \end{vmatrix}$$

Solution. (SABIR Ilyass)

On a pour tout $k \in [\![1, n-1]\!]$, $\deg P_k = k$, donc pour tout $k \in [\![1, n-1]\!]$ la famille $(1, P_1, \cdots, P_k)$ est libre et de cardinal égal à la dimension de $\mathbb{R}_k[X]$ dans base de $\mathbb{R}[X]$.

Or, pour tout $k \in [\![1, n-1]\!]$

$$\sum_{j=0}^{k-1} a_{k,k-j}X^j \in \mathbb{R}_{k-1}[X]$$

donc il existe $\beta_{k,0}, \cdots, \beta_{k,k-1} \in \mathbb{R}$ tel que

$$\sum_{j=0}^{k-1} a_{k,k-j}X^j = \beta_{k,0} + \sum_{j=1}^{k-1} \beta_{k,j}P_j$$

(Avec la convention $\sum_{j=1}^{k-1} \beta_{k,j} P_j = 0$ si $k = 1$)
Pour tout $k \in [\![1, n-1]\!]$

$$L_{n+k} \leftarrow L_{n-k} - \sum_{j=0}^{n-k-1} \beta_{n-k,j} L_j$$

On obtient finalement

$$\Delta = \begin{vmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i)$$

✠✠✠✠✠✠✠

Cet exercice traite d'une suite dont la somme des puissances paires converge vers 1. Cette condition particulière de convergence va nous permettre d'étudier le comportement asymptotique des termes de la suite à l'aide des propriétés des séries convergentes.

Exercice 21.

On considère une suite $(a_n)_{n \in \mathbb{N}^*}$ de nombre réels telle que :

$$\lim_{n \to +\infty} \sum_{k=0}^{n} a_k^{2\beta} = 1, \text{où } \beta \in \mathbb{N}^*$$

Déterminer un équivalent de a_n.

Solution. (SABIR Ilyass)

Posons

$$S_n = \sum_{k=0}^{n} a_k^{2\beta}$$

Si la série de terme général $a_n^{2\beta}$ converge, alors S_n tend vers une limite finie lorsque n tend vers $+\infty$, et $\lim\limits_{n \to +\infty} a_n = 0$.

On ne peut donc avoir $\lim\limits_{n \to +\infty} a_n S_n = 1$. Puisque la série de terme général $a_n^{2\beta} \geqslant 0$ ne converge pas, on a $\lim\limits_{n \to +\infty} S_n = +\infty$

Comme pour tout $n \geq 1$, $a_n^{2\beta} = S_n - S_{n-1}$. L'hypothèse s'écrit :

$$S_n - S_{n-1} \underset{n\to+\infty}{\sim} \frac{1}{S_n^{2\beta}} \quad (S_n > 0 \text{pour } n \text{assez grand})$$

On a alors :

$$\begin{aligned} S_n^{2\beta+1} - S_{n-1}^{2\beta+1} &= (S_n - S_{n-1}) \sum_{j=0}^{2\beta} S_n^j S_{n-1}^{2p-j} \\ &\underset{+\infty}{\sim} \frac{1}{S_n^{2\beta}} \sum_{j=0}^{2\beta} S_n^j S_{n-1}^{2p-j} \\ &= \sum_{j=0}^{2\beta} \left(\frac{S_{n-1}}{S_n}\right)^{2\beta-j} \end{aligned}$$

Or, $1 - \frac{S_{n-1}}{S_n} \underset{+\infty}{\sim} \frac{1}{S_n^{2\beta+1}} \underset{n\to+\infty}{\to} 0 \quad (\text{car } S_n \underset{n\to+\infty}{\to} +\infty)$
alors $S_n \sim S_{n-1}$, ainsi

$$\sum_{j=0}^{2\beta} \left(\frac{S_{n-1}}{S_n}\right)^{2\beta-j} \underset{n\to+\infty}{\to} 2\beta + 1$$

d'où

$$S_n^{2\beta+1} - S_{n-1}^{2\beta+1} \underset{+\infty}{\sim} 2\beta + 1$$

Via le théorème de Césaro, on a :

$$\begin{aligned} S_n^{2\beta+1} &= \sum_{k=1}^{n} (S_k^{2\beta+1} - S_{k-1}^{2\beta+1}) \\ &\underset{n\to+\infty}{\sim} (2\beta+1)n \end{aligned}$$

Par suite,

$$S_n \underset{n\to+\infty}{\sim} ((2\beta+1)n)^{\frac{1}{2\beta+1}}$$

On en déduit finalement :

$$a_n \underset{n\to+\infty}{\sim} \frac{1}{((2\beta+1)n)^{\frac{1}{2\beta+1}}}$$

✠✠✠✠✠✠✠

On considère un polynôme unitaire $P \in \mathbb{Z}[X]$ qui se décompose en produit de deux polynômes Q et R dans $\mathbb{Q}[X]$, avec Q également unitaire. L'objectif

est de montrer que, dans ce cas, Q et R appartiennent nécessairement à $\mathbb{Z}[X]$.

Exercice 22.

Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire, et $Q, R \in \mathbb{Q}[X]$, avec Q unitaire, et $P = Q \cdot R$.
Montrer que $Q, R \in \mathbb{Z}[X]$.

Solution. (SABIR Ilyass)

On définit l'application contenu d'un polynôme de $\mathbb{Z}[X]$ par :
Pour tout $P := \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$,

$$c(P) = \text{pgcd}(a_1, a_2, \ldots, a_n)$$

Un résultat classique stipule que pour tout $P, Q \in \mathbb{Z}[X]$,

$$c(PQ) = c(P)c(Q)$$

Puisque $P = Q.R$, quitte à multiplier par un dénominateur commun des coefficients de Q (resp. de R), on peut trouver $a, b \in \mathbb{N}^*$ tels que $aQ, bR \in \mathbb{Z}[X]$.

On note alors

$$\hat{Q} = aQ \text{ and } \hat{R} = bR$$

On a donc,

$$P = \frac{1}{a.b}\hat{Q}\hat{R}$$

Comme P et Q sont unitaires, le coefficient dominant de $\hat{Q}$ est a (resp. le coefficient dominant de $\hat{R}$ est b).

En particulier, $c(\hat{Q})$ divise a et $c(\hat{R})$ divise b.

De l'égalité

$$abP = \hat{Q}\hat{R}$$

On déduit que :

$$ab = c(abP) = c(\hat{Q}\hat{R})$$

Finalement, on obtient

$$c(\hat{Q}) = a \text{ and } c(\hat{R}) = b$$

Ainsi, $Q = \frac{\hat{Q}}{c(\hat{Q})} \in \mathbb{Z}[X]$ et $R = \frac{\hat{R}}{c(\hat{R})} \in \mathbb{Z}[X]$.

Remarque.

L'hypothèse que Q est unitaire est essentielle. En effet, on peut trouver $P, Q \in \mathbb{Z}[X]$ tels que $P.Q \in \mathbb{Z}[X]$ sans que $P \in \mathbb{Z}[X]$ ou $Q \in \mathbb{Z}[X]$.

Par exemple :

$$(X+1)^2 = (2X+2)\left(\frac{1}{2}X + \frac{1}{2}\right)$$

De même, l'hypothèse que P est unitaire est essentielle, ce qui est clairement visible de la démonstration effectuée.

✠✠✠✠✠✠✠

Cet exercice explore une propriété des polynômes scindés à racines simples dans $\mathbb{R}$, montrant qu'ils ne peuvent pas avoir deux coefficients consécutifs nuls. À travers un raisonnement par l'absurde et deux lemmes, on démontre que les dérivées successives de ces polynômes conservent également cette structure. Une généralisation est aussi proposée.

Exercice 23. (Oral l'X 2007)

Soit $P \in \mathbb{R}[X]$, scindé dans $\mathbb{R}$, et à racines simples.

Montrer que P ne peut pas avoir deux coefficients consécutifs nuls.

Solution. (SABIR Ilyass)

Soit $P \in \mathbb{R}[X]$. Tout d'abord, Montrons le lemme classique suivant :

Lemme 1.

Soit $P \in \mathbb{R}[X]$, si P est scindé sur $\mathbb{R}$ à racines simples, alors P' est également scindé sur $\mathbb{R}$ à racines simples.

Preuve du lemme 1.

Notons

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

Avec $\alpha_1, ..., \alpha_r$ des réels deux à deux distincts (où $r = \deg(P)$), et $\mu \in \mathbb{R}$.

Or, pour tout $i \in [\![1, r]\!]$, $P(\alpha_i) = 0$, et P est dérivable sur $\mathbb{R}$.

D'après le théorème de Rolle, il existe $\beta_i \in]\alpha_i, \alpha_{i+1}[$, tel que

$$P'(\beta_i) = 0$$

avec $\alpha_1 < \beta_1 < \alpha_2 < ... < \alpha_{n-1} < \beta_{r-1} < \alpha_r$. Donc P' admet $\beta_1, ..., \beta_{r-1}$ racines deux à deux distinctes, avec $\deg P' = r - 1$.

On en déduit que P' est scindé à racines simples sur $\mathbb{R}$.

Lemme 2.

Soit $P \in \mathbb{R}[X]$ de degré $n \geq 1$, scindé sur $\mathbb{R}$ à racines simples, alors pour tout $i \in [\![0, n-1]\!]$, $P^{(i)}$ est scindé sur $\mathbb{R}$ à racines simples.

Preuve du lemme 2.

Par l'absurde, supposons que P a deux coefficients consécutifs nuls, On considère alors l'ensemble

$$\mathcal{A} = \{i \in [\![0, r]\!] | a_i = a_{i+1} = 0\}$$

qui est non vide (où $r = \deg P$ et $P = \sum_{i=0}^{r} a_i X^i$).

L'ensemble $\mathcal{A}$ est une partie non vide de $\mathbb{N}$, donc $\mathcal{A}$ admet un plus petit élément, que l'on note

$$n_0 = \min \mathcal{A}$$

On a :

$$\begin{aligned} P^{(n_0)} &= \sum_{i=n_0}^{r} \frac{i!}{(i-n_0)!} a_i X^{i-n_0} \\ &= X^2 \sum_{i=n_0+2}^{r} \frac{i!}{(i-n_0)!} a_i X^{i-n_0-2} \quad (\text{car } a_{n_0} = a_{n_0+1} = 0) \end{aligned}$$

Ainsi, 0 est une racine double de $P^{(n_0)}$, ce qui est absurde (d'après le lemme 2).

D'où le résultat.

Remarque.

Il existe plusieurs polynômes scindés sur $\mathbb{R}$ à racines simples et ayant deux coefficients consécutifs égaux. Par exemple :

$$P = X^2 - X - 1$$

scindé sur $\mathbb{R}$ à racines simples.

On peut de plus généraliser le résultat démontré dans cet exercice.

Généralisation :

Soit $P \in \mathbb{R}[X]$, scindé sur $\mathbb{R}$, tel que pour tout $r \in \mathbb{N}$ l'ordre de multiplicité des racines de P est au plus r. Alors P ne peut pas avoir $(r+1)$ coefficients consécutifs nuls.

La démonstration de ce résultat est presque la même que celle que nous avons faite. En particulier, si l'on note $\alpha_1, ..., \alpha_r$ les racines de P et pour tout $i \in [\![1, r]\!]$ $m(\alpha_i)$ désigne l'ordre de multiplicité de α_i.

Comme chaque α_i est une racine de P, alors P ne peut pas avoir R coefficients consécutifs nuls, avec

$$R = \max_{i=1}^{r} m(\alpha_i)$$

✠✠✠✠✠✠✠

Dans cet exercice, nous nous intéressons à une propriété remarquable concernant la réunion de sous-espaces vectoriels. Plus précisément, nous allons voir que si un nombre fini de sous-espaces vectoriels recouvre entièrement l'espace $\mathbb{R}^n$, alors l'un d'entre eux doit nécessairement être égal à l'espace tout entier. Cette propriété, bien que surprenante à première vue, s'avère être une conséquence des caractéristiques fondamentales des sous-espaces vectoriels.

Exercice 24. (Oral de l'X 2016)

Soient $V_1, \ldots, V_p$ des sous-espaces de $\mathbb{R}^n$ dont la réunion est égale à $\mathbb{R}^n$. Montrons que l'un des V_i est égal à $\mathbb{R}^n$.

Solution. (SABIR Ilyass)

C'est un exercice classique, déjà posé à l'oral de l'ENS dans une version plus forte.

Le résultat est valable pour tout K-espace vectoriel de dimension finie, où K est un corps infini.

Montrons le résultat suivant :

Soit K un corps infini, E un K-espace vectoriel de dimension finie. Alors, il n'existe aucune famille finie $(V_i)_{1\leqslant i\leqslant n}$ de sous-espaces vectoriels stricts de E telle que :

$$E = \bigcup_{i=1}^{n} V_i$$

Raisonnons par l'absurde et supposons qu'il existe une famille $(V_i)_{1\leqslant i\leqslant n}$ de sous-espaces vectoriels stricts de E telle que

$$E = \bigcup_{i=1}^{n} V_i$$

Quitte à retirer un certain nombre de sous-espaces vectoriels, nous pouvons supposer que la famille $(V_i)_{1\leqslant i\leqslant n}$est minimale, c'est-à-dire qu'elle est telle que, pour tout $i \in [\![1, n]\!]$,

$$V_i \not\subset \bigcup_{\substack{j=1 \\ j\neq i}}^{n} V_j$$

Pour V_n par exemple, il existe $y \in V_n$ tel que $y \notin \bigcup_{i=1}^{n-1} V_i$ $(\star)$

D'autre part, $E = \bigcup_{i=1}^{n} V_i$, ce qui est évident puisque V_n est un sous-espace strict de E. Donc, il existe $x \in \bigcup_{i=1}^{n-1} V_i$ et $x \notin V_n$.

Pour tout $\lambda \in K$, on a $x + \lambda y \in E$. Le vecteur $x + \lambda y \notin V_n$, donc

$$x + \lambda y \in \bigcup_{i=1}^{n-1} V_i$$

Ainsi, il existe $i_\lambda \in [\![1, n-1]\!]$ tel que $x + \lambda y \in V_{i_\lambda}$.

Considérons l'application

$$\varphi : \begin{cases} K \to [\![1, n-1]\!] \\ \lambda \mapsto i_\lambda \end{cases}$$

Soient $\lambda, \beta \in K$ tels que $\varphi(\lambda) = \varphi(\beta)$. On a alors $x + \lambda y \in V_{\varphi(\lambda)}$ et $x + \beta y \in V_{\varphi(\beta)} = V_{\varphi(\lambda)}$

Comme $V_{\varphi(\lambda)}$ est un espace vectoriel, alors

$$(\lambda - \beta)y \in V_{\varphi(\lambda)}$$

si $\lambda \neq \beta$ alors $y \in V_{\varphi(\lambda)} \subset \bigcup_{i=1}^{n-1} V_i$, ce qui est absurde en vertu de $(\star)$.

Donc $\lambda = \beta$, et par suite φ est injective. Cette conclusion contredit le fait que K est infini alors que $[\![1, n-1]\!]$ est fini.

✠✠✠✠✠✠✠

Cet exercice explore des propriétés géométriques des racines d'un polynôme et de sa dérivée dans le plan complexe. On étudie notamment la relation entre les racines d'un polynôme et celles de sa dérivée à travers le concept d'enveloppe convexe.

Exercice 25. (Oral l'X 2007)

Soit $P \in \mathbb{C}[X]$

a. Montrer que tout racine de P' est dans l'enveloppe convexe des racines de P.

b. Soit K un convexe fermé de $\mathbb{C}$. On note Ω l'ensemble des complexes w tels que $P^{-1}(\{w\}) \subset K$. Montrer que Ω est convexe.

Solution. (SABIR Ilyass)

a. Cette question est classique, et utilisée pour montrer plusieurs résultats importants. Ce résultat est connu sous le nom de théorème de Lucas.

Soit $z \in \mathbb{C}$ une racine de P'.

Si z est une racine de P, c'est terminé ! Sinon, la clôture de $\mathbb{C}$ permet d'écrire :

$$P = c\prod_{i=1}^{n}(X - z_i)$$

avec $z_1, \ldots, z_n \in \mathbb{C}$, on a donc

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{1}{X - z_i}$$

En particulier,

$$\begin{aligned} 0 &= \frac{P'(z)}{P(z)} \\ &= \sum_{i=1}^{n} \frac{1}{z - z_i} \end{aligned}$$

En multipliant chaque terme de la somme par $\overline{z - z_i}$, on obtient :

$$\sum_{i=1}^{n} \frac{\overline{z - z_i}}{|z - z_i|^2} = 0$$

En conjuguant cette égalité, on obtient :

$$z = \sum_{i=1}^{n} \frac{z_i}{|z - z_i|^2} \cdot \frac{1}{\sum_{i=1}^{n} \frac{1}{|z - z_i|^2}}$$

En posant pour tout $i \in [\![1, n]\!]$,

$$\lambda_i = \frac{1}{|z - z_i|^2} \times \frac{1}{\sum_{i=1}^{n} \frac{1}{|z - z_i|^2}}$$

On obtient donc $\sum_{i=1}^{n} \lambda_i = 1$, et

$$z = \sum_{i=1}^{n} \lambda_i z_i$$

Ce qui montre que z est dans l'enveloppe convexe des z_i.

b. Soient $u, v \in \Omega$. Montrons que pour tout $\lambda \in [0, 1]$ $\lambda\mu + (1 - \lambda)\nu \in \Omega$.
C'est-à-dire que pour tout z tel que $P(z) = \lambda u + (1 - \lambda)v$ est dans K.

Supposons d'abord $\lambda \in \mathbb{Q}$. On peut donc écrire $\lambda = \frac{n}{n+m}$ avec $n, m \geq 0$. Il s'agit de montrer que si $f(z) = \frac{mu+nv}{n+m}$ avec $z \in K$.

Considérons le polynôme :

$$R = (P - u)^n (P - v)^m$$

On note $\mathcal{Z}$ l'ensemble des racines de R.

On a donc, les racines de R sont soit racines de $P - u$ ou $P - v$, donc un élement de K.

Ainsi $\mathcal{Z} \subset K$. Or

$$R' = P'(P - u)^{n-1}(P - v)^{m-1}(n(P - v) + m(P - v))$$

D'après la question a, les racines de R' sont dans l'enveloppe convexe de $\mathcal{Z}$ notée Conv $\mathcal{Z}$.

En particulier, pour tout z tel que $P(z) = \frac{mu+nv}{n+m}$ est une racine de R', donc est dans Conv $\mathcal{Z}$, qui est inclus dans K par convexité de K.

Étudions à présent le cas général, soit $\lambda \in [0,1]$ et $(\lambda_k)_{k\in\mathbb{N}}$ une suite de rationnels de $[0,1]$ convergeant vers λ. Posons :

$$P(X) = (\lambda_k u + (1-\lambda_k)v) = c\prod_{i=1}^{n}(z - z_{i,k})$$

où $P(z) = \lambda u + (1-\lambda)v$, on a donc :

$$(\lambda - \lambda_k)(\mu - \nu) = c\prod_{i=1}^{n}(z - z_{i,k})$$

où les $z_{i,k}$ sont dans K, d'après ce qui précède.

Il en résulte que

$$\prod_{i=1}^{n}(z - z_{i,k}) \xrightarrow[k\to+\infty]{} 0$$

pour tout $\varepsilon > 0$,cil existe $k \in \mathbb{N}$ tel que

$$\prod_{i=1}^{n}|z - z_{i,k}| \leq \varepsilon^{\deg P} = \varepsilon^n$$

Par conséquent, il existe un indice j tel que $|z - z_{j,k}| \leq \varepsilon$. Ainsi z est adhérent à K. Donc $z \in K$.

Remarques.

1. Le théorème de Lucas (partie a) est un résultat fondamental en analyse complexe. Il a de nombreuses applications, notamment dans l'étude de la distribution des zéros des polynômes.

2. La partie b de cet exercice est une généralisation intéressante du théorème de Lucas. Elle montre que la convexité est préservée sous certaines transformations polynomiales.

3. Ces résultats peuvent être étendus à des classes plus larges de fonctions analytiques, au-delà des simples polynômes.

Exercices complémentaires.

1. Montrer que si toutes les racines d'un polynôme P sont réelles, alors toutes les racines de P' sont également réelles.

2. Généraliser le théorème de Lucas aux dérivées d'ordre supérieur : montrer que les racines de $P^{(k)}$ sont dans l'enveloppe convexe des racines de P pour tout $k \geq 1$.

✠✠✠✠✠✠✠

Cet exercice étudie les propriétés de divisibilité d'un polynôme à coefficients entiers admettant une racine rationnelle. On cherche à établir des critères de divisibilité dans $\mathbb{Z}[X]$ et à analyser l'impact de la multiplicité d'une racine sur les coefficients du polynôme.

Exercice 26.

Soit $P = \sum_{k=0}^{n} a_k X^k$ un polynôme de degré n à à coefficients dans $\mathbb{Z}$, et soit $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p \wedge q = 1$. On suppose que $\frac{p}{q}$ est racine de P.
Montrer que $qX - p$ divise P dans $\mathbb{Z}[X]$.

Solution. (SABIR Ilyass)

Soit c l'application définie pour tout $P := \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ par

$$c(P) = \text{pgcd}(a_0, a_1, \ldots, a_n)$$

$c(P)$ est appelé le contenu du polynôme P.
On rappelle que pour tout $P, Q \in \mathbb{Z}[X]$,

$$c(P \cdot Q) = c(P) \cdot c(Q)$$

Si $\frac{p}{q}$ est une racine de P, alors il existe $Q \in \mathbb{Q}[X]$ tel que

$$P = \left(X - \frac{p}{q}\right) Q$$

Quitte à prendre un dénominateur commun des coefficients de Q on peut trouver $R \in \mathbb{Z}[X]$, $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $a \wedge b = 1$ et

$$P = \frac{a}{bq}(qX - p)R$$

On a alors

$$bqP = a(qX - p)R$$

En conséquence

$$c(bqP) = c(a(qX - p)R)$$

avec $P \in \mathbb{Z}[X]$, alors

$$c(bqP) = bq \cdot c(P)$$

et $c(qX-p)=1$ et $R\in\mathbb{Z}[X]$
alors

$$bq\cdot c(P)=a\cdot c(R)$$

On en déduit que $\frac{a}{bq}=\frac{c(P)}{c(R)}$,
D'où $P=c(P)(qX-q)\frac{R}{c(R)}$ avec $\frac{R}{c(R)}\in\mathbb{Z}[X]$
d'où le résultat.

✠✠✠✠✠✠✠

Dans cet exercice, nous étudions une suite définie par un terme initial $u_1>0$ et une relation de récurrence impliquant les termes successifs. Nous chercherons à déterminer le comportement asymptotique de cette suite, notamment sa limite lorsque n tend vers l'infini. Les techniques employées incluront la transformation logarithmique pour simplifier la récurrence et l'analyse des termes par la méthode de variation de la constante.

Exercice 27. (Oral l'X 2007)

Étudier la suite définie par son premier terme $u_1>0$ et la relation de récurrence

$$u_{n+1}=\frac{n+1}{2n}\sqrt{u_n}$$

Solution. (SABIR Ilyass)

Soit $(u_n)_{n\geq 1}$ une suite vérifiant

$$u_{n+1}=\frac{n+1}{2n}\sqrt{u_n},\text{pour tout}\,n\in\mathbb{N}^*\text{ and }u_1>0$$

Par construction, les termes de $(u_n)_{n\geq 1}$ sont tous strictement positifs.
Posons

$$(\beta_n)_{n\geq 1}:=(\ln u_n)_{n\geq 1}$$

On a, pour tout $n\geqslant 1$

$$\beta_{n+1}-\frac{1}{2}\beta_n=\ln\left(\frac{n+1}{2n}\right)$$

Il s'agit d'une relation de récurrence linéaire. Une suite vérifiant cette relation peut s'écrire comme la somme d'une suite vérifiant $\gamma_{n+1} - \frac{1}{2}\gamma_n = 0$, $\forall n \geq 1$, et une solution particulière.

Tout d'abord, une suite $(\gamma_n)_{n\geq 1}$ vérifiant pour tout $n \geq 1$ $\gamma_{n+1} - \frac{1}{2}\gamma_n = 0$, est une suite géométrique de raison $\frac{1}{2}$. Donc, pour tout $n \geq 1$

$$\gamma_n = \frac{\gamma_1}{2^{n-1}}$$

Cherchons une solution particulière, soit $(\Gamma_n)_{n\geq 1}$ une solution particulière. On s'inspire de la méthode de la variation de la constante pour les équations différentielles linéaires.

On pose, pour tout $n \geq 1$

$$(\sigma_n)_{n\geq 1} := (2^{n-1}\Gamma_n)_{n\geq 1}$$

On a pour tout $n \geqslant 1$

$$\Gamma_n = \frac{\sigma_n}{2^{n-1}}$$

Avec pour tout $n \geqslant 1$

$$\Gamma_{n+1} - \frac{1}{2}\Gamma_n = \ln\left(\frac{n+1}{2n}\right)$$

Donc, pour tout $n \geqslant 1$

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

Par suite, pour tout $n \geqslant 1$

$$\begin{aligned} \sigma_n &= \sum_{k=1}^{n-1} (\sigma_{k+1} - \sigma_k) + \sigma_1 \\ &= \sum_{k=1}^{n-1} 2^k \ln\left(\frac{k+1}{2k}\right) + \sigma_1 \end{aligned}$$

En prenant $\sigma_1 = 0$, on obtient, pour tout $n \geq 1$

$$\Gamma_n = \sum_{k=1}^{n-1} \frac{1}{2^{n-1-k}} \ln\left(\frac{k+1}{2k}\right)$$

Donc, pour tout $n \geq 1$

$$\beta_n = \frac{\gamma_1}{2^{n-1}} + \sum_{k=1}^{n-1} \frac{1}{2^{n-1-k}} \ln\left(\frac{k+1}{2k}\right)$$

avec γ_1 est une constante, déterminée par la donnée d'un terme de la suite $(\beta_n)_{n\geq 1}$

Or $\beta_1 = \ln u_1 = \gamma_1$

Finalement, pour tout $n \geq 1$,

$$\beta_n = \frac{\ln u_1}{2^{n-1}} + \sum_{k=1}^{n-1} \frac{1}{2^{n-1-k}} \ln\left(\frac{k+1}{2k}\right)$$

Par suite, pour tout $n \geq 1$

$$\begin{aligned} u_n &= \exp\left(\frac{\ln u_1}{2^{n-1}} + \sum_{k=1}^{n-1} \frac{1}{2^{n-1-k}} \ln\left(\frac{k+1}{2k}\right)\right) \\ &= u_1^{\frac{1}{2^{n-1}}} \prod_{k=1}^{n-1} \left(\frac{k+1}{2k}\right)^{\frac{1}{2^{n-1-k}}} \end{aligned}$$

$\rightarrow$ déterminons la limite de $(u_n)_{n\geq 1}$

Pour tout $n \geqslant 1$, on a

$$\begin{aligned} \ln(u_n) &= \beta_n \\ &= \frac{1}{2^{n-1}} \ln(u_1) + \frac{1}{2^{n-1}} \sum_{k=1}^{n-1} 2^k \ln\left(\frac{k+1}{2k}\right) \end{aligned}$$

Or, $\frac{1}{2^{n-1}} \ln(U_1) \xrightarrow[n\to\infty]{} 0$. De plus, pour tout $n \geq 1$

$$\frac{1}{2^{n-1}} \sum_{k=1}^{n-1} 2^k \ln\left(\frac{k+1}{2k}\right) = \frac{\sum_{k=1}^{n-1} 2^k \ln\left(\frac{k+1}{2k}\right)}{\sum_{k=1}^{n-1} 2^k} \cdot \frac{2^n - 2}{2^{n-1}}$$

La série $\sum\limits_{n\geq 0} 2^n$ diverge, donc on peut appliquer le théorème de Césaro (puisque $\ln\left(\frac{n+1}{2n}\right) \xrightarrow[n\to+\infty]{} \ln\left(\frac{1}{2}\right)$). Il s'ensuit que

$$\ln U_n \xrightarrow[n\to+\infty]{} 2\ln\left(\frac{1}{2}\right) = \ln\left(\frac{1}{4}\right)$$

Par suite,

$$U_n \xrightarrow[n\to+\infty]{} \frac{1}{4}$$

✠✠✠✠✠✠✠

Cet exercice explore l'existence d'un point fixe commun pour deux fonctions continues f et g sur $[0,1]$, en supposant que f est monotone et que $f \circ g = g \circ f$. Nous démontrerons qu'il existe un point $c \in [0,1]$ tel que $f(c) = g(c) = c$.

Exercice 28. (Oral ULM 2008)

Soient f et g deux fonctions continues sur $[0,1] \to [0,1]$ vérifiant $f \circ g = g \circ f$, on suppose que f est monotone, montrer qu'il existe $c \in [0,1]$ tel que

$$f(c) = g(c) = c$$

Solution. (SABIR Ilyass)

Pour prouver qu'il existe $c \in [0,1]$ tel que $f(c) = g(c) = c$, nous utiliserons les propriétés des fonctions continues et monotones, ainsi que la propriété de commutation $f \circ g = g \circ f$.

Étant donné que f est continue et monotone sur l'intervalle $[0,1]$, l'ensemble de ses points fixes,

$$\mathrm{Fix}(f) = \{x \in [0,1] \mid f(x) = x\},$$

est un intervalle fermé $[\alpha, \beta] \subseteq [0,1]$.

En effet, si $x_1, x_2 \in \mathrm{Fix}(f)$ avec $x_1 < x_2$, alors pour tout x entre x_1 et x_2, $f(x)$ sera compris entre $f(x_1)$ et $f(x_2)$, qui sont respectivement égaux à x_1 et x_2. Ainsi, $f(x) \geq x$ ou $f(x) \leq x$, selon que f est croissante ou décroissante. Cela garantit qu'il n'y a pas de sauts, donc $f(x) = x$ pour tous les $x \in [x_1, x_2]$.

Étant donné que $f \circ g = g \circ f$, pour tout $c \in \mathrm{Fix}(f)$, on a

$$f(g(c)) = g(f(c)) = g(c).$$

Cela implique $f(g(c)) = g(c)$, donc $g(c) \in \mathrm{Fix}(f)$. Par conséquent, g applique $\mathrm{Fix}(f)$ dans lui-même :

$$g : \mathrm{Fix}(f) \to \mathrm{Fix}(f).$$

Puisque $\mathrm{Fix}(f)$ est un intervalle fermé $[\alpha, \beta]$ et que g est continue, la restriction de g à $\mathrm{Fix}(f)$ est une fonction continue de $[\alpha, \beta]$ dans lui-même. Par le théorème du point fixe de Brouwer en dimension un (qui affirme que toute fonction continue d'un intervalle fermé dans lui-même a au moins un point fixe, [voir l'exercice 7 ULRS, lemme 1]), il existe un $c \in [\alpha, \beta]$ tel que :

$$g(c) = c.$$

Puisque $c \in \mathrm{Fix}(f)$, on a déjà $f(c) = c$. On a également $g(c) = c$. Par conséquent :

$$f(c) = c \quad \text{et} \quad g(c) = c.$$

✠✠✠✠✠✠✠

Cet exercice explore les propriétés des racines d'un polynôme P et de sa dérivée P', ainsi que les liens entre les racines multiples et le signe d'une expression associée à P et ses dérivées.

Exercice 29. (Oral de l'X 2016)

Soit $P \in \mathbb{R}[X]$ définie sur $\mathbb{R}$.

1. Montrer que toute racine multiple de P' est racine de P
2. Pour $x \in \mathbb{R}$, quel est le signe de $P(x)P''(x) - P'(x)^2$?

Solution. (SABIR Ilyass)

1. La première question est classique. Écrivons

$$P = a \prod_{i=1}^{r} (X - \alpha_i)^{n_i} \prod_{i=1}^{\ell} (X - \beta_i)$$

où $\alpha_1, \ldots, \alpha_r$ sont les racines multiples de P et $\beta_1, \ldots, \beta_\ell$ sont les racines simples de P. Les multiplicités $n_1, \ldots, n_r \geq 2$ représentent les ordres des

racines $\alpha_1, \dots, \alpha_r$ comme étant racines de P. ($\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_\ell$ sont deux à deux distincts)

On a, pour tout $i \in [\![1, r]\!]$,

$$P(\alpha_i) = P'(\alpha_i) = P''(\alpha_i) = \cdots = P^{(n_i-1)}(\alpha_i) = 0 \text{ and } P^{(n_i)}(\alpha_i) \neq 0$$

En particulier, pour tout $i \in [\![1, r]\!]$,

$$P'(\alpha_i) = (P')^{(1)}(\alpha_i) = \cdots = (P')^{(n_i-2)}(\alpha_i) = 0 \text{ and } (P')^{(n_i-1)}(\alpha_i) \neq 0$$

Cela montre que, pour tout $i \in [\![1, r]\!]$, α_i est une racine de P' de multiplicité $n_i - 1$.

En ordonnant $\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_\ell$ par ordre croissant, posons, pour tout $i \in [\![1, r + \ell]\!]$

$$\begin{cases} \lambda_1 = \min\{\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_\ell\} \\ \lambda_i = \min\{(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_\ell) \setminus \{\lambda_1, \dots, \lambda_{i-1}\}\}, \text{si } i \geqslant 2 \end{cases}$$

Ainsi, $\lambda_1, \dots, \lambda_{\ell+r}$ sont exactement les racines de P deux à deux distincts et $\lambda_1 < \lambda_2 < \cdots < \lambda_{\ell+r}$.

Pour tout $i \in [\![1, \ell + r - 1]\!]$, on a P est continue sur $[\lambda_i, \lambda_{i+1}]$ et dérivable sur $]\lambda_i, \lambda_{i+1}[$ avec

$$P(\lambda_i) = P(\lambda_{i+1})$$

Alors d'après le théorème de Rolle, il existe $c_i \in]\lambda_i, \lambda_{i+1}[$ tel que $P'(c_i) = 0$

Donc, on a pour tout $i \in [\![1, r]\!]$ α_i est une racine de P de multiplicité $n_i - 1$, et pour tout $i \in [\![1, r + \ell - 1]\!]$ c_i est une racine de P'.

Ainsi, il existe $Q \in \mathbb{R}[X]$ tel que

$$P' = aQ \prod_{i=1}^{r} (X - \alpha_i)^{n_i - 1} \prod_{i=1}^{\ell+r-1} (X - c_i)$$

Donc P' est scindé sur $\mathbb{R}$.

Concernant P' : une racine γ multiple de P' ne peut pas être un certain c_i puisque $c_1, \ldots, c_{l+r-1}$ sont des racines simples de P'. alors γ est une racine de P.

2- On reprend les notations de la question 1. La fonction $x \mapsto \frac{P'(x)}{P(x)}$ est dérivable sur $\mathbb{R} \setminus \{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r\}$, et on a

$$\frac{P'}{P} = \sum_{i=1}^{r} \frac{n_i}{x - \alpha_i} + \sum_{i=1}^{l} \frac{1}{x - \beta_i}$$

Donc,

$$\frac{P \cdot P'' - (P')^2}{P^2} = -\sum_{i=1}^{r} \frac{n_i}{(x - \alpha_i)^2} - \sum_{i=1}^{l} \frac{1}{(x - \beta_i)^2}$$

Par conséquent, pour tout $x \in \mathbb{R} \setminus \{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r\}$, on a

$$\frac{P(x)P''(x) - (P'(x))^2}{P^2(x)} = -\sum_{i=1}^{r} \frac{n_i}{(x - \alpha_i)^2} - \sum_{i=1}^{l} \frac{1}{(x - \beta_i)^2} < 0$$

Donc, pour tout $x \in \mathbb{R} \setminus \{\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r\}$,

$$P(x)P''(x) - (P'(x))^2 \leq 0$$

Par continuité de $x \mapsto P(x)P''(x) - (P'(x))^2$, on en déduit que, pour tout $x \in \mathbb{R}$

$$P(x)P''(x) - (P'(x))^2 \leq 0$$

Remarque.

À partir de la question 1,

$$P' \wedge P = \prod_{i=1}^{r} (X - \alpha_i)^{n_i - 1}$$

Donc,

$$\deg(P' \wedge P) = \sum_{i=1}^{r} (n_i - 1)$$

D'où

$$\begin{aligned} \deg P - \deg(P' \wedge P) &= l + \sum_{i=1}^{r} n_i - \sum_{i=1}^{r} (n_i - 1) \\ &= l + r \end{aligned}$$

Par conséquent, le nombre de racines distincts de P est $\deg P - \deg(P' \wedge P)$.

✠✠✠✠✠✠✠

La caractérisation des polynômes positifs sur $\mathbb{R}^+$ fait appel à des techniques de décomposition en sommes de carrés, distinctes du cas général sur $\mathbb{R}$ tout entier. Cet exercice propose d'établir une équivalence élégante adaptée au cas des réels positifs.

Exercice 30. (Oral de l'X 2016)

Soit $P \in \mathbb{R}[X]$. Montrer que P est positif sur $\mathbb{R}^+$, si et seulement s'il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + XB^2$.

Solution. (SABIR Ilyass)

Notons

$$\mathcal{H} = \{P \in \mathbb{R}[X] | \exists A, B \in \mathbb{R}[X] \text{ tels que } P = A^2 + XB^2\}$$

Montrons que $\mathcal{H}$ est stable par multiplication.
Soit $(P, Q) \in \mathcal{H}^2$. Il existe alors $A_1, B_1; A_2, B_2 \in \mathbb{R}[X]$ tels que :

$$P = A_1^2 + XB_1^2 \text{ and } Q = A_2^2 + XB_2^2$$

On a donc :

$$\begin{aligned} PQ &= (A_1^2 + XB_1^2)(A_2^2 + XB_2^2) \\ &= (A_1A_2)^2 + (XB_1B_2)^2 + X(A_1^2B_2^2 + A_2^2B_1^2) \\ &= (A_1A_2 - XB_1B_2)^2 + X(A_1B_2 + A_2B_1)^2 \end{aligned}$$

Ce qui montre que $PQ \in \mathcal{H}$.

Pour montrer que pour tout $P \in \mathbb{R}[X]$, P est positif sur $\mathbb{R}^+$ si et seulement s'il existe $A, B \in \mathbb{R}[X]$ tels que

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

Il suffit de montrer l'équivalence :
Pour tout $P \in \mathbb{R}[X]$ irréductible dans $\mathbb{R}[X]$,

P est positif sur $\mathbb{R}^+$ si, et seulement si, il existe $A, B \in \mathbb{R}[X]$ tels que $P = A^2 + XB^2$.

$\Leftarrow$) Notons tout d'abord que la réciproque est évidente.

$\Rightarrow$) Soit $P \in \mathbb{R}[X]$ irréductible dans $\mathbb{R}[X]$.

- **Si** $\deg P = 1$: écrivons $P = aX + b$ avec $(a, b) \in \mathbb{R}^* \times \mathbb{R}$

Puisque pour tout $x \geq 0$, on a $P(x) \geq 0$

D'où $P(0) = b \geq 0$ et $\lim\limits_{x \to +\infty} P(x) \geq 0$ donc $a \geq 0$

On a donc

$$P = (\sqrt{b})^2 + X(\sqrt{a})^2 \in \mathcal{H}$$

- **Si** $\deg P = 2$: écrivons $P = aX^2 + bX + c$ avec $(a, b, c) \in \mathbb{R}^* \times \mathbb{R} \times \mathbb{R}$ et $b^2 < 4ac$

Puisque pour tout $x \geq 0,\ P(x) \geq 0$

Alors $P(0) = c \geq 0$ et $\lim\limits_{x \to +\infty} P(x) \geq 0$ donc $a \geq 0$

On a $|b| < 2\sqrt{ac}$, alors

$$P = (\sqrt{a}X - \sqrt{c})^2 + (b + 2\sqrt{ac})X$$

avec $b + 2\sqrt{ac} \geq |b| + b \geqslant 0$

D'où

$$P = (\sqrt{a}X - \sqrt{c})^2 + X(\sqrt{b + 2\sqrt{ac}})^2 \in \mathcal{H}$$

On obtient ainsi le résultat souhaité !

✠✠✠✠✠✠✠

Cet exercice explore les conditions de positivité d'une suite réelle $(u_n)_{n \geq 0}$ à travers une forme linéaire associée aux polynômes. Il établit une équivalence entre des propriétés de positivité des polynômes et une inégalité bilinéaire sur les coefficients de la suite.

Exercice 31. (Oral de l'X 2016)

Soit $(u_n)_{n\geq 0}$ une suite réelle et ϕ_u l'unique forme linéaire dans $\mathbb{R}[X]$ telle que, pour tout $k \in \mathbb{N}$,

$$\phi_u(X^k) = u_k$$

Montrer l'équivalence entre :

1. $\forall P \in \mathbb{R}[X]\ P(\mathbb{R}) \subset \mathbb{R}^+ \Rightarrow \phi_u(P) \geq 0$
2. $\forall n \in \mathbb{N}\ \forall (x_0, \ldots, x_n) \in \mathbb{R}^{n+1} \sum\limits_{0\leq i,j\leq n} u_{i+j}x_ix_j \geq 0$

Solution. (SABIR Ilyass)

2) $\Rightarrow$ 1) Supposons que pour tout $n \in \mathbb{N}$, pour tout $(x_0, \ldots, x_n) \in \mathbb{R}^{n+1}$

$$\sum_{0\leq i,j\leq n} u_{i+j}x_ix_j \geq 0$$

Soit $P \in \mathbb{R}[X]$, en écrivant $P = \sum\limits_{i=0}^{n} a_iX^i$ où $n \in \mathbb{N}$ et $a_0, \ldots, a_n \in \mathbb{R}$
On a :

$$\begin{aligned}\sum_{0\leq i,j\leq n} u_{i+j}x_ix_j &= \sum_{0\leq i,j\leq n} \phi_u(X^{i+j})x_ix_j \\ &= \phi_u\Big(\sum_{0\leq i,j\leq n} x_ix_jX^{i+j}\Big) \\ &= \phi_u(P^2)\end{aligned}$$

Donc la condition (2) est équivalente à

$$\forall P \in \mathbb{R}[X] \quad \phi_u(P^2) \geq 0 \quad (*)$$

Montrons maintenant que :

$$\forall P \in \mathbb{R}[X], \quad P(\mathbb{R}) \subset \mathbb{R}^+ \Rightarrow \phi_u(P) \geq 0$$

Soit $P \in \mathbb{R}[X]$ tel que $P(\mathbb{R}) \subset \mathbb{R}^+$
- Si P admet une racine réelle, en écrivant

$$P = a\prod_{i=1}^{r}(X-\alpha_i)^{m_i}\prod_{i=1}^{\ell}(X^2-\lambda_iX+\beta_i)^{n_i}$$

où $(m_i, n_i, \alpha_i, \lambda_i, \beta_i) \in \mathbb{N} \times \mathbb{N} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$ pour tout i, avec $a > 0$ et $\lambda_i^2 < 4\beta_i$.

Les $\alpha_1, \ldots, \alpha_r$ sont les racines réelles de P.

On a alors $\lim\limits_{x\to\infty} P(x) \geq 0$, donc P est de degré pair.

Soit $i_0 \in [\![1, r]\!]$, on a

$$P \underset{x\to\alpha_{i_0}}{\sim} a(X-\alpha_{i_0})^{m_{i_0}} \prod_{\substack{i=1\\ i\neq i_0}}^{r} (\alpha_{i_0}-\alpha_i)^{m_i} \prod_{i=1}^{\ell} (\alpha_{i_0}^2 - \lambda_i\alpha_{i_0} + \beta_i)^{n_i}$$

Le signe de Pau voisinage de α_{i_0} est celui de $(X-\alpha_{i_0})^{m_{i_0}}$. En particulier, $(X-\alpha_{i_0})^{m_{i_0}}$ est positive au voisinage de α_{i_0}, donc m_{i_0} est pair. Cela est vrai pour tout $i_0 \in [\![1, r]\!]$.

Notons pour tout $i \in [\![1, r]\!]$

$$m_i = 2d_i$$

On a alors

$$P = a\prod_{i=1}^{r}(X-\alpha_i)^{2d_i} \prod_{i=1}^{\ell}(X^2 - \lambda_i X + \beta_i)^{n_i}$$

Notons

$$\mathcal{L} = \{P \in \mathbb{R}[X] | \exists (A, B) \in \mathbb{R}[X]^2 \,\text{tel que}\, P = A^2 + B^2\}$$

Pour tout $P, Q \in \mathcal{L}$, il existe $(A, B), (C, D) \in \mathbb{R}[X]^2$ tels que

$$P = A^2 + B^2 \text{ and } Q = C^2 + D^2$$

Ainsi, $\mathcal{L}$ est stable par produit.

Montrons que pour tout $a, b \in \mathbb{R}$ tels que $a^2 < 4b$, on a

$$X^2 + aX + b \in \mathcal{L}$$

Soit $(a, b) \in \mathbb{R}^2$, tel que $a^2 < 4b$, on a

$$\begin{aligned} X^2 + aX + b &= \left(X + \frac{a}{2}\right)^2 + b - \frac{a^2}{4} \\ &= \left(X + \frac{a}{2}\right)^2 + \left(\sqrt{b - \frac{a^2}{4}}\right)^2 \\ &\in \mathcal{L} \end{aligned}$$

En particulier, pour tout $i \in [\![1, l]\!]$, on a $X^2 - \lambda_i X + \beta_i \in \mathcal{L}$. Par stabilité par produit, on en déduit que

$$\prod_{i=1}^{\ell} (\alpha_{i_0}^2 - \lambda_i \alpha_{i_0} + \beta_i)^{n_i} \in \mathcal{L}$$

Donc, il existe $A, B \in \mathbb{R}[X]$ tels que

$$\prod_{i=1}^{\ell} (\alpha_{i_0}^2 - \lambda_i \alpha_{i_0} + \beta_i)^{n_i} = A^2 + B^2$$

Par suite,

$$\begin{aligned} P &= a \prod_{i=1}^{r} (X - \alpha_i)^{2d_i} (A^2 + B^2) \\ &\quad \left(\sqrt{a} \prod_{i=1}^{r} (X - \alpha_i)^{d_i} A \right)^2 + \left(\sqrt{a} \prod_{i=1}^{r} (X - \alpha_i)^{d_i} B \right)^2 \end{aligned}$$

Ainsi, par linéarité de ϕ_u :

$$\begin{aligned} \phi_u(P) &= a\phi_u((\prod_{i=1}^{r} (X - \alpha_i)^{\alpha_i} A)^2) + a\phi_u((\prod_{i=1}^{r} (X - \alpha_i)^{\alpha_i} B)^2) \\ &\geqslant 0 \end{aligned}$$

1) $\Rightarrow$ 2) Supposons que pour tout $P \in \mathbb{R}[X]$

$$P(\mathbb{R}) \subset \mathbb{R}^+ \Rightarrow \phi_u(P) \geq 0$$

Montrons que, pour tout $n \in \mathbb{N}$, pour tout $x_0, x_1, \ldots, x_n \in \mathbb{R}^{n+1}$

$$\sum_{0 \leq i,j \leq n} u_{i+j} x_i x_j \geq 0$$

Soient $n \in \mathbb{N}$ et $(x_0, \ldots, x_n) \in \mathbb{R}^{n+1}$. On a

$$\sum_{0 \leq i,j \leq n} u_{i+j} x_i x_j = \phi_u((\sum_{i=0}^{n} x_i X^i)^2)$$

Or, pour tout $x \in \mathbb{R}$,

$$(\sum_{i=0}^{n} x_i X^i)^2 \geq 0$$

Donc

$$\phi_u((\sum_{i=0}^{n} x_i X^i)^2) \geq 0$$

Ainsi,

$$\sum_{0\leq i,j\leq n} u_{i+j} x_i x_j \geq 0$$

D'où l'équivalence.

Remarque. Un exercice similaire a été posé à l'oral de l'X 2007 :

Soit $P \in \mathbb{R}[X]$, Montrer l'équivalence suivante :

$$\forall x \in \mathbb{R}, \quad P(x) \geqslant 0 \quad \Leftrightarrow \quad \exists (A,B) \in \mathbb{R}[X]^2 \quad P = A^2 + B^2$$

✠✠✠✠✠✠✠

L'étude des propriétés arithmétiques des sommes harmoniques révèle des résultats surprenants. Cet exercice combine la théorie des nombres et l'analyse pour établir une propriété remarquable concernant la divisibilité de ces sommes par des carrés de nombres premiers.

Exercice 32. (le théorème de Wolstenholme)

Pour tout $n \in \mathbb{N}^*$, on note :

$$\sum_{k=1}^{n-1} \frac{1}{k} = \frac{a_n}{b_n}, \text{avec } a_n, b_n \in \mathbb{N} \text{ tels que } a_n \wedge b_n = 1$$

Montrer que pour tout nombre premier $p \geqslant 5$, on a p^2 divise a_p.

Solution. (SABIR Ilyass)

Soit $p \geqslant 5$, un nombre premier. Dans $\mathbb{Z}/p\mathbb{Z}$, on a :

$$\begin{aligned}
\frac{2}{p}\sum_{k=1}^{p-1}\frac{1}{k} &= \frac{2}{p}\left(\sum_{k=1}^{(p-1)/2}\frac{1}{k}+\sum_{k=1+(p-1)/2}^{p-1}\frac{1}{k}\right)\\
&= \frac{2}{p}\sum_{k=1}^{(p-1)/2}\frac{1}{k}+\frac{1}{p-k}\\
&= 2\sum_{k=1}^{(p-1)/2}\frac{1}{k(p-k)}\\
&= -\sum_{k=1}^{p-1}\frac{1}{k^2}\\
&= -\sum_{k=1}^{p-1}k^2\\
&= -\frac{p(p-1)(2p-1)}{6}
\end{aligned}$$

Ainsi,

$$\sum_{k=1}^{p-1}\frac{1}{k} = -\frac{(p-1)(2p-1)}{12}p^2$$

D'où le résultat.

✠✠✠✠✠✠✠

Cet exercice porte sur l'inégalité de Hölder, utilisée pour comparer des sommes et produits de valeurs positives. Il s'agit de démontrer l'inégalité, d'étudier le cas d'égalité, puis d'appliquer cette inégalité à une propriété des produits augmentés.

Exercice 33. (Inégalité de Hölder)

Soient $m, n \in \mathbb{N}^*$, et soient $(a_{2,1}, \ldots, a_{2,n})$, $(a_{1,1}, \ldots, a_{1,n}), \ldots$ et $(a_{m,1}, \ldots, a_{m,n})$ des réels positifs.

1. Montrer que :

$$\prod_{i=1}^{m}\left(\sum_{j=1}^{n} a_{i,j}\right) \geqslant \left(\sum_{j=1}^{n} \sqrt[m]{\prod_{i=1}^{m} a_{i,j}}\right)^{m}$$

2. Étudier le cas d'égalité dans l'inégalité de Hölder.

3. Soient $a_1, \ldots, a_n > 0$, Montrer que :

$$(1+a_1)(1+a_2)\ldots(1+a_n) \geqslant (1+\sqrt[n]{a_1 a_2 \ldots a_n})^n$$

Solution. (SABIR Ilyass)

1- Soient $m, n \in \mathbb{N}^\star$, $(a_{2,1}, \ldots, a_{2,n}), (a_{1,1}, \ldots, a_{1,n}), \ldots$,et $(a_{m,1}, \ldots, a_{m,n})$ des réels positifs.

Montrons que :

$$\prod_{i=1}^{m}\left(\sum_{j=1}^{n} a_{i,j}\right) \geqslant \left(\sum_{j=1}^{n} \sqrt[m]{\prod_{i=1}^{m} a_{i,j}}\right)^{m}$$

On sait que la fonction ln est concave sur $]0, +\infty[$.

D'après l'inégalité de Jensen, pour tous $p_1, .., p_m > 0$ tels que

$$\frac{1}{p_1} + \cdots + \frac{1}{p_m} = 1$$

et pour tous $x_1, \ldots, x_m > 0$, on a :

$$\ln\left(\sum_{i=1}^{m} \frac{x_i^{p_i}}{p_i}\right) \geqslant \sum_{i=1}^{m} \ln(x_i)$$

Ainsi :

$$\sum_{i=1}^{m} \frac{x_i^{p_i}}{p_i} \geqslant \prod_{i=1}^{m} x_i \quad (\mathrm{AM-GM}\ \textit{généralisée})$$

En particulier, pour tout $j \in [\![1, n]\!]$, posons $x_i = \dfrac{a_{i,j}}{\left(\sum_{k=1}^{n} a_{i,k}\right)}$, et $p_i = m$ pour tout $i \in [\![1, m]\!]$.

On obtient, pour tout $j \in [\![1, n]\!]$:

$$\begin{aligned}\sum_{i=1}^{m} \frac{a_{i,j}}{m\left(\sum_{k=1}^{n} a_{i,k}\right)} &\geqslant \prod_{i=1}^{m} \left(\frac{a_{i,j}}{\left(\sum_{k=1}^{n} a_{i,k}\right)}\right)^{\frac{1}{m}} \\ &= \frac{\sqrt[m]{\prod_{i=1}^{m} a_{i,j}}}{\prod_{i=1}^{m}\left(\sum_{k=1}^{n} a_{i,k}\right)^{\frac{1}{m}}}\end{aligned}$$

En sommant sur j, on obtient :

$$\sum_{j=1}^{n}\sum_{i=1}^{m} \frac{a_{i,j}}{m\left(\sum_{k=1}^{n} a_{i,k}\right)} \geqslant \sum_{j=1}^{n} \frac{\sqrt[m]{\prod_{i=1}^{m} a_{i,j}}}{\prod_{i=1}^{m}\left(\sum_{k=1}^{n} a_{i,k}\right)^{\frac{1}{m}}}$$

Avec :

$$\begin{aligned}\sum_{j=1}^{n}\sum_{i=1}^{m} \frac{a_{i,j}}{m\left(\sum_{k=1}^{n} a_{i,k}\right)} &= \sum_{i=1}^{m} \frac{1}{m} \sum_{j=1}^{n} \frac{a_{i,j}}{\sum_{k=1}^{n} a_{i,k}} \\ &= \sum_{i=1}^{m} \frac{1}{m} \\ &= 1\end{aligned}$$

On obtient finalement :

$$1 \geqslant \sum_{j=1}^{n} \frac{\sqrt[m]{\prod_{i=1}^{m} a_{i,j}}}{\prod_{i=1}^{m}\left(\sum_{k=1}^{n} a_{i,k}\right)^{\frac{1}{m}}}$$

Donc :

$$\prod_{i=1}^{m}\left(\sum_{k=1}^{n} a_{i,k}\right)^{\frac{1}{m}} \geqslant \sum_{j=1}^{n} \sqrt[m]{\prod_{i=1}^{m} a_{i,j}}$$

D'où :

$$\prod_{i=1}^{m}\left(\sum_{j=1}^{n} a_{i,j}\right) \geqslant \left(\sum_{j=1}^{n} \sqrt[m]{\prod_{i=1}^{m} a_{i,j}}\right)^{m}$$

2. L'égalité dans l'inégalité de Hölder est atteinte si, pour tout $j \in [\![1, n]\!]$, on a :

$$\sum_{i=1}^{m} \frac{a_{i,j}}{m\left(\sum\limits_{k=1}^{n} a_{i,k}\right)} = \prod_{i=1}^{m} \left(\frac{a_{i,j}}{\left(\sum\limits_{k=1}^{n} a_{i,k}\right)} \right)^{\frac{1}{m}}$$

Cela implique :

$$\ln\left(\sum_{i=1}^{m} \frac{a_{i,j}}{m\left(\sum\limits_{k=1}^{n} a_{i,k}\right)}\right) = \sum_{i=1}^{m} \ln\left(\frac{a_{i,j}}{\left(\sum\limits_{k=1}^{n} a_{i,k}\right)} \right)$$

Étant donné que la fonction ln est strictement concave, cela signifie que $\frac{a_{i,j}}{\left(\sum\limits_{k=1}^{n} a_{i,k}\right)}$ est indépendant de i, d'où l'existence d'une constante $C_j > 0$ telle que, pour tout $i, l \in [\![1, m]\!]$

$$\frac{a_{i,j}}{a_{l,j}} = C_j$$

3. Soient $a_1, \ldots, a_n > 0$. Montrons que :

$$(1 + a_1)(1 + a_2) \ldots (1 + a_n) \geqslant (1 + \sqrt[n]{a_1 a_2 \ldots a_n})^n$$

Méthode 1.

Par application directe de l'inégalité de Hölder, le résultat suit.

Méthode 2.

En appliquant l'inégalité arithmético-géométrique, on obtient :

$$\frac{1}{1 + a_1} + \cdots + \frac{1}{1 + a_n} \geqslant \frac{n}{\sqrt[n]{(1 + a_1) \ldots (1 + a_n)}}$$

Et

$$\frac{a_1}{1 + a_1} + \cdots + \frac{a_n}{1 + a_n} \geqslant \frac{n \sqrt[n]{a_1 \ldots a_n}}{\sqrt[n]{(1 + a_1) \ldots (1 + a_n)}}$$

En sommant les deux, on obtient :

$$n \geqslant \frac{n\left(1 + \sqrt[n]{a_1 \ldots a_n}\right)}{\sqrt[n]{(1 + a_1) \ldots (1 + a_n)}}$$

ce qui entraîne :

$$(1+a_1)(1+a_2)\dots(1+a_n) \geqslant (1+\sqrt[n]{a_1a_2\dots a_n})^n$$

✠✠✠✠✠✠✠

Cet exercice explore les propriétés des suites complexes dont la puissance p-ième tend vers 1 et dont la moyenne arithmétique converge. L'objectif est de caractériser l'ensemble des valeurs possibles de cette moyenne limite.

Exercice 34.

Soit $n \geqslant 1$ et soit P est une matrice de $M_n(\mathbb{C})$. On a l'équivalence :

Le rayon spectral de $P < 1$ si et seulement si $\lim\limits_{k\to+\infty} P^k = 0$.

Solution. (SABIR Ilyass)

$\Leftarrow$) Supposons que $\lim\limits_{k\to+\infty} P^k = 0$
Soit $n \geqslant 1$ et soit P est une matrice de $M_n(\mathbb{C})$.
Pour toute norme N sur $M_{n,1}(\mathbb{C})$, on note :

$$\mathcal{N}(N) : T \in M_n(\mathbb{C}) \longmapsto \sup_{x\neq 0} \frac{N(Tx)}{N(x)}$$

$\mathcal{N}(N)$ est une norme sur $M_n(\mathbb{C})$. De plus, pour tout $(x,T) \in M_{n,1}(\mathbb{C}) \times M_n(\mathbb{C})$:

$$N(Tx) \leq \mathcal{N}(N)(T)N(x) \quad (\maltese)$$

Fixons maintenant une norme N de $M_n(\mathbb{C})$. Soit λ une valeur propre de P et x_λ un vecteur propre de P associé à λ.

D'après ($\maltese$), pour tout $k \in \mathbb{N}$:

$$N(P^k x_\lambda) \leq \mathcal{N}(N)(P)^k N(x_\lambda)$$

Ainsi, pour tout $k \in \mathbb{N}$

$$|\lambda|^k N(x_\lambda) \leq \mathcal{N}(P)^k N(x_\lambda)$$

Avec $N(x_\lambda) \neq 0$ (puisque $x_\lambda \neq 0$), on en déduit que pour tout $k \in \mathbb{N}$:

$$|\lambda|^k \leq \mathcal{N}(P^k)$$

Comme $\lim_{k\to+\infty} P^k = 0$ et $\dim M_n(\mathbb{C}) < +\infty$, donc toutes les normes de $M_n(\mathbb{C})$ sont équivalentes.

On a donc $\lim_{k\to+\infty} P^k = 0$ dans l'espace $(M_n(\mathbb{C}), \mathcal{N}(N))$.

Puisque $\lim_{k\to+\infty} \mathcal{N}(P^k) = 0$, alors $\lim_{k\to+\infty} |\lambda|^k = 0$.

Ceci n'est possible que si $|\lambda| < 1$, et ça pour tout $\lambda \in \mathrm{Sp}(P)$.

Ainsi,

$$\rho(P) = \max_{\lambda\in\mathrm{Sp}(P)} |\lambda| < 1.$$

$\Rightarrow$) Supposons que $\rho(P) = \max_{\lambda\in\mathrm{Sp}(P)} |\lambda| < 1$.

Toute matrice carrée P peut être mise sous forme de Jordan. Il existe une matrice inversible S telle que :

$$P = SJS^{-1}$$

où J est la matrice de Jordan composée de blocs associés aux valeurs propres de P.

Donc pour tout $k \in \mathbb{N}$:

$$P^k = (SJS^{-1})^k = SJ^kS^{-1}$$

Chaque bloc de Jordan J_i associé à une valeur propre λ_i a la forme :

$$J_i = \lambda_i I + N$$

où N est une matrice nilpotente.

La k-ième puissance d'un bloc de Jordan est donnée par :

$$J_i^k = \lambda_i^k \sum_{j=0}^{k} \begin{pmatrix} k \\ j \end{pmatrix} \frac{1}{\lambda_i^j} N^j$$

Comme $|\lambda_i| < 1$, les termes λ_i^k tendent vers 0. Même en tenant compte des puissances de k dues aux termes en N, l'ensemble tend vers 0 :

$$\lim_{k\to+\infty} J_i^k = 0$$

Puisque chaque bloc J_i^k tend vers la matrice nulle, il en est de même pour J^k, et donc :

$$\begin{aligned}\lim_{k\to+\infty} P^k &= \lim_{k\to+\infty} SJ^kS^{-1} \\ &= S\left(\lim_{k\to+\infty} J^k\right)S^{-1} \\ &= 0\end{aligned}$$

D'où l'équivalence.

✠✠✠✠✠✠✠

Cet exercice explore les propriétés des suites complexes dont la puissance p-ième tend vers 1 et dont la moyenne arithmétique converge. L'objectif est de caractériser l'ensemble des valeurs possibles de cette moyenne limite.

Exercice 35.

Soit $p \in \mathbb{N}^*$, soit E l'ensemble des suites (u_n) de nombres complexes vérifiant $\lim_{n\to+\infty} u_n^p = 1$, et telles que la suite de terme général $S_n = \frac{1}{n}\sum_{k=1}^{n} u_k$ converge. On considère l'application φ de E dans $\mathbb{C}$ qui, à la suite (u_n), associe la limite l de la suite (S_n). Déterminer $\varphi(E)$.

Solution. (SABIR Ilyass)

Soit $p \in \mathbb{N}^*$,

Notons W_p l'ensemble des racines p-ièmes de l'unité, données par $\omega_k = e^{\frac{2i\pi k}{p}}$ pour tout $1 \leq k \leq p$.

Pour déterminer l'image $\varphi(E)$ de la fonction φ, nous devons trouver toutes les limites possibles $l \in \mathbb{C}$ telles qu'il existe une suite $(u_n) \in E$ satisfaisant les conditions suivantes :

1. $\lim_{n\to+\infty} u_n^p = 1$,
2. La suite $S_n = \frac{1}{n}\sum_{k=1}^{n} u_k$ converge vers l.

La condition $\lim_{n\to+\infty} u_n^p = 1$ implique que les p-ièmes puissances des u_n tendent vers 1. Cela signifie que les u_n s'approchent des racines p-ièmes de l'unité dans le plan complexe.

Les racines p-ièmes de l'unité sont données par :

$$C_p = \left\{ e^{2i\pi\frac{m}{p}} \mid m = 0, 1, \ldots, p-1 \right\}.$$

La convergence de S_n signifie que la moyenne des u_n se stabilise lorsque n croît.

Construction des Suites et Limites :

- Si $u_n \to \zeta$ où $\zeta \in C_p$, alors $u_n^p \to \zeta^p = 1$. La limite de S_n sera $l = \zeta$.

- Si u_n prend des valeurs dans C_p avec certaines fréquences, nous pouvons définir α_m comme la fréquence asymptotique de $u_n = \zeta_m$.
Alors, $S_n \to l = \sum_{m=0}^{p-1} \alpha_m \zeta_m$. avec $\alpha_m \geq 0$ et $\sum_{m=0}^{p-1} \alpha_m = 1$.

- Même si les u_n ne sont pas exactement les racines de l'unité mais s'en approchent, tant que $u_n^p \to 1$, une logique similaire s'applique.

L'équation $u_n^p \to 1$ implique que chaque u_n s'approche d'une solution de $z^p = 1$, c'est-à-dire des racines p-ièmes de l'unité.

Plus précisément, pour tout $\varepsilon > 0$, il existe N tel que pour tout $n \geq N$, $\mid u_n^p - 1 \mid < \varepsilon$.

Donc, pour n suffisamment grand, il existe $m_n \in \{0, 1, \ldots, p-1\}$ tel que u_n est proche de ω_{m_n}.

On peut écrire :

$$u_n = e^{2i\pi m_n/p} e^{i\varepsilon_n},$$

où : $m_n \in \{0, 1, \ldots, p-1\}$ (car u_n est proche de la m_n-ème racine de l'unité), et $\varepsilon_n \underset{n\to\infty}{\to} 0$ (petite déviation par rapport à la racine de l'unité exacte).

On peut écrire la moyenne S_n comme suit :

$$\begin{aligned} S_n &= \frac{1}{n} \sum_{k=1}^{n} u_k \\ &= \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi m_k/p} e^{i\varepsilon_k} \end{aligned}$$

Comme $\varepsilon_k \underset{k\to\infty}{\to} 0$, pour les grandes valeurs de n, $e^{i\varepsilon_k} = 1 + i\varepsilon_k + o(\varepsilon_k)$. Par conséquent :

$$u_k = e^{2i\pi m_k/p} + e^{2i\pi m_k/p} i\varepsilon_k + o(\varepsilon_k)$$

La moyenne S_n devient :

$$S_n = \frac{1}{n}\sum_{k=1}^{n} e^{2i\pi m_k/p} + \frac{1}{n}\sum_{k=1}^{n} e^{2i\pi m_k/p} i\varepsilon_k + o(\varepsilon_k)$$

Le second terme $\frac{1}{n}\sum_{k=1}^{n} e^{2i\pi m_k/p} i\varepsilon_k$ implique des ε_k qui sont petits et tendent vers zéro.

Comme $\varepsilon_k \underset{k\to\infty}{\to} 0$ et sont bornés, la somme des ε_k sur n termes divisée par n tend vers zéro :

$$\left|\frac{1}{n}\sum_{k=1}^{n} \varepsilon_k\right| \leq \frac{1}{n}\sum_{k=1}^{n} |\varepsilon_k| \underset{k\to\infty}{\to} 0.$$

Par conséquent, le terme d'erreur disparaît dans la limite :

$$\lim_{n\to\infty} \frac{1}{n}\sum_{k=1}^{n} e^{2i\pi m_k/p} i\varepsilon_k = 0$$

La limite de S_n est déterminée par les fréquences des racines de l'unité $e^{2i\pi m/p}$ parmi les u_k :

$$l = \lim_{n\to\infty} S_n = \sum_{m=0}^{p-1} \alpha_m e^{2i\pi m/p}$$

où α_m est la fréquence asymptotique de u_k étant proche de $e^{2i\pi m/p}$.

Définissons $N_m(n)$ comme le nombre de $k \leq n$ tels que u_k soit proche de $e^{2i\pi m/p}$.

La fréquence asymptotique est donnée par $\alpha_m = \lim_{n\to\infty} \frac{N_m(n)}{n}$.

Comme $\sum_{m=0}^{p-1} N_m(n) = n$, on a $\sum_{m=0}^{p-1} \alpha_m = 1$.

La limite l est une moyenne pondérée des racines de l'unité :

$$l = \sum_{m=0}^{p-1} \alpha_m e^{2i\pi m/p}.$$

Chaque α_m représente la proportion de termes u_k proches d'une racine de l'unité donnée.

Comme $\alpha_m \geq 0$ et $\sum_{m=0}^{p-1} \alpha_m = 1$, l est une combinaison convexe des racines p-ièmes de l'unité.

L'ensemble de tous ces l forme l'enveloppe convexe de C_p :

$$\varphi(E) = \text{Conv}\{e^{2\pi i m/p} \mid m = 0, 1, \ldots, p-1\}.$$

✠✠✠✠✠✠✠

Cet exercice est inspiré d'un problème de l'Olympiade Internationale de Mathématiques (IMO) 2021. Il s'agit d'un défi combinatoire où vous devrez utiliser des raisonnements arithmétiques et logiques pour résoudre un problème de partition de cartes.

Exercice 36. (Problème 1 IMO 2021 Jour 1)

Soit $n \geqslant 100$ un entier. Ivan écrit les nombres $n, n+1, \ldots, 2n$ chacun sur une carte différente. Il mélange ensuite ces $n+1$ cartes et les divise en deux tas. Montrez qu'au moins un des tas contient deux cartes dont la somme des nombres est un carré parfait.

Solution. (SABIR Ilyass)

Nous généralisons ce problème en posant la question suivante :

Généralisation du problème 1.

Soit $r \in \mathbb{N}$ tel que $r \geqslant 1$, et soit $n \geqslant \frac{5r^2}{2} + \frac{5r}{2}$ un entier. Ivan écrit les nombres $n, n+1, \ldots, 2n$ chacun sur une carte différente. Il mélange ensuite ces $n+1$ cartes et les divise en $2r$ tas. Montrez qu'au moins un des tas contient deux cartes dont la somme des nombres est un carré parfait.

Remarquons que l'exerice est un cas particulier où $r = 1$. Nous nous intéressons maintenant à la résolution de cette généralisation.

Pour avoir deux cartes dans l'un des tas de sorte que la somme de leurs nombres soit un carré parfait, il est suffisant de montrer qu'il existe $r+1$ cartes telles que la somme de chaque paire de ces cartes soit un carré parfait.

Soient $x_1, \ldots, x_{2r+1} \in \mathbb{N}$, et $a_1, \ldots, a_{2r+1} \in [\![n, 2n]\!]$ satisfaisant le système d'équations suivant :

$$\begin{aligned} a_1 + a_2 &= x_1^2 \\ a_2 + a_3 &= x_2^2 \\ &\vdots \\ a_{2r} + a_{2r+1} &= x_{2r}^2 \\ a_{2r+1} + a_1 &= x_{2r+1}^2 \end{aligned}$$

Pour conclure, il suffit de prouver que ce système d'équations admet une solution (avec certaines conditions sur $x_1, \ldots, x_n$), où les inconnues sont $(a_1, \ldots, a_{r+1}) \in [\![n, 2n]\!]^{2r+1}$.

On a :

$$\sum_{\text{cyc}} (a_1 + a_2) = \sum_{\text{cyc}} x_1^2 = \sum_{k=1}^{r+1} x_k^2$$

Remarquons que :

$$x_{2r+2} = x_1, x_{2r+3} = x_2, \ldots, x_{4r+2} = x_{2r+1}$$

et

$$a_{2r+2} = a_1, a_{2r+3} = a_2, \ldots, a_{4r+2} = a_{2r+1}$$

On a pour tout $l \in [\![0, r]\!]$

$$\begin{aligned} \sum_{k=1}^{2r+1} (-1)^k (a_{k+l} + a_{k+l+1}) &= \sum_{k=0}^{r-1} [(a_{2k+l+2} + a_{2k+l+3}) - (a_{2k+l+2} + a_{2k+l+1})] - (a_{2r+l+1} + a_{2r+2+l}) \\ &= \sum_{k=0}^{r-1} [a_{2k+l+3} - a_{2k+l+1}] - (a_{2r+l+1} + a_{2r+2+l}) \\ &= \sum_{k=0}^{r-1} [a_{2(k+1)+l+1} - a_{2k+l+1}] - (a_{2r+l+1} + a_{2r+2+l}) \\ &= a_{2r+l+1} - a_{l+1} - (a_{2r+l+1} + a_{2r+2+l}) \\ &= -a_{2r+2+l} - a_{l+1} \\ &= -2a_{l+1} \end{aligned}$$

Ainsi, pour tout $l \in [\![0, r]\!]$,

$$a_{l+1} = \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(a_{k+l} + a_{k+l+1}) = \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}x_{k+l}^2$$

Par translation, nous pouvons en conclure que pour tout $j \in [\![1, r+1]\!]$,

$$a_j = \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(a_{k+j-1} + a_{k+j}) = \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}x_{k+j-1}^2$$

Nous cherchons à trouver $(x_1, x_2, \ldots, x_{2r+1}) \in \mathbb{N}$, satisfaisant :

$$\frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}x_{k+j-1}^2 \in [\![n, 2n]\!]$$

pour tout $j \in [\![1, r+1]\!]$, où $x_{2r+2} = x_1, x_{2r+3} = x_2, \ldots, x_{4r+2} = x_{2r+1}$.

Pour minimiser la valeur de

$$\frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}x_{k+j-1}^2$$

pour tout $j \in [\![1, r+1]\!]$, il est naturel de considérer $x_1, x_2, \ldots, x_{2r+1}$ comme étant consécutifs.

Et en raison de la somme alternée, et pour simplifier le calcul, nous considérons $\alpha \in \mathbb{N}^\star$, tel que, pour tout $j \in [\![1, 2r+1]\!]$

$$x_j = \alpha + j - r$$

On a pour tout $j \in [\![1, 2r+1]\!]$

$$\begin{aligned}
a_j &= \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(\alpha + k + j - r - 1)^2 \\
&= \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(\alpha^2 + 2(k+j-r-1)\alpha + (k+j-r-1)^2) \\
&= \left(\frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}\right)\alpha^2 + \left(\sum_{k=1}^{2r+1}(-1)^{k-1}(k+j-r-1)\right)\alpha + \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(k+j-r-1)^2 \\
&= \frac{1}{2}\alpha^2 + \left(\sum_{k=1}^{2r+1}(-1)^{k-1}(k+j-r-1)\right)\alpha + \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(k+j-r-1)^2
\end{aligned}$$

où

$$\begin{aligned}\sum_{k=1}^{2r+1}(-1)^{k-1}(k+j-r-1) &= \sum_{k=1}^{2r+1}(-1)^{k-1}k + (j-r-1)\sum_{k=1}^{2r+1}(-1)^{k-1} \\ &= \sum_{k=1}^{r}[2k-(2k-1)] + j - r - 1 + (2r+1) \\ &= \left(\sum_{k=1}^{r}1\right) + j + r \\ &= 2r + j\end{aligned}$$

et

$$\begin{aligned}\frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(k+j-r-1)^2 &= \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}(k^2+2k(j-r-1)+(j-r-1)^2) \\ &= \frac{1}{2}\sum_{k=1}^{2r+1}(-1)^{k-1}k^2 + (j-r-1)\sum_{k=1}^{2r+1}(-1)^{k-1}k \\ &\quad + \frac{(j-r-1)^2}{2}\sum_{k=1}^{2r+1}(-1)^{k-1} \\ &= \frac{1}{2}\sum_{k=1}^{r}[(2k)^2-(2k-1)^2] + (j-r-1)r + \frac{(j-r-1)^2}{2} + (2r+1)^2 \\ &= \frac{1}{2}\sum_{k=1}^{r}[4k-1] + (j-r-1)r + \frac{(j-r-1)^2}{2} + (2r+1)^2 \\ &= r(r+1) - \frac{r}{2} + (j-r-1)r + \frac{(j-r-1)^2}{2} + (2r+1)^2 \\ &= \frac{9r^2}{2} + \frac{9r}{2} + \frac{j^2}{2} + \frac{3}{2} - j\end{aligned}$$

Donc,

$$\begin{aligned}a_j &= \frac{1}{2}\alpha^2 + (2r+j)\alpha + \frac{9r^2}{2} + \frac{9r}{2} + \frac{j^2}{2} + \frac{3}{2} - j \\ &= \frac{1}{2}(\alpha-1)^2 + (2r+j+1)(\alpha-1) + \frac{9r^2}{2} + \frac{13r}{2} + \frac{j^2}{2} + 2\end{aligned}$$

Maintenant, nous nous intéressons à trouver la valeur maximale et minimale de $a_1, \ldots, a_{2r+1}$. Pour cela, nous considérons la fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ définie pour tout $x \in \mathbb{R}$ par :

$$\begin{aligned}f(x) &= \frac{1}{2}\alpha^2 + (2r+x)\alpha + \frac{9r^2}{2} + \frac{9r}{2} + \frac{x^2}{2} + \frac{3}{2} - x \\ &= \frac{x^2}{2} + (\alpha-1)x + \frac{1}{2}\alpha^2 + 2r\alpha + \frac{9r^2}{2} + \frac{9r}{2} + \frac{3}{2}\end{aligned}$$

On a :

$$\Delta_f = (\alpha-1)^2 - 2\left(\frac{1}{2}\alpha^2 + 2r\alpha + \frac{9r^2}{2} + \frac{9r}{2} + \frac{3}{2}\right) = -4\alpha(1+r) - 9r^9 - 9r - 2 < 0$$

et

$$\lim_{x\to+\infty} f(x) = +\infty$$

Ainsi, f est croissante sur $\mathbb{R}$, en particulier

$$\min_{1\leqslant j\leqslant 2r+1} a_j = a_1 \text{ and } \max_{1\leqslant j\leqslant 2r+1} a_j = a_{2r+1}$$

Avec

$$a_1 = \frac{1}{2}\alpha^2 + (2r+1)\alpha + \frac{9r^2}{2} + \frac{9r}{2} + 1$$

et

$$a_{2r+1} = \frac{1}{2}\alpha^2 + (4r+1)\alpha + \frac{13r^2}{2} + \frac{9r}{2} + 1$$

Le problème devient de trouver $\alpha \in \mathbb{N}$ tel que $a_1 \geqslant n$ et $\backslash a_{2r+1} \leqslant 2n$, donc

$$\begin{aligned} \frac{1}{2}\alpha^2 + (2r+1)\alpha + \frac{9r^2}{2} + \frac{9r}{2} + 1 &\geqslant n \\ \frac{1}{2}\alpha^2 + (4r+1)\alpha + \frac{13r^2}{2} + \frac{9r}{2} + 1 &\leqslant 2n \end{aligned}$$

Donc, étant donné que $\alpha > 0$, on a :

$$\begin{aligned} \alpha &\geqslant -(2r+1) + \sqrt{2n - 5r^2 - 5r - 1} \\ \alpha &\leqslant -(4r+1) + \sqrt{4n + 3r^2 - r - 1} \end{aligned}$$

Pour avoir un entier entre $r + \frac{1}{2} + \sqrt{2n - 5r^2 - 5r - 1}$ et $2r + \frac{1}{2} + \sqrt{2n + 3r^2 - r - 1}$, il suffit que :

$$\left(-(4r+1) + \sqrt{4n + 3r^2 - r - 1}\right) - \left(-(2r+1) + \sqrt{2n - 5r^2 - 5r - 1}\right) \geqslant 1$$

Ainsi,

$$\sqrt{4n + 3r^2 - r - 1} - \sqrt{2n - 5r^2 - 5r - 1} - 2r - 1 \geqslant 0$$

Nous considérons la fonction $h : \mathbb{R} \to \mathbb{R}$définie pour tout $x \geqslant \frac{5r^2}{2} + \frac{5r}{2}$ par :

$$h(x) = \sqrt{4x + 3r^2 - r - 1} - \sqrt{2x - 5r^2 - 5r - 1} - 2r - 1$$

La fonction h est dérivable sur l'intervalle$\left]\frac{5}{2}r^2 + \frac{5}{2}r + \frac{1}{2}, +\infty\right[$. Et pour tout $x \in \left]\frac{5}{2}r^2 + \frac{5}{2}r + \frac{1}{2}, +\infty\right[$, on a :

$$\begin{aligned}
h'(x) &= \frac{2}{\sqrt{4x + 3r^2 - r - 1}} - \frac{1}{\sqrt{2x - 5r^2 - 5r - 1}} \\
&= \frac{2\sqrt{2x - 5r^2 - 5r - 1} - \sqrt{4x + 3r^2 - r - 1}}{\sqrt{(2x + 3r^2 - r - 1)(2x - 5r^2 - 5r - 1)}} \\
&= \frac{4(2x - 5r^2 - 5r - 1) - (4x + 3r^2 - r - 1)}{2\sqrt{2x - 5r^2 - 5r - 1}\sqrt{4x + 3r^2 - r - 1}\left(2\sqrt{2x - 5r^2 - 5r - 1} + \sqrt{4x + 3r^2 - r - 1}\right)} \\
&= \frac{4x - 23r^2 - 19r - 3}{\sqrt{(2x + 3r^2 - r - 1)(2x - 5r^2 - 5r - 1)}\left(\sqrt{2x - 5r^2 - 5r - 1} + \sqrt{2x + 3r^2 - r - 1}\right)} \\
&< 0
\end{aligned}$$

Par conséquent, elle est croissante sur $[23r^2 + 19r + 3, +\infty[$, de plus :

$$\begin{aligned}
h(23r^2 + 19r + 3) &= \sqrt{4(23r^2 + 19r + 3) + 3r^2 - r - 1} \\
&\quad - \sqrt{2(23r^2 + 19r + 3) - 5r^2 - 5r - 1} - 2r - 1 \\
&= \sqrt{95r^2 + 75r + 11} - \sqrt{41r^2 + 33r + 5} - 2r - 1 \\
&> 0
\end{aligned}$$

Donc, pour tout $n \geqslant 23r^2 + 19r + 3$, on a :

$$\left(-(4r + 1) + \sqrt{4n + 3r^2 - r - 1}\right) - \left(-(2r + 1) + \sqrt{2n - 5r^2 - 5r - 1}\right) \geq 1$$

Le problème est complètement résolu.

Maintenant, pour aller plus loin et rendre ce problème plus difficile, nous proposons les défis suivants :

Quelques défis.

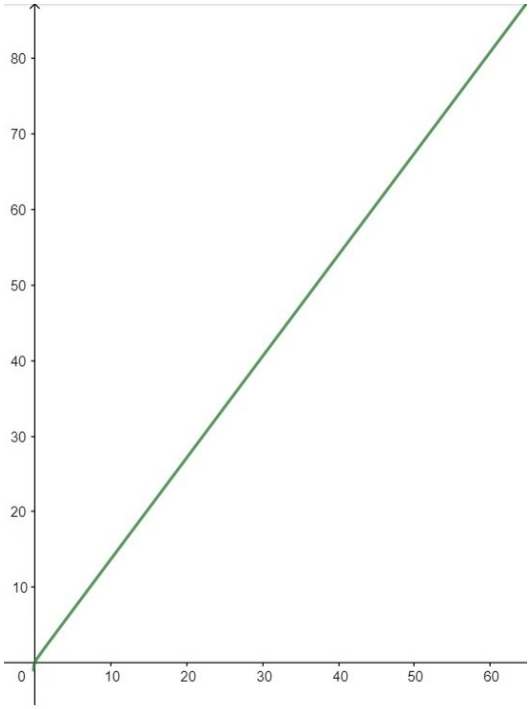


FIGURE 3 – Graphe de la fonction $r \longmapsto \sqrt{95r^2+75r+11} - \sqrt{41r^2+33r+5} - 2r - 1$

Défi 1.

$\star$ Soit $r > 1$ un entier, trouvez le plus petit entier $f(r)$ tel que, pour tout $n \geqslant f(r)$, si l'on écrit les nombres $n, n+1, \ldots, 2n$ chacun sur une carte différente, puis que l'on mélange ces $n+1$ cartes et qu'on les divise en deux tas, alors il existe r cartes dans l'un des tas dont la somme des nombres est un carré parfait.

Défi 2.

$\star$ Soient $r, s > 1$ deux entiers. Trouvez le plus petit entier $g(r,s)$ tel que, pour tout $n \geqslant g(r,s)$, si l'on écrit les nombres $n, n+1, \ldots, n+s$ chacun sur une carte différente, puis que l'on mélange ces $s+1$ cartes et qu'on les divise en deux tas, alors il existe r cartes dans l'un des tas dont la somme des nombres est un carré parfait.

Défi 3.

$\star$ Soient $r, s, t, v, w > 1$ cinq entiers, trouvez le plus petit entier $h(r, s, t, v, w)$ tel que, pour tout $n \geqslant h(r, s, t, v, w)$, si l'on écrit les nombres $n, n+1, \ldots, n+s$ chacun sur une carte différente, puis que l'on mélange ces $s + 1$ cartes et qu'on les divise en t tas, alors il existe v cartes dans l'un des tas dont la somme des nombres est une puissance parfaite de w.

Quatrième partie

Sujets d'étude

Cette partie explore quatre sujets complexes en mathématiques, chacun abordant un domaine distinct et fondamental :

1. **Probabilité que des entiers soient premiers entre eux** : ce sujet se concentre sur la probabilité d'obtenir des entiers premiers entre eux dans un ensemble donné, en utilisant des concepts de la théorie des probabilités et des méthodes combinatoires.
2. **Les polynômes irréductibles sur un corps fini** : ce sujet analyse le nombre de polynômes irréductibles dans un corps fini, un aspect essentiel de l'algèbre et de la théorie des corps, avec des applications potentielles en cryptographie et dans les structures algébriques.
3. **Distribution des puissances d'un nombre dans une base de numération** : ce sujet examine la manière dont les puissances d'un nombre se répartissent dans une base spécifique, en analysant les fréquences d'apparition des chiffres en première position selon une approche probabiliste.
4. **Théorème de Dirichlet sur les progressions arithmétiques** : ce théorème fondamental en théorie des nombres démontre l'existence d'une infinité de nombres premiers dans certaines progressions arithmétiques, abordant la répartition des nombres premiers, un sujet de grande importance en mathématiques pures et appliquées.

Sujet 1 : Probabilité que l entiers soient premiers entre eux.

SABIR Ilyass

$\star\star\star$

Soit $l \in \mathbb{N}^\star$, notons $\Omega = (\mathbb{N}^*)^l$, nous considérons l'espace probabiliste $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$, où $\mathbb{P}$ est la fonction de masse de probabilité définie par :

$$\mathbb{P} : I \in \mathcal{P}(\Omega) \longmapsto \lim_{n\to+\infty} \frac{\text{card}\,(I \bigcap \Omega_n)}{n^l} \in [0,1]$$

où $\Omega_n = [\![1, n]\!]^l$.

Notons

$$A_l = \left\{(a_1, a_2, \ldots, a_l) \in \mathbb{N}_*^l | \bigwedge_{k=1}^{l} a_k = 1\right\}$$

et pour tout $n \geqslant 1$,

$$A_{n,l} = \left\{(a_1, a_2, \ldots, a_l) \in [\![1, n]\!]^l | \bigwedge_{k=1}^{l} a_k = 1\right\}$$

Soient $p_1, \ldots, p_k$ des nombres premiers inférieurs à n, et $(U_i)_{i\in[\![1,k]\!]}$ une famille d'ensembles définie pour tout $i \in [\![1, k]\!]$ par :

$$U_i = \{(a_1, a_2, \ldots, a_l) \in [\![1, n]\!]^l | \forall j \in [\![1, l]\!], p_i | a_j\}$$

Nous pouvons facilement constater que :

$$A_{l,n} = \overline{\bigcup_{i=1}^{k} U_i}$$

Pour calculer la cardinalité, nous utiliserons le principe d'inclusion-exclusion.

Lemme 1. (Formule de Poincaré) Soient $E_1, \ldots, E_n$ des ensembles finis, alors :

$$\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} (-1)^{k-1} \#\left(\bigcap_{j=1}^{k} E_{i_j}\right)$$

Preuve du lemme 1. Pour $n \geqslant 2$, la preuve pour $n = 2$ a déjà été vue. Supposons que la formule est vraie pour n, montrons-la pour $n+1$.

En appliquant d'abord le cas $n = 2$, puis la distributivité des intersections, on obtient :

$$\begin{aligned}
\#\left(\bigcup_{i=1}^{n+1} E_i\right) &= \#\left(\left(\bigcup_{i=1}^{n} E_i\right) \bigcup E_{n+1}\right) \\
&= \#\left(\bigcup_{i=1}^{n} E_i\right) + \#(E_{n+1}) - \#\left(\left(\bigcup_{i=1}^{n} E_i\right) \bigcap E_{n+1}\right) \\
&= \#\left(\bigcup_{i=1}^{n} E_i\right) + \#(E_{n+1}) - \#\left(\left(\bigcup_{i=1}^{n} \left(E_i \bigcap E_{n+1}\right)\right)\right)
\end{aligned}$$

Les premiers et derniers termes sont des unions n, pour lesquelles nous avons supposé la formule vraie. Par conséquent, nous pouvons conclure.

$$\#\left(\bigcup_{i=1}^{n} E_i\right) = \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^{k-1} \#\left(\bigcap_{j=1}^{k} E_{i_j}\right)$$

Et

$$\#\left(\left(\bigcup_{i=1}^{n} \left(E_i \bigcap E_{n+1}\right)\right) = \sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^{k-1} \#\left(\bigcap_{j=1}^{k} \left(E_{i_j} \bigcap E_{n+1}\right)\right)\right.$$

Alors

$$\begin{aligned}
\#\Big(\bigcup_{i=1}^{n+1} E_i\Big) &= \sum_{k=1}^{n} \sum_{1 \leq i_1 < \cdots < i_k \leq n} (-1)^{k-1} \#\Big(\bigcap_{j=1}^{k} E_{i_j}\Big) + \#(E_{n+1}) \\
&\quad + \sum_{k=1}^{n} \sum_{1 \leq i_1 < \cdots < i_k \leq n} (-1)^{k} \#\Big(\bigcap_{j=1}^{k} \Big(E_{i_j} \cap E_{n+1}\Big)\Big)
\end{aligned}$$

Le côté droit peut être réécrit comme

$$\begin{aligned}
&\sum_{k=1}^{n} \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} (-1)^{k-1} \#\left(\bigcap_{j=1}^{k} E_{i_j}\right) + \#(E_{n+1}) \\
= &\sum_{k=1}^{n+1} \sum_{\substack{1 \leqslant i_1 < \cdots < i_k \leqslant n+1 \\ i_k \neq n+1}} (-1)^{k-1} \#\left(\bigcap_{j=1}^{k} E_{i_j}\right) + \sum_{k=1}^{n+1} \#(E_k)
\end{aligned}$$

Et

$$\begin{aligned}&\sum_{k=1}^{n}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n}(-1)^k\#\left(\bigcap_{j=1}^{k}\left(E_{i_j}\bigcap E_{n+1}\right)\right)\\ =\ &\sum_{k=2}^{n+1}\sum_{\substack{1\leqslant i_1<\cdots<i_k<i_k\leqslant n+1\\ i_k=n+1}}(-1)^{k-1}\#\left(\bigcap_{j=1}^{k}E_{i_j}\right)\end{aligned}$$

Nous concluons que

$$\begin{aligned}\#\left(\bigcup_{i=1}^{n+1}E_i\right)=\sum_{k=1}^{n+1}\#(E_k)+\sum_{k=1}^{n+1}\Bigg[&\sum_{\substack{1\leq i_1<\cdots<i_k\leq n+1\\ i_k\neq n+1}}(-1)^{k-1}\#\Big(\bigcap_{j=1}^{k}E_{i_j}\Big)\\ &+\sum_{\substack{1\leq i_1<\cdots<i_k\leq n+1\\ i_k=n+1}}(-1)^{k-1}\#\Big(\bigcap_{j=1}^{k}E_{i_j}\Big)\Bigg].\end{aligned}$$

Ainsi,

$$\#\left(\bigcup_{i=1}^{n+1}E_i\right)=\sum_{k=1}^{n+1}\sum_{1\leqslant i_1<\cdots<i_k\leqslant n+1}(-1)^{k-1}\#\left(\bigcap_{j=1}^{k}E_{i_j}\right)$$

ce qui justifie la formule pour $n+1$.

Définition 1. (La fonction de Möbius) Soit $n\in\mathbb{N}^\star$, on note $\mu(n)$ l'entier défini par :

$$\mu(n)=\begin{cases}0, & \text{si } n \text{ possède un facteur premier au carré,}\\ 1, & \text{si } n \text{ est sans facteur premier au carré et a un nombre pair de facteurs premiers,}\\ -1, & \text{si } n \text{ est sans facteur premier au carré et a un nombre impair de facteurs premiers.}\end{cases}$$

D'après le lemme 1, on a

$$\#\left(\bigcup_{i=1}^{k}U_i\right)=\sum_{j=1}^{k}\sum_{1\leqslant i_1<\cdots<i_j\leqslant k}(-1)^{j-1}\#\left(\bigcap_{m=1}^{j}U_{i_m}\right)$$

Pour conclure, il suffit de calculer $\bigcap\limits_{m=1}^{j}U_{i_m}$, pour tout $\leqslant i_1<\cdots<i_j\leqslant k$

Soit $I \subset [\![1,k]\!]$ non vide, le cardinal de l'intersection $\bigcap_{i\in I} U_i$ est égal au nombre des l-uplets de multiples strictement positifs de $\prod_{i\in I} p_i$ inférieurs ou égaux à n, ce cardinal est égal à : $\left\lfloor \frac{n}{\prod_{i\in I} p_i} \right\rfloor^l$.

La formule de Poincaré donne :

$$\#\left(\bigcup_{i=1}^{k} U_i\right) = \sum_{j=1}^{k} \sum_{1\leqslant i_1<\cdots<i_j\leqslant k} (-1)^{j-1} \left\lfloor \frac{n}{\prod_{m=1}^{j} p_{i_m}} \right\rfloor^l$$

Par conséquent,

$$\#A_{l,n} = n^l - \#\left(\bigcup_{i=1}^{k} U_i\right) = \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^l$$

Donc,

$$\frac{\#(A_{l,n})}{n^l} = \frac{1}{n^l} \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor^l$$

Pour continuer la démonstration, nous avons besoin d'une propriété fondamentale de la fonction de Möbius.

Proposition 1. Pour tout entier $n \neq 1$, on a

$$\sum_{d|n} \mu(d) = 0$$

Preuve. **Méthode 1.** Soit $n = \prod_{i=1}^{m} p_i^{a_i}$ la décomposition en facteurs premiers de n, et $d \in \mathbb{N}$, on a :

$d|n$ and $\mu(d) \neq 0$ si et seulement si $d = \prod_{i\in J} p_i^{a_i}$ avec $J \subset [\![1,m]\!]$. Donc

$$\mu(d) = (-1)^{\#J}$$

Par suite,

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{J\subset[\![1,m]\!]} (-1)^{\#J} \\ &= (1-1)^m \\ &= 0 \quad (\text{car } m > 0) \end{aligned}$$

Méthode 2. Soit $n \geqslant 2$. D'après le théorème fondamental de l'arithmétique, il existe des entiers premiers $(p_1, \ldots, p_r) \in \mathcal{P}^r$ et des entiers $\alpha_1, \ldots, \alpha_r \geqslant 1$ tels que $n = \prod_{i=1}^{r} p_i^{\alpha_i}$

On a alors :

$$\sum_{d|n} \mu(d) = \sum_{k_1=0}^{\alpha_1} \sum_{k_2=0}^{\alpha_2} \cdots \sum_{k_r=0}^{\alpha_r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Donc :

$$\sum_{d|n} \mu(d) = \sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!] k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) + \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Puisque pour tout $(k_1, \ldots, k_r) \in \prod_{i=1}^{r} [\![0, \alpha_i]\!]$ tel qu'il existe $i_0 \in [\![1, r]\!]$ avec $k_{i_0} \geqslant 2$, alors $\prod_{i=1}^{r} p_i^{k_i}$ est divisible par $p_{i_0}^2$, donc

$$\mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$$

Ce qui implique que :

$$\sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!] k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$$

Par conséquent :

$$\sum_{d|n} \mu(d) = \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Pour tout $(k_1, \ldots, k_r) \in [\![0, 1]\!]^r$, on a $\sum_{i=1}^{r} k_i$ est le nombre de facteurs premiers distincts de

$\prod_{i=1}^{r} p_i^{k_i}$, et $\prod_{i=1}^{r} p_i^{k_i}$ n'est pas divisible par le carré d'un nombre premier.

Ainsi :

$$\begin{aligned}\sum_{d|n}\mu(d) &= \sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{i=1}^{r}k_i}\\ &= \prod_{i=1}^{r}\left(\sum_{k_1=0}^{1}(-1)^{k_i}\right)\\ &= (1-1)^r\\ &= 0\end{aligned}$$

Pour l'étude asymptotique de $\frac{\#(A_{l,n})}{n^l}$, il semble naturel de remplacer le terme $\frac{1}{n^l}\left\lfloor\frac{n}{d}\right\rfloor^l$ par son équivalent $\frac{1}{d^l}$. La différence entre les deux sommes s'écrit :

$$\left|\frac{\#(A_{l,n})}{n^l}-\sum_{d=1}^{n}\frac{\mu(d)}{d^l}\right| = \left|\sum_{d=1}^{n}\mu(d)\left(\frac{1}{n^l}\left\lfloor\frac{n}{d}\right\rfloor^l-\frac{1}{d^l}\right)\right|$$

Comme $\left\lfloor\frac{n}{d}\right\rfloor > \frac{n}{d}-1$, On a

$$\begin{aligned}\sum_{k=1}^{l}\binom{l}{k}\frac{1}{d^k n^{l-k}} &= \left(\frac{1}{d}-\frac{1}{n}\right)^l-\frac{1}{d^l}\\ &< \frac{1}{n^l}\left\lfloor\frac{n}{d}\right\rfloor^l-\frac{1}{d^l}\\ &\leqslant 0\end{aligned}$$

Ce qui donne

$$\begin{aligned}\left|\frac{\#(A_{l,n})}{n^l}-\sum_{d=1}^{n}\frac{\mu(d)}{d^l}\right| &\leqslant \sum_{d=1}^{n}\sum_{k=1}^{l}\binom{l}{k}\frac{1}{d^k n^{l-k}}\\ &= \sum_{k=1}^{l}\binom{l}{k}\frac{1}{n^{l-k}}\left(\sum_{d=1}^{n}\frac{1}{d^k}\right)\end{aligned}$$

Ainsi,

$$\begin{aligned}\sum_{k=1}^{l}\binom{l}{k}\frac{1}{n^{l-k}}\left(\sum_{d=1}^{n}\frac{1}{d^k}\right) &\underset{n\to+\infty}{\sim} \binom{l}{1}\frac{1}{n^{l-1}}\log(n)+\sum_{k=2}^{l}\binom{l}{k}\frac{1}{n^{l-k}}\sum_{d=1}^{+\infty}\frac{1}{d^k}\\ &= O\left(\frac{1}{n^{l-1}}\log(n)\right)\end{aligned}$$

Par suite,

$$\mathbb{P}(A_l)=\lim_{n\to+\infty}\frac{\#(A_{l,n})}{n^l}=\sum_{d=1}^{+\infty}\frac{\mu(d)}{d^l}$$

Définition 2. On définit la fonction zêta de Riemann, pour tout $z \in \mathbb{C}$ tel que $\mathrm{Re}(z) > 1$, par

$$\zeta(z) = \sum_{n=1}^{+\infty} \frac{1}{n^z}$$

Proposition 2. Pour tout nombre complexe z tel que $\mathrm{Re}(z) > 1$, on a :

$$\frac{1}{\zeta(z)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^z}$$

Preuve. Soit $z \in \mathbb{C}$, tel que $\mathrm{Re}(z) > 1$,on a, via la proposition 1 :

$$\begin{aligned}
\zeta(z).\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^z} &= \left(\sum_{n=1}^{+\infty} \frac{1}{n^z}\right)\left(\sum_{n=1}^{+\infty} \frac{\mu(n)}{n^z}\right) \\
&= \sum_{n,d\geqslant 1} \frac{\mu(d)}{(n.d)^z} \\
&= \sum_{n\geqslant 1}\sum_{d|n} \frac{\mu(d)}{n^z} \\
&= 1
\end{aligned}$$

On en conclut que

$$\mathbb{P}(A_l) = \frac{1}{\zeta(l)}$$

Remarque 1. On peut déduire directement de ce résultat le théorème d'Euclide, qui énonce que l'ensemble des nombres premiers est infini.

Sujet 2 : Les polynômes irréductibles sur $K[X]$.

SABIR Ilyass

⋆⋆⋆

L'objectif. Soit K un corps commutatif fini, on veut trouver le nombre des polynômes irréductibles sur $K[X]$ de degré n.

⋆⋆⋆⋆⋆⋆⋆⋆⋆

Théorème 1.

Il existe un nombre premier p et un entier $n \in \mathbb{N}$, tel que

$$\#K = p^n$$

Preuve du théorème 1.

Notons L le plus petit sous corps de K.

Puisque K est fini, alors il existe un nnombre premier p tel que L est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, en particulier $\#L = p$.

On note :

$$\begin{aligned} n &:= [K : \mathbb{Z}/p\mathbb{Z}] \\ &= \dim_L(K) \\ &< +\infty \end{aligned}$$

Kest un L espace-vectoriel de dimension n. Notons $\mathcal{B} = (e_1, \ldots, e_n)$ une base de K comme Lespace-vectoriel. De plus l'application :

$$\begin{array}{ccc} L^n & \to & K \\ (x_1, \ldots, x_n) & \longmapsto & \sum_{k=1}^{n} x_k e_k \end{array}$$

est bijective, en particulier :

$$\begin{aligned} \#K &= \#(L^n) \\ &= p^n \end{aligned}$$

$\star\star\star\star\star\star\star\star\star$

On note pour tout entier $n \in \mathbb{N}^*$, $\mathcal{P}_K(n)$ l'ensemble des polynômes unitaires irréductibles de degré n sur $K[X]$.

Pour tout polynôme $P \in K[X]$ irréductible, et pour tout $a \in K\backslash\{0\}$ $a.P$ est également irréductible sur $K[X]$.

On a donc, pour tout entier $n \in \mathbb{N}^*$, le nombre de polynômes irréductibles de degré n est :

$$(\#K - 1).\#\mathcal{P}_K(n)$$

Il ne reste plus qu'à trouver le cardinal de $\mathcal{P}_K(n)$ pour tout $n \in \mathbb{N}^*$.

Théorème 2.

Notons $\#K = q$. Soit $n \in \mathbb{N}^*$, on a

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_K(d)} P(X)$$

Preuve du théorème 2.

Pour tout entier $d \in \mathbb{N}^*$ et pour tout $P \in \mathcal{P}_K(d)$, on a $M = K/(P)$ est un corps (car K est principal), de cardinal q^d , donc isomorphe à $\mathbb{Z}/q^d\mathbb{Z}$. Ainsi, pour tout $x \in M$:

$$x^{q^d} = x$$

Mais si $n = d.k$ pour un $k \in \mathbb{N}^*$, on a

$$x^{q^n} = x^{q^{d.k}} = (((x^{q^d})^{q^d}) \ldots)^{q^d} \quad (k \text{ fois})$$

Par une récurrence immédiate sur k, ceci est égal à x. Autrement dit,

$$X^{q^n} X = 0 \in M[X]$$

Donc P divise $X^{q^n} X$ dans $K[X]$.

Comme les éléments de $\mathcal{P}_K(d)$ sont irréductibles, le produit $\prod_{d|n} \prod_{P \in \mathcal{P}_K(d)} P(X)$ divise lui aussi $X^{q^n} X$.

Réciproquement, soit P un facteur irréductible de degré d de $X^{q^n} X$ dans $K[X]$.

Comme $\mathbb{Z}/q^n\mathbb{Z}$ est un corps de décomposition de $X^{q^n} X$, P est scindé sur $\mathbb{Z}/q^n\mathbb{Z}$.

Si x est une racine de P, on a

$$\begin{aligned}[\mathbb{Z}/q^n\mathbb{Z} : \mathbb{Z}/q\mathbb{Z}] &= n \\ &= [\mathbb{Z}/q^n\mathbb{Z} : \mathbb{Z}/q\mathbb{Z}(x)][\mathbb{Z}/q\mathbb{Z}(x) : \mathbb{Z}/q\mathbb{Z}]\end{aligned}$$

Mais comme P est irréductible, $\mathbb{Z}/q\mathbb{Z}(x)$ est un corps de rupture de P de degré d sur $\mathbb{Z}/q\mathbb{Z}$, donc d divise n.

Il suffit alors de montrer que $X^{q^n}X$ n'admet pas de facteur double (ou plus). En effet, si un tel facteur existe, alors $X^{q^n}X$ admet une racine double dans un corps de décomposition.

Cependant, comme le polynôme dérivé de $X^{q^n}X$ est $q^nX^{q^n-1}1 = -1$ (à cause de la caractéristique), $X^{q^n}X$ n'a pas de racine double dans un corps de décomposition, ce qui termine la preuve.

Définition 1. (La fonction de Möbius)

Soit $n \in \mathbb{N}^*$. On note $\mu(n)$ l'entier défini par :

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carr é} d\prime \text{un nombre premier} \\ (-1)^r & \text{si } r \text{ est le nombre de facteurs premiers distincts de } n, \\ & n \text{ non divisible par le carr é} d\prime \text{un nombre premier} \end{cases}$$

Proposition 1.

pour tout $n \neq 1$, on a l'égalité :

$$\sum_{d|n} \mu(d) = 0$$

Preuve de la proposition 1.

Méthode 1.

Soit $n = \prod_{i=1}^{m} p_i^{a_i}$ la décomposition en facteurs premiers de n.

De plus si $d \in \mathbb{N}$, alors :

$d$divise n and $\mu(d) \neq 0$ si et seulement si $d = \prod_{i \in J} p_i^{a_i}$ with $J \subset [\![1, m]\!]$ et alors

$$\mu(d) = (-1)^{\#J}$$

On en déduit que :

$$\begin{aligned}\sum_{d|n}\mu(d) &= \sum_{J\subset[\![1,m]\!]}(-1)^{\#J}\\ &= (1-1)^m\\ &= 0 \qquad (\text{car } m>0)\end{aligned}$$

Méthode 2.

Soit $n \geqslant 2$. D'après le théorème fondamentale d l'arithmétique, il existe $(p_1,\dots,p_r)\in\mathcal{P}^r$ et $\alpha_1,\dots,\alpha_r \geqslant 1$ tels que

$$n=\prod_{i=1}^{r}p_i^{\alpha_i}$$

On a

$$\begin{aligned}\sum_{d|n}\mu(d) &= \sum_{k_1=0}^{\alpha_1}\sum_{k_2=0}^{\alpha_2}\cdots\sum_{k_r=0}^{\alpha_r}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)\\ &= \sum_{\substack{(k_1,\dots,k_r)\in\prod_{i=1}^{r}[\![0,\alpha_i]\!]\\ \exists i_0\in[\![1,r]\!]k_{i_0}\geqslant 2}}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)+\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)\end{aligned}$$

Puisque pour tout $(k_1,\dots,k_r)\in\prod_{i=1}^{r}[\![0,\alpha_i]\!]$ tel qu'il existe $i_0\in[\![1,r]\!]$ avec $k_{i_0}\geqslant 2$, on a :

$$\prod_{i=1}^{r}p_i^{k_i} \text{ est divisible par } p_{i_0}^2$$

Alors,

$$\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)=0$$

D'où

$$\sum_{\substack{(k_1,\dots,k_r)\in\prod_{i=1}^{r}[\![0,\alpha_i]\!]\\ \exists i_0\in[\![1,r]\!]k_{i_0}\geqslant 2}}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)=0$$

Par suite

$$\sum_{d|n}\mu(d)=\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)$$

Pour tout $(k_1, \ldots, k_r) \in [\![0,1]\!]^r$, on a $\sum_{i=1}^{r} k_i$ est le nombre de facteurs premiers distincts de $\prod_{i=1}^{r} p_i^{k_i}$ et $\prod_{i=1}^{r} p_i^{k_i}$ est non divisible par le carré d'un nombre premier, alors

$$\begin{aligned}\sum_{d|n}\mu(d) &= \sum_{(k_1,\ldots,k_r)\in[\![0,1]\!]^r} (-1)^{\sum_{i=1}^{r} k_i} \\ &= \prod_{i=1}^{r}\left(\sum_{k_1=0}^{1}(-1)^{k_i}\right) \\ &= (1-1)^r \\ &= 0\end{aligned}$$

Théorème 3. (La formule d'inversion de Möbius)

Soit H une fonction non nulle de $\mathbb{N}^*$ dans $\mathbb{C}$ telle que

$$\forall n, m \in \mathbb{N}, H(n.m) = H(n)H(m)$$

On se donne également deux fonctions F et G de$[1, +\infty[$ dans $\mathbb{C}$ telles que, pour tout $x > 1$:

$$G(x) = \sum_{1\leqslant k\leqslant x} F\left(\frac{x}{k}\right) H(k)$$

Alors, pour tout $x > 1$, on a :

$$F(x) = \sum_{1\leqslant k\leqslant x} \mu(k) G\left(\frac{x}{k}\right) H(k)$$

Preuve du théorème 3.

On a

$$H(1) = H(1 \times 1) = H(1)^2$$

Et puisque $H \neq 0$ alors $H(1) = 1$.

Pour tout $x \in [1, +\infty[$, on a :

$$\begin{aligned}
\sum_{1\leqslant k\leqslant x} \mu(k) G\left(\frac{x}{k}\right) H(k) &= \sum_{1\leqslant k\leqslant x} \mu(k) \sum_{1\leqslant i\leqslant \frac{x}{k}} F\left(\frac{x}{i.k}\right) H(i)H(k) \\
&= \sum_{1\leqslant k\leqslant x} \sum_{1\leqslant i\leqslant \frac{x}{k}} \mu(k) F\left(\frac{x}{i.k}\right) H(i.k) \\
&= \sum_{1\leqslant k.i\leqslant x} \mu(k) F\left(\frac{x}{i.k}\right) H(i.k) \\
&= \sum_{1\leqslant m\leqslant x} \sum_{d|m} \mu(d) F\left(\frac{x}{m}\right) H(m) \\
&= \sum_{1\leqslant m\leqslant x} F\left(\frac{x}{m}\right) H(m) \left(\sum_{d|m} \mu(d)\right) \\
&= (x)H(1) + \sum_{2\leqslant m\leqslant x} F\left(\frac{x}{m}\right) H(m) \left(\sum_{d|m} \mu(d)\right)
\end{aligned}$$

D'après la proposition 1, pour tout $m \geqslant 2$, on a :

$$\sum_{d|m} \mu(d) = 0$$

D'où :

$$F(x) = \sum_{1\leqslant k\leqslant x} \mu(k) G\left(\frac{x}{k}\right) H(k)$$

Corollaire 1.

Pour tout entier $n \in \mathbb{N}^*$, on a :

$$\#\mathcal{P}_K(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) (\#K)^d$$

Preuve du corollaire

Soit $n \in \mathbb{N}^*$, notons $\#K = q$. D'après théorème 1, on a :

$$X^{q^n} - X = \prod_{d|n} \prod_{P\in\mathcal{P}_K(d)} P(X)$$

Donc :

$$\begin{aligned}
q^n &= \deg(X^{q^n} - X) \\
&= \sum_{d|n} \sum_{P\in\mathcal{P}_K(d)} \deg(P(X)) \\
&= \deg\left(\prod_{d|n} \prod_{P\in\mathcal{P}_K(d)} P(X)\right)
\end{aligned}$$

Par suite :

$$\sum_{d|n} d.\#\mathcal{P}_K(d) = q^n$$

D'où, d'après la formule d'inversion de Möbius :

$$\#\mathcal{P}_K(n) = \frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)(\#K)^d$$

$\star\star\star\star\star\star\star\star\star$

Pour aller plus loin. On veut trouver le nombre de polynômes irréductibles sur $K[X]$.

On a que le nombre de polynômes irréductibles sur $K[X]$ est :

$$\begin{aligned}\sum_{n=1}^{+\infty}(\#K-1).\#\mathcal{P}_K(n) &= (\#K-1)\sum_{n=1}^{+\infty}\#\mathcal{P}_K(n)\\ &= (\#K-1)\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)(\#K)^d\end{aligned}$$

Pour simplifier l'écriture, on pose $\#K = q$, et on a :

$$\begin{aligned}\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d &= \sum_{n=1}^{+\infty}\sum_{d|n}\frac{1}{n}\mu\left(\frac{n}{d}\right)q^d\\ &= \sum_{n=1}^{+\infty}\sum_{d=1}^{+\infty}\frac{1}{n}\mu\left(\frac{n}{d}\right)1_{\mathbb{N}}\left(\frac{n}{d}\right)q^d\end{aligned}$$

Avec $\mu(r) = 0$ pour les nombres rationnels (on définit simplement un prolongement de μ qui n'a pas d'influence sur le résultat de la somme, puisque $1_{\mathbb{N}}(r) = 0$si r n'est pas entier).

On a alors, d'après le théorème de Fubini et par positivité des termes de la somme :

$$\begin{aligned}\sum_{n=1}^{+\infty}\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d &= \sum_{d=1}^{+\infty}\sum_{n=1}^{+\infty}\frac{1}{n}\mu\left(\frac{n}{d}\right)1_{\mathbb{N}}\left(\frac{n}{d}\right)q^d\\ &= \sum_{d=1}^{+\infty}\sum_{n=1}^{+\infty}\frac{1}{d.n}\mu(n)q^{d.n}\\ &= \sum_{d=1}^{+\infty}\frac{1}{d}\sum_{n=1}^{+\infty}\frac{1}{n}\mu(n)(q^d)^n\end{aligned}$$

Pour tout entier $d \in \mathbb{N}^*$, essayons de calculer la somme de la série $\sum_{n\geqslant 1} \frac{1}{n}\mu(n)(q^d)^n$

Notons pour tout $r \in \mathbb{N}^\star$, p_r le r-ième nombre premier.

On a pour tout $N \in \mathbb{N}^\star$, par définition de la fonction de Möbius :

$$\begin{aligned}
\sum_{n_1=0}^{+\infty}\sum_{n_2=0}^{+\infty}\cdots\sum_{n_N=0}^{+\infty}\frac{1}{\prod_{i=1}^{N} p_i^{n_i}}\mu\left(\prod_{i=1}^{N} p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N} p_i^{n_i}} &= \sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N} p_i^{n_i}}\mu\left(\prod_{i=1}^{N} p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N} p_i^{n_i}} \\
&= \sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N} p_i^{n_i}}(-1)^{\sum_{i=1}^{N} n_i}(q^d)^{\prod_{i=1}^{N} p_i^{n_i}} \\
&= \sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N} (-p_i)^{n_i}}(q^d)^{\prod_{i=1}^{N} p_i^{n_i}}
\end{aligned}$$

Calculons maintenant

$$A_N := \sum_{n_1,\ldots,n_N\in\{0,1\}}\frac{1}{\prod_{i=1}^{N} (-p_i)^{n_i}}(q^d)^{\prod_{i=1}^{N} p_i^{n_i}}$$

Pour tout entier $N \in \mathbb{N}^*$, on a :

$$\begin{aligned}
\sum_{n_N=0}^{1}\frac{1}{\prod_{i=1}^{N}(-p_i)^{n_i}}(q^d)^{\prod_{i=1}^{N} p_i^{n_i}} &= \frac{1}{\prod_{i=1}^{N-1}(-p_i)^{n_i}}\sum_{n_N=0}^{1}\frac{1}{(-p_N)^{n_N}}\left[(q^d)^{\prod_{i=1}^{N-1} p_i^{n_i}}\right]^{n_N} \\
&= \frac{1}{\prod_{i=1}^{N-1}(-p_i)^{n_i}}\left(1-\frac{1}{p_N}(q^d)^{\prod_{i=1}^{N-1} p_i^{n_i}}\right).
\end{aligned}$$

Ainsi,

$$A_N = \sum_{n_1=0}^{1}\cdots\sum_{n_{N-1}=0}^{1}\frac{1}{\prod_{i=1}^{N-1}(-p_i)^{n_i}}\left(1-\frac{1}{p_N}\left(q^d\right)^{\prod_{i=1}^{N-1} p_i^{n_i}}\right).$$

Avec,

$$\begin{aligned}
\sum_{n_1=0}^{1}\cdots\sum_{n_{N-1}=0}^{1}\frac{1}{\prod_{i=1}^{N-1}(-p_i)^{n_i}} &= \prod_{i=1}^{N-1}\left(\sum_{n_i=0}^{1}\frac{1}{(-p_i)^{n_i}}\right) \\
&= \prod_{i=1}^{N-1}\left(1-\frac{1}{p_i}\right)
\end{aligned}$$

On obtient alors

$$\begin{aligned} A_N &= \prod_{i=1}^{N-1}\left(1-\frac{1}{p_i}\right) - \frac{1}{p_N}\sum_{n_1=0}^{1}\cdots\sum_{n_{N-1}=0}^{1}\frac{(q^d)^{\prod_{i=1}^{N-1}p_i^{n_i}}}{\prod_{i=1}^{N-1}(-p_i)^{n_i}} \\ &= \prod_{i=1}^{N-1}\left(1-\frac{1}{p_i}\right) - \frac{1}{p_N}A_{N-1} \end{aligned}$$

Par suite,

$$(-1)^N\left(\prod_{i=1}^{N}p_i\right)A_N - (-1)^{N-1}\left(\prod_{i=1}^{N-1}p_i\right)A_{N-1} = (-1)^N p_N\prod_{i=1}^{N-1}(p_i-1)$$

Par sommation téléscopique, on obtient :

$$(-1)^N\left(\prod_{i=1}^{N}p_i\right)A_N = -p_1A_1 + \sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)$$

Or,

$$\begin{aligned} p_1A_1 &= 2\sum_{n\in\{0,1\}}\frac{1}{(-2)^n}(q^d)^{2^n} \\ &= 2\left(1-\frac{1}{2}(q^d)^2\right) \\ &= 2-q^{2d} \end{aligned}$$

D'où :

$$A_N = \frac{(-1)^N}{\prod_{i=1}^{N}p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)$$

Enfin :

$$\sum_{n_1,\dots,n_N\in\mathbb{N}}\frac{1}{\prod_{i=1}^{N}p_i^{n_i}}\mu\left(\prod_{i=1}^{N}p_i^{n_i}\right)(q^d)^{\prod_{i=1}^{N}p_i^{n_i}} = \frac{(-1)^N}{\prod_{i=1}^{N}p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)$$

Avec :

$$\left|\frac{(-1)^N}{\prod_{i=1}^{N}p_i}(q^{2d}-2)\right| \leqslant \frac{q^{2d}-2}{2^N} \underset{N\to+\infty}{\to} 0$$

Et :

$$\begin{aligned}\left|\frac{(-1)^N}{\prod_{i=1}^{N} p_i}\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right| &\leqslant \sum_{k=2}^{N}\frac{1}{\prod_{i=k+1}^{N} p_i}\prod_{i=1}^{k-1}\left(1-\frac{1}{p_i}\right)\\ &\leqslant \sum_{k=2}^{N}\frac{1}{2^{N-k}}\\ &< 4\\ &< +\infty\end{aligned}$$

Par suite, la limite de :

$$\frac{(-1)^N}{\prod_{i=1}^{N} p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)$$

existe lorsque N tend vers $+\infty$ et est fini.

On a alors

$$\begin{aligned}\#\mathcal{P}_K(n) &= \sum_{d=1}^{+\infty}\frac{1}{d}\left(\lim_{N\to+\infty}\frac{(-1)^N}{\prod_{i=1}^{N} p_i}\left(q^{2d}-2-\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)\right)\\ &= \sum_{d=1}^{+\infty}\frac{1}{d}\left(\lim_{N\to+\infty}\frac{(-1)^{N-1}}{\prod_{i=1}^{N} p_i}\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)\end{aligned}$$

Or,

$$\sum_{d=1}^{+\infty}\frac{1}{d}\left(\lim_{N\to+\infty}\frac{(-1)^{N-1}}{\prod_{i=1}^{N} p_i}\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)\right)=\alpha\sum_{d=1}^{+\infty}\frac{1}{d}=+\infty$$

Avec

$$\alpha=\lim_{N\to+\infty}\frac{(-1)^{N-1}}{\prod_{i=1}^{N} p_i}\sum_{k=2}^{N}(-1)^k p_k\prod_{i=1}^{k-1}(p_i-1)$$

Finalement, on a

$$\sum_{n=1}^{+\infty}(\#K-1).\#\mathcal{P}_K(n)=+\infty$$

Pour n'importe quel corps K commutatif et fini, il existe une infinité de polynômes irréductibles dans $K[X]$.

Corollaire 2.

Pour tout entier $N \in \mathbb{N}^*$, il existe une infinité de polynômes irréductibles sur $K[X]$.

Remarque 1.

On peut éviter tous ces calculs en montrant tout simplement que

$$\#\mathcal{P}_K(n) \underset{n\to+\infty}{\sim} \frac{(\#K)^n}{n}$$

Puisque la série $\sum_{n>0} \frac{(\#K)^n}{n}$ est à terme positifs et divergente, alors

$$\sum_{n=1}^{+\infty} (\#K - 1).\#\mathcal{P}_K(n) = +\infty$$

Sujet 3 : La distribution des puissances d'un nombre dans une base de numération

SABIR Ilyass

⋆ ⋆ ⋆

Objectif. Soient $a, b \geq 2$ deux entiers tels que a est non divisible par b.

Notons

$$\Omega = \{a^k | k \in \mathbb{N}^*\}$$

On considère l'espace probabilisé $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$, où $\mathbb{P}$ est la probabilité

$$\mathbb{P} : I \in \mathcal{P}(\Omega) \longmapsto \lim_{n \to +\infty} \frac{\text{card}(I \cap \Omega_n)}{n} \in [0, 1]$$

Où $\Omega_n = \{a^k / k \in [\![1, n]\!]\}$.

soit X une variable aléatoire réelle définie sur $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ par :

$$X : x \in \Omega \longmapsto \text{le premier chiffre de l'écriture de } x \text{ dans la base } b.$$

On veut calculer $\mathbb{P}(X = i)$ pour tout $i \in [\![1, b-1]\!]$.

Définition 1. (Suite équirépartie). Une suite de réels du segment $[0, 1]$ est dite équirépartie si, pour tout intervalle I inclus dans $[0, 1]$, la probabilité pour qu'un terme de la suite soit dans I est égale à la longueur de I.

Autrement dit, pour une suite de réels $(a_n)_{n \in \mathbb{N}}$ du segment $[0, 1]$, la suite $(a_n)_{n \in \mathbb{N}}$ est dite équirépartie si pour tout $0 \leq a < b \leq 1$

$$\lim_{n \to +\infty} \frac{\text{Card}(\{k \in [\![1, n]\!] | a_k \in [a, b]\})}{n} = b - a$$

Définition 2. (Suite équirépartie modulo 1). Soit $(a_n)_{n \in \mathbb{N}}$ uns suite réelle.

La suite $(a_n)_{n \in \mathbb{N}}$ est dite équirépartie modulo 1 si la suite $(a_n - E(a_n))_{n \in \mathbb{N}}$ est équirépartie.

On fixe a et b, on note pour tout $i \in [\![1, b-1]\!]$ et pour tout $n \in \mathbb{N}^*$, $N_i(n)$ le nombre d'éléments de l'ensemble $\Omega_n = \{a^k | k \in [\![1, b-1]\!]\}$ dont le premier chiffre en base b est i.

Remarquons tout d'abord qu'il existe deux entiers non nuls $(k, c) \in \mathbb{N} \times \mathbb{N}^*$ tels que $a = cb^k$ avec b ne divise pas c. [1]

Puisque a n'est pas une puissance de b, alors $c \geq 2$, et le premier chiffre des puissances de a dans la base b est le même que celui de c. On pourra supposer dans la suite, sans perte de généralité que b ne divise pas a.

Lemme 1. (Critère de Weyl)

Soit $(a_n)_{n\in\mathbb{N}}$ une suite de $[0, 1]$. Les assertions suivantes sont équivalentes :

1. $(a_n)_{n\in\mathbb{N}}$ est équirépartie.
2. Pour toute fonction $f : [0, 1] \to \mathbb{R}$ continue , on a
$$\lim_{n\to+\infty} \frac{1}{n} \sum_{k=1}^{n} f(a_k) = \int_0^1 f(t)dt$$
3. Pour tout $p \in \mathbb{N}^*$, on a
$$\lim_{n\to+\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi p a_k} = 0$$

Preuve du lemme 1.

Notons pour tout $0 \leq a \leq b \leq 1$:

$$X_n(a, b) = Card\{k \in [\![1, n]\!] | a_k \in [a, b]\}$$

$(i) \Rightarrow (ii)$: On a pour tout $0 \leq a \leq b \leq 1$:

$$\frac{X_n(a, b)}{n} = \frac{1}{n} \sum_{k=1}^{n} \chi_{[a,b]}(a_k)$$

où $\chi_{[a,b]}$ désigne la fonction caractéristique du segment $[a, b]$, et que

$$\int_a^b \chi_{[a,b]}(x)dx = b - a$$

1. $k = \max\{j \in \mathbb{N}, b^j \text{divise } a\}$, k existe puisque $\{j \in \mathbb{N} | b^j \text{divise } a\}$ est une partie de $\mathbb{N}$ non vide car contient 0 et majorée.

La propriété (ii) est donc vérifiée pour les fonctions caractéristiques d'un segment. Or, toute fonction f en escalier sur $[0,1]$ est une combinaison linéaire de fonctions caractéristiques de segments (éventuellement réduits à un point pour obtenir les valeurs de f aux points de discontinuité).

Par linéarité, la propriété (ii) est alors vraie pour toute fonction en escalier.

Montrons maintenant que (ii) est vérifiée pour toute fonction continue.

Soit $f : [0,1] \to \mathbb{R}$ une fonction continue et $\varepsilon > 0$. On sait qu'on peut trouver une fonction en escalier g qui approche f uniformément à ε près sur $[0,1]$, c'est-à-dire telle que $\|f - g\|_\infty \leq \varepsilon$. Grâce à l'inégalité triangulaire, pour tout $n \geq 1$, on peut majorer

$$\left| \frac{1}{n} \sum_{k=1}^{n} f(a_k) - \int_0^1 f(x)dx \right|$$

par :

$$\left| \frac{1}{n} \sum_{k=1}^{n} (f(a_k) - g(a_k)) \right| + \left| \frac{1}{n} \sum_{k=1}^{n} g(a_k) - \int_0^1 g(x)\,dx \right| + \left| \int_0^1 g(x)\,dx - \int_0^1 f(x)\,dx \right|$$

avec

$$\left| \frac{1}{n} \sum_{k=1}^{n} (f(a_k) - g(a_k)) \right| \leq \varepsilon \text{ and } \left| \int_0^1 g(x)dx - \int_0^1 f(x)dx \right| \leq \varepsilon$$

Pour le deuxième terme, comme la fonction g est en escalier, ce terme devient inférieur à ε à partir d'un certain rang N.

Bref, pour tout entier $n \geq N$

$$\left| \frac{1}{n} \sum_{k=1}^{n} f(a_k) - \int_0^1 f(x)dx \right| \leq 3\varepsilon$$

Ce qui prouve (ii).

Montrons réciproquement que $(ii) \Rightarrow (i)$.

Une fonction caractéristique d'un segment I (distinct de $[0,1]$) présente au moins une discontinuité, donc elle ne peut pas être obtenue comme limite uniforme d'une suite de fonctions continues. En fait, on n'a pas besoin d'une approximation uniforme : il suffit d'encadrer χ_I par deux suites de fonctions

continues affines par morceaux qui convergent vers χ_I au sens de la norme intégrale.

Prenons pour commencer un segment $I = [\alpha, \beta]$ avec $0 < \alpha < \beta < 1$.

On considère les suites de fonctions continues définies pour tout $k \in \mathbb{N}^*$ suffisamment grand par : φ_k est nulle sur les segments $[0, \alpha]$ et $[\beta, 1]$, vaut 1 sur le segment $\left[\alpha + \frac{1}{k}, \beta - \frac{1}{k}\right]$, et est affine sur les deux segments qui restent, et ψ_k est nulle sur les segments $\left[0, \alpha - \frac{1}{k}\right]$ et $\left[\beta + \frac{1}{k}, 1\right]$, vaut 1 sur le segment $[\alpha, \beta]$, et est affine sur les deux segments qui restent.

On observe que, pour tout p assez grand,

$$\varphi_p \leq \chi_I \leq \psi_p$$

Il en résulte que, pour tout n assez grand,

$$\frac{1}{n}\sum_{k=1}^{n} \varphi_p(a_k) \leq \frac{\chi_n(\alpha, \beta)}{n} \leq \frac{1}{n}\sum_{k=1}^{n} \psi_p(a_k)$$

Par hypothèse :

$$\begin{aligned} \lim_{n\to+\infty} \frac{1}{n}\sum_{k=1}^{n} \varphi_p(a_k) &= \int_0^1 \varphi_p(x)dx \\ &= \beta - \alpha - \frac{1}{p} \end{aligned}$$

et

$$\begin{aligned} \lim_{n\to+\infty} \frac{1}{n}\sum_{k=1}^{n} \psi_p(a_k) &= \int_0^1 \psi_p(x)dx \\ &= \beta - \alpha + \frac{1}{p} \end{aligned}$$

Soit $\varepsilon > 0$. Choisissons p tel que $\frac{1}{p} < \varepsilon$. Il existe N tel que pour $n \geq N$

$$\left|\frac{\chi_n(\alpha, \beta)}{n} - (\beta - \alpha)\right| \leq 2\varepsilon$$

Ainsi, $\left(\frac{\chi_n(\alpha,\beta)}{n}\right)_{n\geq 1}$ converge vers $\beta - \alpha$, lorsque $0 < \alpha < \beta < 1$. Il est aisé d'adapter cela lorsque $\alpha = 0$ ou $\beta = 1$.

(iii) $\Rightarrow$ **(i)** résulte directement de (ii) puisque pour tout $p \in \mathbb{N}^*$:

$$\begin{aligned} \lim_{n\to+\infty} \frac{1}{n}\sum_{k=1}^{n} e^{2i\pi p a_k} &= \int_0^1 \cos(2\pi p x) + i\int_0^1 \sin(2\pi p x) \\ &= 0 \end{aligned}$$

Montrons enfin que **(iii) ⇒ (ii)**

Par linéarité, on a la propriété (ii) pour tous les polynômes trigonométriques du type

$$x \longmapsto c_0 + \sum_{k=1}^{n} (c_k \cos(2k\pi x) + d_k \sin(2k\pi x))$$

D'après le théorème de Weierstrass trigonométrique, toute fonction continue $f : [0,1] \to \mathbb{R}$ vérifiant $f(0) = f(1)$ est limite uniforme d'une suite de polynômes trigonométriques de ce type. Comme précédemment, on en déduit que (ii) est vérifiée pour une telle fonction g vérifiant

$$g(0) = g(1) \text{ et } \int_0^1 |f(x) - g(x)|dx \leq \varepsilon$$

Comme dans l'implication $(ii) \Rightarrow (i)$, cela suffit pour prouver que (ii) est aussi vraie pour f.

D'où les propositions (i), (ii) et (iii) sont toutes équivalentes.

Lemme 2.

Soit $\theta > 0$. Alors la suite $(n\theta)_{n\in\mathbb{N}^*}$ est équirépartie modulo 1 si et seulement si $\theta \notin \mathbb{Q}$.

Preuve du lemme 2.

Par définition d'une suite équirépartie modulo 1, la suite $(a_n)_{n\in N^*} = (n\theta)_{n\in N^*}$ est équirépartie modulo 1 si et seulement si la suite $(a_n - E(a_n))_{n\in N^*}$ est équirépartie.

Comme les fonctions $\varphi_k : x \to e^{2ik\pi x}$ sont toutes 1-périodiques pour tout entier non nul k, alors on a encore l'équivalence suivante :

La suite $(a_n)_{n\in\mathbb{N}^*} = (n.\theta)_{n\in\mathbb{N}^*}$ est équirépartie modulo 1 si et seulement si pour tout $k \in \mathbb{N}^*$

$$\lim_{n\to+\infty} \frac{1}{n} \sum_{j=1}^{n} \varphi_k(a_j) = 0$$

Supposons que $\theta \notin \mathbb{Q}$. On a donc $\varphi_k(\theta) \neq 1$. Par suite, pour tous entiers

k et n non nuls :

$$\begin{aligned}\frac{1}{n}\sum_{j=1}^{n}\varphi_k(a_j) &= \frac{1}{n}\sum_{j=1}^{n}\varphi_k(j.\theta)\\ &= \frac{1}{n}\sum_{j=1}^{n}\varphi_k(\theta)^j\\ &= \frac{\varphi_k(\theta)}{n}\frac{\varphi_k(\theta)^n-1}{\varphi_k(\theta)-1}\end{aligned}$$

Comme pour tout $k, n \in \mathbb{N}^*$, on a

$$\left|\frac{\varphi_k(\theta)}{n}\frac{\varphi_k(\theta)^n-1}{\varphi_k(\theta)-1}\right| \leq \frac{2|\varphi_k(\theta)|}{n|\varphi_k(\theta)-1|} \xrightarrow[n\to+\infty]{} 0$$

Alors la suite $(a_n)_{n\in\mathbb{N}^*} = (n.\theta)_{n\in\mathbb{N}^*}$ est équirépartie modulo 1.

Supposons que $\theta \in \mathbb{Q}$, alors il existe $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que

$$\theta = \frac{a}{b}$$

On pose

$$(x_n)_{n\in\mathbb{N}^*} := (a_n - E(a_n))_{n\in\mathbb{N}^*}$$

On a pour tout $n, q \in \mathbb{N}^*$:

$$\begin{aligned}x_{n+b} &= (n+b).\theta - E((n+b)\frac{a}{b})\\ &= n.\theta - E(n.\frac{a}{b})\\ &= x_n\end{aligned}$$

Donc $(x_n)_{n\in\mathbb{N}^*}$est b-périodique , En posant

$$r = \min_{0\leqslant i\leqslant b-1}(x_i) \leq 1$$

Il n'existe aucun élément de la suitet $(x_n)_{n\in\mathbb{N}^*}$ dans $]0, r[$, donc le suite $(x_n)_{n\in\mathbb{N}^*}$ n'est pas équirépartie, d'où l'équivalence.

Revenons à notre question. Soient $i \in [\![1, b-1]\!]$ et $k \in \mathbb{N}^*$. Commençons par traduire le fait que i est le premier chiffre de a^k en base b.

Dans toute la suite, nous travaillons dans la base de numération b.

L'entier a^k commence par i si et seulement s'il existe $n \in \mathbb{N}$ tel que

$$i.b^n \leq a^k < (i+1).b^n$$

C'est-à-dire, si et seulement s'il existe un entier n tel que :

$$\frac{\ln i}{\ln b} + n \leq k\frac{\ln a}{\ln b} < \frac{\ln(i+1)}{\ln b} + n$$

Cela se traduit encore par : l'entier a^k commence par i si et seulement s'il existe $k \in \mathbb{N}$ tel que le résidu modulo 1 de $k\frac{\ln a}{\ln b}$ soit dans l'intervalle $\left[\frac{\ln i}{\ln b}, \frac{\ln(i+1)}{\ln b}\right[$.

On pose

$$\theta = \frac{\ln a}{\ln b}$$

On a alors, pour tout entier p non nul, $N_i(p)$ est exactement le nombre d'entiers $k \in [\![1, p]\!]$ tels que $k.\theta$ modulo 1 appartienne à $\left[\frac{\ln i}{\ln b}, \frac{\ln(i+1)}{\ln b}\right[$.

Or, si a divise b, alors il existe $r, c \in \mathbb{N}^*$ tels que $b = a^r \cdot c$ et c ne divise pas b. On a alors :

$$\frac{\ln b}{\ln a} = r + \frac{\ln c}{\ln a}$$

Donc

$$\frac{\ln(a)}{\ln(b)} \in \mathbb{Q} \,\text{si and seulement si}\, \frac{\ln(c)}{\ln(a)} \in \mathbb{Q}$$

Ainsi, pour montrer que $\frac{\ln(a)}{\ln(b)} \notin \mathbb{Q}$, il suffit de montrer que $\frac{\ln(c)}{\ln(a)} \notin \mathbb{Q}$. Alors, on pourra supposer ici sans perte de généralité que b ne divise pas a et a ne divise pas b.

Montrons par l'absurde que $\theta = \frac{\ln(a)}{\ln(b)} \notin \mathbb{Q}$. Si ce n'est pas le cas, il existe un couple $(u, v) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que :

$$\frac{\ln(a)}{\ln(b)} = \frac{u}{v}$$

alors

$$a^v = b^u$$

Écrivons :

$$a = \prod_{i=1}^{r} p_i^{\alpha_i} \quad \text{et} \quad b = \prod_{i=1}^{r} p_i^{\beta_i}$$

où $p_1, \ldots, p_r$ sont des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_r \in \mathbb{N}$.

Par suite :

$$a^v = \prod_{i=1}^{r} p_i^{v\alpha_i} \quad \text{et} \quad b^u = \prod_{i=1}^{r} p_i^{u\beta_i}$$

Par l'unicité de la décomposition en produit de facteurs premiers, on a pour tout $k \in [\![1, r]\!]$,

$$u\alpha_k = v\beta_k$$

Or, comme b ne divise pas a, alors il existe $i_0 \in [\![1, r]\!]$ tel que $\alpha_{i_0} < \beta_{i_0}$. De même a ne divise pas b, alors il existe $j_0 \in [\![1, r]\!]$ tel que $\beta_{j_0} < \alpha_{j_0}$.

D'une part :

$$u\alpha_{i_0} = v\beta_{i_0} < u\beta_{i_0}$$

Donc $v < u$.

D'autre part :

$$u\alpha_{j_0} = v\beta_{j_0} < v\alpha_{j_0}$$

Donc $u < v$.

Ainsi, $u < v$ et $v < u$, ce qui est absurde.

Donc

$$\theta = \frac{\ln(a)}{\ln(b)} \notin \mathbb{Q}$$

D'après le lemme 2, on a donc la suite $(k.\theta)_{k\in\mathbb{N}}$ est équirépartie modulo 1, alors :

$$\begin{aligned} \mathbb{P}(X = i) &= \lim_{n\to+\infty} \frac{N_i(n)}{n} \\ &= \frac{\ln(i+1) - \ln(i)}{\ln(b)} \end{aligned}$$

Remarques et commentaires. 1. On remarque tout d'abord que l'expression de $\mathbb{P}(X = i)$ est indépendante de a, c'est-à-dire que, dans n'importe quelle base b, la répartition des puissances des nombres entiers non divisibles par b suit les mêmes fréquences d'apparition des chiffres en première position.

2. La probabilité décroît en fonction de i, ce qui signifie que l'apparition du chiffre 1 en première position est la plus fréquente. En effet, dans la base

10, la fréquence d'apparition du chiffre 1 en première position dans la suite des puissances d'un nombre non divisible par 10 est approximativement de 30,1 %. On donne ci-dessous un tableau indiquant la probabilité d'apparition des chiffres 1, 2, ..., 9 dans les puissances d'un entier non divisible par 10 en base décimale :

i	1	2	3	4	5	6	7	8	9
$\mathbb{P}(X=i)$	30.1%	17.6%	12.46%	9.69%	7.91%	6.69%	5.79%	5.11%	4.57%

3. Remarquons aussi que pour tout $i \in [\![1, b-1]\!]$, on a :

$$\mathbb{P}(X=i) = \frac{\ln(i+1) - \ln(i)}{\ln(b)} > 0$$

Ainsi, pour tout $i \in [\![1, b-1]\!]$, il existe une infinité de puissances de a dont le développement b-adique commence par i.

On donnera une autre preuve de ce résultat.

Fixons $i \in [\![1, b-1]\!]$. Pour montrer le résultat, il suffit de démontrer qu'il existe une infinité de couple $(n,k) \in \mathbb{N}^2$ tels que

$$i \leq \frac{a^n}{b^k} < i+1$$

Cela revient à trouver une infinité de couples $(n,k) \in \mathbb{N}^2$ tels que

$$\ln(i) \leq n\ln(a) - k\ln(b) < \ln(i+1)$$

Le résultat est prouvé grâce à la densité de $\frac{\ln(a)}{\ln(b)}\mathbb{N} + \mathbb{Z}$, car $\frac{\ln(a)}{\ln(b)} \notin \mathbb{Q}$.

C'est ce que nous allons montrer dans les deux lemmes suivants :

Lemme 3. (Sous-groupes additifs de $\mathbb{R}$)

Soit G un sous-groupe de $(\mathbb{R}, +)$ non réduit à $\{0\}$. Alors G est soit dense dans $\mathbb{R}$, soit de la forme $a\mathbb{Z}$ avec $a > 0$.

Preuve du lemme 3.

le raisonnement est basé sur la borne inférieure de $\mathbb{R}_*^+ \cap G$.

Comme G est non réduit à $\{0\}$, alors il existe $x \neq 0$ tel que $x \in G$. Puisque G est un groupe, on a aussi $-x \in G$, donc $|x| \in G$.

Par conséquent, $\mathbb{R}_*^+ \cap G \neq \emptyset$. Cette partie est minorée par 0, donc d'après l'axiome de la borne inférieure, on a l'existence de $r = \inf \mathbb{R}_*^+ \cap G$.

$\rightarrow$ **Si** $r > 0$, montrons que $r \in G$ par l'absurde.

Supposons que r ne soit pas dans G. Comme $r > 0$, d'après la caractérisation de la borne inférieure, il existe $x \in R_*^+ \cap G$ tel que

$$r < x < 2r$$

Puisque $x - r > 0$, il existe aussi $y \in R_*^+ \cap G$ tel que , donc on a $r < y < x < 2r$r <y <x <2r.
Or, $0 < x - y < r0$ <x y <r, ce qui implique que $x - y \in R_*^+ \cap G$

$$r < y < r + (x - r) = x$$

Donc,

$$r < y < x < 2r$$

Or, $0 < x - y < r$, ce qui implique que $x - y \in R_*^+ \cap G$ et $x - y < r$, contradiction.

Donc, $r \in G$.

Par stabilité de la somme dans G, on a $r\mathbb{Z} \subseteq G$.

Réciproquement, soit $x \in G$. Posons $k = \lfloor x/r \rfloor$. Comme G est un groupe, le réel $x - k \cdot r \in G$, et comme $k \leq x/r < k + 1$, alors $0 \leq x - k \cdot r < r$. Nécessairement, $x - k \cdot r = 0$, c'est-à-dire $x = k \cdot r \in r\mathbb{Z}$.

$\rightarrow$ **Si** $r = 0$**,** on va montrer que G est dense dans $\mathbb{R}$. Pour cela, soient $a < b$ dans $\mathbb{R}$.

Comme $r = 0$, par la caractérisation de la borne inférieure, on a l'existence de $x \in \mathbb{R}_*^+ \cap G$ tel que $0 < x < b - a$.

On note

$$C_{b,a} = \{k \in \mathbb{N} | kx < b\}$$

Il est clair que $C_{b,a}$ est une partie non vide de $\mathbb{N}$ et majorée, donc elle admet un plus grand élément que l'on note n_0.

Comme l'entier $n_0 + 1 \notin C_{b,a}$ et $n_0 \in C_{b,a}$, alors

$$(n_0 + 1)x \geq b \text{ and } n_0 x < b$$

Par suite,

$$a < b - x \leq n_0 x < b$$

D'où $]a, b[\cap G \neq \varnothing$, c'est-à-dire que G est dense dans $\mathbb{R}$. Le lemme est prouvé.

Lemme 4.

Soit θ un irrationnel, alors $\theta\mathbb{N} + \mathbb{Z}$ est dense dans $\mathbb{R}$.

Preuve du lemme 4.

on a $\theta\mathbb{Z}+\mathbb{Z}$ est un sous-groupe additif de $\mathbb{R}$. D'après le lemme précédent, on a $\theta\mathbb{Z} + \mathbb{Z}$ est soit dense dans $\mathbb{R}$, soit de la forme $a\mathbb{Z}$ avec $a > 0$ (en effet, $a > 0$ car $\theta\mathbb{Z} + \mathbb{Z}$ n'est pas réduit à $\{0\}$).

Supposons qu'il existe $a > 0$, tel que

$$\theta\mathbb{Z} + \mathbb{Z} = a\mathbb{Z}$$

Comme $1, \theta \in \theta\mathbb{Z}+\mathbb{Z} = a\mathbb{Z}$, alors il existe $(u, v) \in \mathbb{N}^* \times \mathbb{Z}$ tel que $1 = u.a$ et $\theta = v.a$

Ainsi, $\theta = \frac{v}{u} \in \mathbb{Q}$, ce qui est absurde. Donc $\theta\mathbb{Z} + \mathbb{Z}$ est dense dans $\mathbb{R}$.

Montrons maintenant que l'ensemble $\theta\mathbb{N} + \mathbb{Z}$ reste dense dans $\mathbb{R}$. Soient $a < b$ dans $\mathbb{R}$. On a l'existence de $x = n\theta + m \in \theta\mathbb{Z}+\mathbb{Z}$ tel que $0 < x < b-a$.

Si n est un entier naturel, soit m_0 le plus grand entier strictement inférieur à a. La suite $(kx + m_0)_{k\in\mathbb{N}}$ rencontre nécessairement l'intervalle $]a, b[$, puisqu'il s'agit d'une suite arithmétique de raison $x < b - a$. Il existe donc dans ce cas un élément de $\theta\mathbb{N} + \mathbb{Z}$ dans $]a, b[$.

Si $m < 0$, alors $-x \in \theta\mathbb{N} + \mathbb{Z}$. Soit m_0 un entier strictement supérieur à b. Il existe au moins un élément de la suite $(m_0 - k.x)_{k\in\mathbb{N}}$ qui appartient à $]a, b[$.

4. Pour un nombre a puissance de b, les puissances de a sont aussi des puissances de b, Ainsi, le premier chiffre des puissances de a est toujours égal à 1 dans la base b.

5. La répartition des chiffres en fonction des fréquences reste complexe à comprendre, notamment dans la base décimale. Par exemple, le dernier chiffre d'un nombre pair ne peut pas être impair. De plus, la suite des derniers chiffres des puissances d'un entier k est périodique : elle a une période de 1 si k est divisible par 10, et une période de 4 si k est pair mais non divisible par 10. On peut le démontrer aisément, puisque $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 6$, et $2^5 = 2$, bouclant ainsi la période.

Si k est impair, on peut discuter des différents cas possibles de manière analogue. En général, l'étude du comportement du dernier chiffre dans une base de numération b se réduit aux nombres $0, 1, \ldots, b-1$. Cependant, pour l'avant-dernier chiffre, les choses deviennent plus complexes. En base décimale, par exemple, pour qu'un nombre soit divisible par 25, il doit se terminer par l'un des couples de chiffres suivants : 00, 25, 50 ou 75. Or, les puissances de 5 ne sont pas divisibles par 100 (car aucune puissance de 5 n'est divisible par 2).

On peut étudier les variations de chaque chiffre à une position donnée dans les puissances d'un nombre spécifique dans une base déterminée. Par exemple, il serait possible d'examiner les variations du chiffre en cinquième position à gauche dans les puissances de 7 en base décimale. Cependant, cette analyse reste complexe.

6. La probabilité donnée dans est caractéristique de la fréquence de la distribution des puissances jusqu'à l'infini. En effet, il est impossible de trouver une partie finie non vide $I \subset \mathbb{N}$ et un entier $i^* \in [\![1, b-1]\!]$ tels que

$$\frac{\mathrm{Card}(\{k \in I \mid i \text{ est le premier chiffre de } a^k \text{ dans la base } b\})}{\mathrm{Card}(I)} = \mathbb{P}(X = i) = \frac{\ln(i+1) - \ln(i)}{\ln(b)}$$

Car sinon, on aurait

$$\frac{\ln(i+1) - \ln(i)}{\ln(b)} \in \mathbb{Q}.$$

Donc il existerait $(u, v) \in (\mathbb{N}^*)^2$ tels que

$$(i+1)^u = i^v \cdot b^v.$$

Comme $\gcd(i, i+1) = 1$, il en découlerait que b divise $i+1$, donc forcément $i = b - 1$. Cependant,

$$(b-1)^v = b^{u-v},$$

absurde !

Sujet 4 : Le théorème de Dirichlet

Le théorème de la progression arithmétique.

SABIR Ilyass

⋆⋆⋆

Introduction. On va présenter ici un résultat fondamental concernant les nombres premiers. Selon le théorème d'Euclide, les nombres premiers sont infinie, un fait dont la démonstration est relativement simple (la preuve de ce théorème ne sera cependant pas donnée ici ; pour ceux qui souhaiteraient en savoir plus, une démonstration est disponible sur le site suivant : Cantor's Paradise).

L'une des questions les plus profondes en mathématiques est celle de la répartition des nombres premiers parmi les entiers. Bien que les mathématiques aient considérablement progressé, la distribution des nombres premiers reste mystérieuse et pose de nombreux défis non résolus, comme la conjecture de Goldbach ou l'hypothèse de Riemann sur la fonction Zêta.

Cela ne signifie pas pour autant qu'il n'existe aucun résultat sur la distribution des nombres premiers. Au contraire, certains résultats remarquables fournissent des réponses partielles à cette question complexe. Parmi eux figure le théorème de Dirichlet, un des plus beaux résultats sur les nombres premiers, qui énonce que pour tout $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ premiers entre eux, il existe une infinité de nombres premiers de la forme $an + b$.

L'étude des nombres premiers et de leur distribution est ainsi cruciale, non seulement pour l'avancement des mathématiques, mais aussi pour des domaines comme l'informatique et la physique.

L'objectif principal. On veut montrer le résultat suivant :

Pour tout $(a, b) \in \mathbb{N}^* \times \mathbb{N}^*$ premiers entre eux, on a une infinité de nombres premiers qui s'écrivent sous la forme : $an + b$.

Remarque.

Soit $(a, b) \in \mathbb{N}^\star \times \mathbb{N}^\star$, si a et b ne sont pas premiers entre eux (c'est-à-dire si $a \wedge b > 1$), alors pour tout entier $n \in \mathbb{N}$ on a :

$$a.n + b = a \wedge b \left(\frac{a}{a \wedge b} n + \frac{b}{a \wedge b} \right)$$

Donc, par définition d'un nombre premier, on peut trouver au plus un nombre permier de la forme $a.n + b = a \wedge b \left(\frac{a}{a \wedge b} n + \frac{b}{a \wedge b} \right)$

On en déduit que la condition a et b sont premiers entre eux est une condition nécessaire pour que le résultat soit vrai. On va montrer sans la suite que cette condition est suffisante.

Quelques exemples et premiers résultats. Avant de commencer la démonstration de notre théorème principal, nous allons d'abord voir quelques exemples qui montrent la validité de ce théorème pour des cas particuliers.

Exemple 1. On sait, d'après le lemme d'Euclide, qu'il existe une infinité de nombres premiers. Puisque les nombres premiers sont tous impairs, sauf 2, il existe donc une infinité de nombres premiers de la forme $2n + 1$, avec $n \in \mathbb{N}$.

Question 1.

Existe-il une infinité de nombres premiers congrus à 3 modulo 4 ?

Réponse.

Raisonnons par l'absurde, et supposons qu'il n'en existe qu'un nombre fini n. Notons-les $p_1, \ldots, p_n$, et considérons l'entier

$$N = 4.p_1 \ldots p_n - 1 \geqslant 2$$

Aucun des p_k ne divise N, puisque N est impair et que ses diviseurs premiers ne sont pas dans l'ensemble $\{p_1, \ldots, p_n\}$. Par conséquent, ils ne sont pas congrus à 3 modulo 4. Par imparité et par primabilité, tous les diviseurs premiers de N sont congus à 1 modulo 4, et donc N est congru à 1 modulo 4. Or, manifestement, N est congru à 3 modulo 4, ce qui est contradictoire.

De la même manière, on peut montrer qu'il existe une infinité de nombre premiers de la forme $4n + 1$, et bien d'autres encore...

Pasons une question plus forte :

Question 2.

Existe-il une infinité de nombres premiers de la forme $3n + 1$, et une infinité de nombres premiers de la forme $4n + 15$, ainsi qu'une infinité de nombres premiers de la forme $5n + 1$... ?

De manière générale, pour un entier $\lambda \in \mathbb{N}^*$, Existe-t-il une infinité de nombres premiers de la forme $\lambda n + 1$?

Réponse.

En nous basant sur une méthode due à Leonard Euler, qui a utilisé les polynômes cyclotomiques pour montrer ce résultat.

Commençons par définir les polynômes cyclotomiques :

Définition 1. Soit $n \in \mathbb{N}^*$. On définit le n-ième polynôme cyclotomique par :

$$\Phi_n = \prod_{\substack{1 \leqslant k \leqslant n \\ k \wedge n = 1}} \left(X - e^{\frac{2i.k\pi}{n}} \right)$$

Théorème 1. Pour tout $n \in \mathbb{N}^\star$, on a : $\Phi_n \in \mathbb{Z}[X]$

Preuve du théorème 1. Soit $n \in \mathbb{N}^\star$. Montrons d'abord que

$$X^n - 1 = \prod_{d|n} \Phi_d$$

. On sait que :

$$X^n - 1 = \prod_{l=1}^{n} \left(X - e^{\frac{2i.k\pi}{n}} \right)$$

Notons, pour tout entier $d \geqslant 1$, R_d l'ensemble des racines primitives d-ièmes de l'unité et $\mathbb{U}_d$ l'ensemble des racines d-ièmes de l'unité.

On a, par définition :

$$\Phi_n = \prod_{\xi \in R_n} (X - \xi)$$

Si $\xi \in \mathbb{U}_n$, l'ordre de ξ est un diviseur d de n, et alors $\xi \in R_d$. Par conséquent, $\mathbb{U}_n$ est une réunion disjointe des R_d pour $d|n$. S'où il résulte :

$$\begin{aligned} X^n - 1 &= \prod_{\xi \in R_n} (X - \xi) \\ &= \prod_{d|n} \left(\prod_{\xi \in R_d} (X - \xi) \right) \\ &= \prod_{d|n} \Phi_d \end{aligned}$$

Nous allons établir que Φ_n est à coefficients entiers par récurrence sur $n \geqslant 1$ en utilisant le résultat suivant :

Lemme 1. Soient A et B deux polynômes à coefficients entiers, B étant non nul et unitaire. Alors Q et R, le quotient et le reste de la division euclidienne de A par B dans $\mathbb{C}[X]$, sont aussi à coefficients entiers.

Preuve du lemme 1. La division euclidienne est invariante par extension de corps, alors $Q, R \in \mathbb{Q}[X]$.

On a :

$$A = B.Q + R$$

On définit l'application $\mathcal{C} : \mathbb{Z}[X] \to \mathbb{Z}$ pour tout $P = \sum_{n=0}^{N} a_n X^n \in \mathbb{Z}[X]$ par :

$$\mathcal{C}(P) = \bigwedge_{n=0}^{N} a_n$$

Pour $P = \sum_{n=0}^{N} a_n X^n$ et $Q = \sum_{n=0}^{M} b_n X^n \in \mathbb{Z}[X]$, par définition de $\mathcal{C}$, on a

$$\frac{P}{\mathcal{C}(P)}, \frac{Q}{\mathcal{C}(Q)} \in \mathbb{Z}[X]$$

et les coefficients de $\frac{P}{\mathcal{C}(P)}$ (resp. de $\frac{Q}{\mathcal{C}(Q)}$) sont premiers entre eux.

Pour tout entier premier p, p ne divise pas tous les coefficients de $\frac{P}{\mathcal{C}(P)}$ (resp. de $\frac{Q}{\mathcal{C}(Q)}$), donc dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a $\frac{P}{\mathcal{C}(P)} \neq 0$ et $\frac{Q}{\mathcal{C}(Q)} \neq 0$.

Or, $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc l'anneau $\mathbb{Z}/p\mathbb{Z}[X]$ est int è gre. Par conséquent, dans $\mathbb{Z}/p\mathbb{Z}[X]$ on a

$$\frac{P}{\mathcal{C}(P)} \times \frac{Q}{\mathcal{C}(Q)} \neq 0$$

Ainsi, $p$ne divise pas tous les coefficients de $\frac{P}{\mathcal{C}(P)} \times \frac{Q}{\mathcal{C}(Q)}$, et donc p ne divise pas $\mathcal{C}\left(\frac{P}{\mathcal{C}(P)} \times \frac{Q}{\mathcal{C}(Q)}\right)$, et ça pour tout nombre premier p.

Alors,

$$\mathcal{C}\left(\frac{P}{\mathcal{C}(P)} \times \frac{Q}{\mathcal{C}(Q)}\right) = 1$$

Par suite

$$\mathcal{C}(P.Q) = \mathcal{C}(P)\mathcal{C}(Q)$$

Soit $b \in \mathbb{N}^*$ un entier tel que $b.Q, b.R \in \mathbb{Z}[X]$. On a alors :

$$b.A = (b.Q)B + b.R$$

Donc

$$\begin{aligned} \mathcal{C}(b.A - b.R) &= \mathcal{C}(B)\mathcal{C}(b.Q) \\ &= \mathcal{C}(b.Q) \end{aligned}$$

Comme B et A sont unitaires, alors Q est aussi unitaire, donc le coefficient dominant de $b.Q$ est b, en particulier, $\mathcal{C}(b.Q)|b$, donc $\frac{b}{\mathcal{C}(b.Q)} \in \mathbb{N}$.

De même, on montre que $b|\mathcal{C}(b.Q)$, donc $\mathcal{C}(b.Q) = b$.

Ainsi,

$$Q = \frac{b.Q}{\mathcal{C}(b.Q)} \in \mathbb{Z}[X]$$

Par suite

$$R = A - B.Q \in \mathbb{Z}[X]$$

D'où le résultat.

Établissons maintenant par récurrence sur n que Φ_n est à coefficients entiers.

1. C'est vrai pour $n = 1$ (par définition).

2. Si $n \geqslant 2$, Φ_n est le quotient dans $\mathbb{C}[x]$ de $X^n - 1$ par B, où B est égal au produit des Φ_d, où d est un diviseur strict de n.

Si on suppose la propriété vraie pour les entiers inférieurs ou égaux à $n-1$, chacun de ces Φ_d est à coefficients entièrs et unitaire par définition. Donc, B est aussi à coefficients entiers et unitaire. En vertu du lemme 1, Φ_n est à coefficients entiers.

Soit p un nombre premier qui divise $\Phi_n(a)$, où $a \in \mathbb{Z}$, mais ne divise aucun $\Phi_d(a)$, où d parcourt l'ensemble des diviseur stricts de n.

Soit $a \in \mathbb{Z}$. Comme p divise $\Phi_n(a)$, il divise aussi $a^n - 1$. Ainsi, l'ordre de $\overline{a}$dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ divise n.

Montrons que cet ordre est exactement n. Si $d < n$, on a dans $\mathbb{Z}/p\mathbb{Z}$

$$\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}$$

Or, si d' divise d, alors d' divise aussi n et par hypothèse sur p,

$$\overline{\Phi_{d'}(a)} \neq 0$$

Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le produit de ces éléments non nuls est également non nul, si bien que $\overline{a}^d \neq 1$.

L'ordre de $\overline{a}$ est donc n. Comme cet ordre divise $p-1$ d'après le théorème de Lagrange, p est de la forme $\lambda n + 1$ avec $\lambda \in \mathbb{N}$.

Montrons maintenant que pour $n \geqslant 1$ fixé, il existe une infinité de nombres premiers de la forme $\lambda n + 1$ avec $\lambda \in \mathbb{N}$.

Raisonnons par l'absurde et supposons qu'il existe un nombre fini d'entiers premiers congrus à 1 modulo n, soient $p_1, \dots, p_q$.

Si on arrive à trouver a et p vérifiant les hypothèses, assure que p est congru à 1 modulo n. Cela sera insuffisant pour aboutir à une contradiction, p pouvant être alors un des p_i.

Pour éviter cela, changeons n en $N = n.p_1 \dots p_q$.

Si p est congru à 1 modulo N, p ne peut être un des $p_i$et pourtant, il est congru à 1 modulo n.

Il faut donc trouver $a \in \mathbb{Z}$ et p premier, tels que p divise $\Phi_N(a)$, mais aucun des $\Phi_d(a)$, pour $d|N, d < N$.

On note

$$B = \prod_{d|N, d<N} \Phi_d$$

Le problème est donc de trouver $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_N(a)$,et ne divise pas $B(a)$.

Puisque les deux polynômes B et Φ_N sont scindés sur $\mathbb{C}$ et n'ont aucune racine commune, alors ils sont premiers entre eux dans $\mathbb{C}[X]$, donc aussi dans $\mathbb{Q}[X]$, puisque ces polynômes sont à coefficients rationnels et que le pgcd est invariant par extension de corps.

D'après le théorème de Bezout, il existe donc un couple $(U, V) \in \mathbb{Q}[X]^2$ tel que

$$U\Phi_N + VB = 1$$

Il existe $a \in \mathbb{Z}$ tel que $U' = a.U$ et $V' = a.V$ appartient à $\mathbb{Z}[X]$.

Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$, on peut même choisir a tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$, étant donné l'infinité de $a \in \mathbb{Z}$ vérifiant $a.U \in \mathbb{Z}[X]$ et $a.V \in \mathbb{Z}[X]$.

On a donc

$$a = U'\Phi_N + V'B$$

et en particulier $a = U'(a)\Phi_N(a) + V'(a)B(a)$ $(\star)$

Soit $p$un nombre premier divisant $\Phi_N(a)$. Alors p divise $a^N - 1$, car Φ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$. Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$, et donc $\overline{a}$ est inversible, ce qui signifie que a est premier avec p.

Si p divise $B(a)$, il diviserait a, d'après $(\star)$, ce qui est exclu. On est donc dans les hypothèses : p est congru à 1 modulo N, et donc modulo n, avec p forcément distinct des p_i, pour $1 \leqslant i \leqslant q$, C'est la contradiction voulue.

Le premier théorème de Mertens. Commençons par démontrer le théorème de Legendre :

Théorème 2. (Théorème de Legendre) Soit $n \in \mathbb{N}^*$, Pour tout nombre premier p, on a :

$$v_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right]$$

Preuve du théorème 2. Soit $n \in \mathbb{N}^*$et p premier. On note

$$n_0 = \max \left\{ k \in \mathbb{N} | \frac{n}{p^k} \geqslant 1 \right\}$$

En réalité, la somme $\sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right]$ est finie, car pour tout $k \geqslant n_0 + 1$, on a $\left[\frac{n}{p^k} \right] = 0$.

On a donc :

$$\sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right] = \sum_{k=1}^{n_0} \left[\frac{n}{p^k} \right]$$

On commence par démontrer le lemme suivant :

Lemme 2. Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}$, le nombre de multiples de a dans $[\![1, b]\!]$est $\left[\frac{b}{a} \right]$.

Preuve du lemme 2. Soit $(a, b) \in \mathbb{N}^* \times \mathbb{N}$,

1. Cas où $b < a$:

Il n'existe aucun multiple de a entre 1 et b, donc le nombre de multiples de a dans $[\![1, b]\!]$est

$$0 = \left[\frac{b}{a}\right]$$

2. Cas où $b \geqslant a$:

Soit $x \in [\![1, b]\!]$ tel que a divise x. Alors, il existe $k \in \mathbb{N}^*$ tel que $x = ka$.

On a $1 \leqslant ka \leqslant b$, donc $0 < \frac{1}{a} \leqslant k \leqslant \frac{b}{a}$.

En prenant la partie entière, on obtient

$$1 \leqslant k \leqslant \left[\frac{b}{a}\right]$$

Réciproquement, pour tout entier k tel que $1 \leqslant k \leqslant \left[\frac{b}{a}\right]$, on a

$$a \leqslant ak \leqslant a\left[\frac{b}{a}\right] \leqslant b$$

Donc ka est bien un multiple de a dans $[\![1, b]\!]$.

Ainsi, le nombre de multiples de a dans $[\![1, b]\!]$ est $\left[\frac{b}{a}\right]$.

Pour tout nombre premier p, on a :

$$\begin{aligned} v_p(n!) &= v_p\left(\prod_{k=1}^{n} k\right) \\ &= \sum_{k=1}^{n} v_p(k) \end{aligned}$$

On note, pour tout $i \in [\![0, n_0]\!]$,

$$A_i = \{k \in [\![1, n]\!] | p^i \text{ divise } k \text{ et } p^{i+1} \text{ ne divise pas } k\}$$

On a bien $(A_i)_{0 \leqslant i \leqslant n_0}$ est une partition de $[\![1, n]\!]$ (par construction), donc

$$v_p(n!) = \sum_{i=0}^{n_0} \left(\sum_{k \in A_i} v_p(k) \right)$$

Or, pour tout $i \in [\![0, n_0]\!]$ et pour tout $k \in A_i$, p^i divise k et p^{i+1} ne divise pas k, donc pour tout $i \in [\![0, n_0]\!]$ et pour tout $k \in A_i$:

$$v_p(k) = i$$

D'où,

$$\begin{aligned} v_p(n!) &= \sum_{i=0}^{n_0} i.\#(A_i) \\ &= \sum_{i=1}^{n_0} i.\#(A_i) \end{aligned}$$

Or, pour tout $i \in [\![1, n_0]\!]$, on a :

$$A_i = \{k \in [\![1, n]\!] | p^i \text{ divise } k \text{ et } p^{i+1} \text{ ne divise pas } k\}$$

Ainsi,

$$A_i = \{k \in [\![1, n]\!] | p^i \text{ divise } k\} \backslash \{k \in [\![1, n]\!] | p^{i+1} \text{ divise } k\}$$

Puisque

$$\{k \in [\![1, n]\!] / p^{i+1} \text{ divise } k\} \subset \{k \in [\![1, n]\!] / p^i \text{ divise } k\}$$

Alors,

$$\#A_i = \#\{k \in [\![1, n]\!] / p^i \text{ divise } k\} - \#\{k \in [\![1, n]\!] / p^{i+1} \text{ divise } k\}$$

Donc,

$$\#A_i = \left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor$$

Ainsi,

$$\begin{aligned} v_p(n!) &= \sum_{i=1}^{n_0} i. \left(\left\lfloor \frac{n}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^{i+1}} \right\rfloor \right) \\ &= \sum_{k=1}^{n_0} \left\lfloor \frac{n}{p^k} \right\rfloor \\ &= \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \end{aligned}$$

Théorème 3. (La formule de Mertens)

Pour tout $x > 1$, on a

$$\sum_{p \leqslant x} \frac{\log(p)}{p} \underset{x \to +\infty}{=} \log(x) + O(1)$$

Preuve du théorème 3. Soit $x > 2$, notons $n = [x]$. On a

$$n! = \prod_{p \leqslant x} p^{v_p(n!)}$$

Donc,

$$\log(n!) = \sum_{p \leqslant x} v_p(n!) \log(p)$$

Pour tout nombre premier $p \leqslant x$, d'après le théorème de Legendre, on a :

$$\begin{aligned} \frac{n}{p} - 1 &< \left[\frac{n}{p}\right] \\ &< v_p(n!) \\ &= \sum_{k=1}^{+\infty} \left[\frac{n}{p^k}\right] \\ &\leqslant \sum_{k=1}^{+\infty} \frac{n}{p^k} \\ &= \frac{n}{p-1} \\ &= \frac{n}{p} + \frac{n}{p(p-1)} \end{aligned}$$

Ainsi,

$$\begin{aligned} n \sum_{p \leqslant x} \left(\frac{\log(p)}{p} - \frac{\log(p)}{n}\right) &\leqslant \log(n!) \\ &= \sum_{p \leqslant x} v_p(n!) \log(p) \\ &\leqslant n \sum_{p \leqslant x} \left(\frac{\log(p)}{p} + \frac{\log(p)}{p(p-1)}\right) \end{aligned}$$

Donc :

$$\frac{\log(n!)}{n} - \sum_{p \leqslant x} \frac{\log(p)}{p(p-1)} - \log(x) \leqslant \sum_{p \leqslant x} \frac{\log(p)}{p} - \log(x)$$

Et

$$\sum_{p \leqslant x} \frac{\log(p)}{p} - \log(x) \leqslant \frac{\log(n!)}{n} - \log(x) + \sum_{p \leqslant x} \frac{\log(p)}{n}$$

Avec :

$$\begin{aligned}\sum_{p\leqslant x}\frac{\log(p)}{n} &= \frac{1}{n}\log\left(\prod_{p\leqslant x}p\right)\\ &= \frac{1}{n}\log\left(\prod_{p\leqslant n}p\right)\end{aligned}$$

Or, on a pout tout entier $m \geqslant 0$

$$\begin{aligned}2\times 4^m &= (1+1)^{2m+1}\\ &= \sum_{k=0}^{2m+1}\left(\begin{array}{c}2m+1\\ k\end{array}\right)\end{aligned}$$

Donc,

$$\begin{aligned}\left(\begin{array}{c}2m+1\\ m\end{array}\right) &= \frac{1}{2}\left[\left(\begin{array}{c}2m+1\\ m\end{array}\right)+\left(\begin{array}{c}2m+1\\ m+1\end{array}\right)\right]\\ &\leqslant \frac{1}{2}\sum_{k=0}^{2m+1}\left(\begin{array}{c}2m+1\\ k\end{array}\right)\\ &= 4^m\end{aligned}$$

Pour tout nombre premier $m+1 < p \leqslant 2m+1$, on a p divise $(2m+1)!$, donc p divise

$$m!(m+1)!\left(\begin{array}{c}2m+1\\ m\end{array}\right)$$

Comme $p > m+1$, alors p ne divise ni $m!$ ni $(m+1)!$, d'où, d'après le lemme de Gauss, p divise $\left(\begin{array}{c}2m+1\\ m\end{array}\right)$.

Ainsi,

$$\prod_{m+1<p\leqslant 2m+1} p \,\text{divise}\left(\begin{array}{c}2m+1\\ m\end{array}\right)$$

D'où,

$$\begin{aligned}\prod_{m+1<p\leqslant 2m+1} p &\leqslant \left(\begin{array}{c}2m+1\\ m\end{array}\right)\\ &\leqslant 4^m\end{aligned}$$

Montrons maintenant par récurrence que pour tout $m \in \mathbb{N}^*$, on a :

$$\prod_{p \leqslant m} p \leqslant 4^m$$

Pour $m = 1$, on a

$$\begin{aligned} \prod_{p \leqslant m} p &= \prod_{p \leqslant 1} p \\ &= 1 \\ &\leqslant 4 \end{aligned}$$

Soit $m \in \mathbb{N}^*$, supposons que pour tout $k \in [\![1, m]\!]$

$$\prod_{p \leqslant k} p \leqslant 4^k$$

et montrons que

$$\prod_{p \leqslant m+1} p \leqslant 4^{m+1}$$

Si $m+1$ n'est pas premier, on a alors :

$$\begin{aligned} \prod_{p \leqslant m+1} p &= \prod_{p \leqslant m} p \\ &\leqslant 4^m \\ &\leqslant 4^{m+1} \end{aligned}$$

Si $(m+1)$ est premier :

Si $m = 1$, on a

$$\begin{aligned} \prod_{p \leqslant m+1} p &= 2 \\ &\leqslant 4^2 \end{aligned}$$

Si $m > 1$, alors $m+1$ est impair, donc il existe $k_0 \in [\![1, m]\!]$ tel que $m + 1 = 2k_0 + 1$.

On a alors :

$$\begin{aligned} \prod_{p \leqslant m+1} p &= \prod_{p \leqslant 2k_0+1} p \\ &= \prod_{p \leqslant k_0+1} p \prod_{k_0+1 < p \leqslant 2k_0+1} p \\ &\leqslant 4^{k_0} \times 4^{k_0+1} \\ &= 4^{m+1} \end{aligned}$$

D'où pour tout $n \in \mathbb{N}^*$

$$\prod_{p \leqslant m} p \leqslant 4^m$$

Par suite :

$$\begin{aligned}
\sum_{p \leqslant x} \frac{\log(p)}{n} &= \frac{1}{n} \log\left(\prod_{p \leqslant x} p\right) \\
&= \frac{1}{n} \log\left(\prod_{p \leqslant n} p\right) \\
&\leqslant \frac{1}{n} \log(4^n) \\
&= \log(4)
\end{aligned}$$

Et on a :

$$\sum_{p \leqslant x} \frac{\log(p)}{p(p-1)} \leqslant \sum_{2 \leqslant k \leqslant n} \frac{\log(k)}{k(k-1)}$$

Comme

$$\frac{\log(k)}{\sqrt{k}} \underset{k \to +\infty}{\longrightarrow} 0$$

alors

$$\frac{\log(k)}{k(k-1)} = o\left(\frac{1}{\sqrt{k}(k-1)}\right)$$

avec

$$\frac{1}{\sqrt{k}(k-1)} \underset{k \to +\infty}{\sim} \frac{1}{k^{3/2}} \text{ et} \sum_{k \geqslant 2} \frac{1}{k^{3/2}} \text{ converge}$$

Alors $\sum_{k \geqslant 2} \frac{1}{\sqrt{k}(k-1)}$ converge, et par suite $\sum_{k \geqslant 2} \frac{\log(k)}{k(k-1)}$ converge.

On a donc par positivité des termes :

$$\begin{aligned}
\sum_{p \leqslant x} \frac{\log(p)}{p(p-1)} &\leqslant \sum_{2 \leqslant k \leqslant n} \frac{\log(k)}{k(k-1)} \\
&\leqslant \sum_{k=2}^{+\infty} \frac{\log(k)}{k(k-1)} \\
&< +\infty
\end{aligned}$$

D'où,

$$\frac{\log(n!)}{n} - \sum_{k=2}^{+\infty} \frac{\log(k)}{k(k-1)} - \log(x) \leqslant \sum_{p \leqslant x} \frac{\log(p)}{p} - \log(x) \leqslant \frac{\log(n!)}{n} - \log(x) + \log(4)$$

D'après la formule de stirling :

$$\frac{\log(n!)}{n} = \log(n) - 1 + O\left(\frac{\log(n)}{n}\right)$$

Donc :

$$\frac{\log(n!)}{n} - \log(x) = \log\left(\frac{n}{x}\right) - 1 + O\left(\frac{\log(n)}{n}\right)$$

Avec $n \leqslant x < n+1$, donc

$$1 - \frac{1}{x} < \frac{n}{x} \leqslant 1$$

On a donc

$$\log\left(1 - \frac{1}{x}\right) \leqslant \log\left(\frac{n}{x}\right) \leqslant 0$$

Il existe $N_1 \in \mathbb{N}$ et $M > 0$ tels que pour tout $m \geqslant N_1$, on a

$$\left|O\left(\frac{\log(m)}{m}\right)\right| \leqslant M.\frac{\log(m)}{m}$$

Donc pour tout $x \geqslant N_1$, et pour tout $n \geqslant N_1$, on a :

$$\begin{aligned}\left|\frac{\log(n!)}{n} - \log(x)\right| &\leqslant 1 + \left|\log\left(\frac{n}{x}\right)\right| + M\frac{\log(n)}{n} \\ &\leqslant 1 + \log\left(\frac{x}{x-1}\right) + M.\frac{\log(n)}{n}\end{aligned}$$

Donc :

$$\begin{aligned}\left|\frac{\log(n!)}{n} - \log(x)\right| &\leqslant 1 + \left|\log\left(\frac{n}{x}\right)\right| + M\frac{\log(n)}{n} \\ &\leqslant 1 + \log\left(\frac{x}{x-1}\right) + M\end{aligned}$$

Comme $\log \frac{x}{x-1} \underset{x\to+\infty}{\to} 0$, alors il existe $\eta > 0$ tel que pour tout $x \geqslant \eta$, on a

$$\text{og}\,\frac{x}{x-1} \leqslant 1$$

Pour $N = \max(N_1, [\eta] + 1)$, on a pour tout $x \geqslant N$:

$$\left|\frac{\log(n!)}{n} - \log(x)\right| \leqslant 2 + M$$

Donc pour tout $x \geqslant \eta$, on a :

$$-\sum_{k=2}^{+\infty}\frac{\log(k)}{k(k-1)} - 2 - M \leqslant \sum_{p\leqslant x}\frac{\log(p)}{p} - \log(x) \leqslant 2 + M + \log(4)$$

Par suite :

$$\left|\sum_{p\leqslant x}\frac{\log(p)}{p}-\log(x)\right|\leqslant 2+M+\max\left(\log(4),\sum_{k=2}^{+\infty}\frac{\log(k)}{k(k-1)}\right)$$

D'où,

$$\sum_{p\leqslant x}\frac{\log(p)}{p}=\log(x)+O(1)$$

Quelques résultats sur les groupes finis

Définition 2. Soit G un groupe commutatif fini dont on notera la loi multiplicativement.

On dit qu'un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^\star$ est un caractère de G. Soient χ et χ' deux caractères de G. Le produit $\chi\chi_0$ est défini par la formule :

$$\chi\chi'(g)=\chi(g)\chi'(g)\,\text{pour}\,g\in G.$$

On note 1 le caractère constant de valeur 1. L'ensemble $\hat{G}$ des caractères de G est ainsi muni d'une loi de groupe d'élément neutre 1.

On note $\widehat{\hat{G}}$ le groupe des caractères de $\hat{G}$.

On note enfin $\overline{\chi}$ le caractère qui à $g\in G$ associe le conjugué $\overline{\chi(g)}$ de $\chi(g)$.

Pour tout $z\in G$, considérons l'application$\varphi_x\in\widehat{\hat{G}}$ définie par :

$$\forall\chi\in\hat{G},\quad\varphi_x(\chi)=\chi(x)$$

Théorème 4. le morphisme :

$$\begin{cases}G\to\widehat{\hat{G}}\\ x\longmapsto\varphi_x\end{cases}$$

est injectif

Preuve du théorème 4. Soit $x \in G$ tel que $x \neq 1$ et $\text{gr}(x)$ le sous-groupe de G engendré par x. Montrons qu'il existe un caractère χ de $\text{gr}(x)$ tel que $\chi(x) \neq 1$.

Comme $\text{gr}(x)$ est cyclique, alors il est isomorphe à $\mathbb{Z}/m\mathbb{Z}$, où $m = o(x)$; l'ordre de x dans G.

Et comme $\mathbb{Z}/m\mathbb{Z}$ est isomprphe à $\mathbb{U}_m$; le groupe des racines m-ièmes de l'unité, alors $\text{gr}(x)$ est isomorphe à $\mathbb{U}_m$.

Puisque $x \neq 1$, alors $m \geqslant 2$, et donc il existe un caractère de $\mathbb{U}_m$ qui ne prend la valeur 1 qu'en 1.

Via l'isomorphisme, on en déduit l'existance d'un caractère χ de $\text{gr}(x)$ qui ne prend la valeur 1 qu'en 1_G.

D'où l'existance d'un caractère χ de $\text{gr}(x)$ tel que $\chi(x) \neq 1$.

Soit F la famille des sous-groupes H de G contenant $\text{gr}(x)$ tels que χ se prolonge en un caractère de H. Montrer que F admet un élément G' de cardinal maximal.

Supposons que $G\prime \neq G$. Soit y un élément de G qui n'est pas dans $G\prime$.

On a :

$$F = \{H \,\text{sous groupe de}\, G | \,\text{gr}(x) \subset H \text{ and } \chi \,\text{se prolonge en un caract è re de}\, H\}$$

Considèrons l'ensemble :

$$A_F = \{\#H | H \in F\}$$

A_F est une partie de $\mathbb{N}$. Comme $\text{gr}(x)$ est un sous-groupe de G tel que $\text{gr}(x) \subset \text{gr}(x)$ et χ se prolonge en un caractère de H, alors $\text{gr}(x) \in F$, donc $F \neq \emptyset$, et par suite $A_F \neq \emptyset$.

Puisque G est un groupe fini, alors

$$\forall H \subset F, H \,\text{est fini et}\, \#H \leqslant \#G$$

D'où A_F est une partie de $\mathbb{N}$, non vide majorée.

Par conséquent, A_F possède un plus grand élément.

Il en résulte que F admet un élement G' de cardinal maximal.

Condidèrons l'ensemble

$$K = \{m \in \mathbb{N}^* | y^m \in G'\}$$

K est une partie non vide de $\mathbb{N}$, puisqu'il contient l'ordre de y (qui est fini, puisque G est fini, et $1_G \in G'$).

Ainsi, K admet un plus petit élément, d'où l'existence de $n \in \mathbb{N}^*$minimal tel que $y^n \in G'$.

Soit χ' un caractère de G' prolongeant χ et posons $a = \chi'(g^n)$.

Soit b une racine n-ième de a dans $\mathbb{C}$.

Pour tous $m, k \in \mathbb{Z}$ et $g, g' \in G'$, en effectuant la division euclidienne de $m - k$ par n, on a l'existence de $(q, r) \in \mathbb{Z} \times [\![0, n-1]\!]$ tel que :

$$m - k = q.n + r$$

comme $g^n \in G'$, alors $g^{q.n} \in G'$.

Si $g^m.g = y^k g'$, alors $g^{m-k} = g'.g^{-1} \in G'$. On a alors

$$g^r = g^{m-k}.g^{-q.n} \in G'$$

Alors $r = 0$, (car sinon, on trouve une contraduction avec le caratère minimale de $n \geqslant 1$).

Donc,

$$g^{m-k} = g'.g^{-1}$$

ce qui implique

$$g^{q.n} = g^{-1}.g'$$

Puisque χ' est un caractère, alors :

$$\begin{aligned} \chi'(g').\chi'(g^{-1}) &= \chi'((g^n)^q) \\ &= (\chi'(g^n))^q \\ &= a^q \\ &= b^{m-k} \end{aligned}$$

Il vient donc :

$$\chi'(g')b^k = \chi'(g)b^m$$

On peut donc définir χ'' pour tout $(m, g) \in \mathbb{Z} \times G'$ par :

$$\chi''(g^m g) = b^m \chi'(g)$$

On a ainsi $\chi''_{/G} = \chi'$, par constuction

$$\chi''_{/G} = \chi'_{/G} = \chi$$

Puisque χ' prolonge χ à G', on peut alors prolonger χ au groupe engendré par g et G'.

L'hypothèse $G' \neq G$ conduit à une absurdité, car le groupe engendré par G' et g a un cardinal strictement supérieur à celui de G' (puisque $y \notin G'$). On en déduit donc que

$$G' = G$$

Pour tout $g \in G$distinct de 1, on dispose d'un caractère χ de G tel que $\chi(g) \neq 1$, donc $\phi_g(\chi) \neq 1$ autrement dit $\phi_g \neq 1$.

On en déduit que l'application $g \longmapsto \varphi_g$ est injective (puisque ϕ_g est un morphisme).

Théorème 5. Pour tout $x \in G$:

$$\sum_{\chi \in \hat{G}} \chi(x) = 0 \,\text{si}\, x \neq 1$$

et

$$\sum_{\chi \in \hat{G}} \chi(x) = \#\hat{G} \,\text{si}\, x = 1$$

Preuve du théorème 5. Soit $(\chi', x) \in \hat{G} \times G$. Considérons l'application $\varphi : \hat{G} \longrightarrow \hat{G}$ définie pour tout $\chi \in \hat{G}$ par :

$$\varphi(\chi) = \chi.\chi'$$

Cette application est bien définie et bijective.

Ainsi, on a :

$$\sum_{\chi \in \hat{G}} \chi(x) = \sum_{\chi \in \hat{G}} (\chi.\chi')(x)$$

Si $x \neq 1$, il existe, d'après ce qui précède un $\chi' \in \hat{G}$ tel que $\chi'(x) \neq 1$. On obtient alors :

$$(1 - \chi'(x)) \sum_{\chi \in \hat{G}} \chi(x) = 0$$

Comme $1 - \chi'(x) \neq 0$, on en déduit que :

$$\sum_{\chi \in \hat{G}} \chi(x) = 0$$

Si $x = 1$, on a :

$$\begin{aligned} \sum_{\chi \in \hat{G}} \chi(x) &= \sum_{\chi \in \hat{G}} 1 \\ &= \#\hat{G} \end{aligned}$$

Théorème 6. Pour tout caractère $\chi \in \hat{G}$, on a :

$$\sum_{g \in G} \chi(g) = 0 \,\text{si}\, \chi \neq 1$$

et

$$\sum_{g \in G} \chi(g) = \#G \,\text{si}\, \chi = 1$$

Preuve du théorème 6. Si $\chi \neq 1$, soit $y \in G$ tel que $\chi(y) \neq 1$. L'application $g \in G \to g.y \in G$ est bijective. On a alors :

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{g \in G} \chi(g.y) \\ &= \left(\sum_{g \in G} \chi(g) \right) \chi(y) \end{aligned}$$

D'où

$$(1 - \chi(y)) \left(\sum_{g \in G} \chi(g) \right) = 0$$

Comme $1 - \chi(y) \neq 0$, on en déduit que

$$\sum_{g \in G} \chi(g) = 0$$

Si $\chi \neq 1$, on a

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{g \in G} 1 \\ &= \#G \end{aligned}$$

Théorème 7. le morphisme

$$\begin{cases} G \to \widehat{\hat{G}} \\ x \longmapsto \varphi_x \end{cases}$$

est bijectif.

Preuve du théorème 7. On a :

$$\begin{aligned} \sum_{(\chi,x)\in\hat{G}\times G} \chi(x) &= \sum_{\chi\in\hat{G}}\sum_{x\in G}\chi(x) \\ &= \sum_{\chi\in\hat{G}\setminus\{1\}}\sum_{x\in G}\chi(x) + \sum_{x\in G}1(x) \\ &= \#G \end{aligned}$$

D'autre part :

$$\begin{aligned} \sum_{(\chi,x)\in\hat{G}\times G} \chi(x) &= \sum_{x\in G}\sum_{\chi\in\hat{G}}\chi(x) \\ &= \sum_{x\in G\setminus\{1\}}\sum_{\chi\in\hat{G}}\chi(x) + \sum_{\chi\in\hat{G}}\chi(1) \\ &= \#\hat{G} \end{aligned}$$

On en déduit que $\#\hat{G} = \#G$,donc $\#\widehat{\hat{G}} = \#G$

Puisque le morphisme $\begin{cases} G \to \widehat{\hat{G}} \\ x \longmapsto \varphi_x \end{cases}$ est injectif, alors il est bijectif (c'est un isomorphisme de groupes).

La démonstration du théorème de Dirichlet. On va utiliser plusieurs fois une transformée connue sous le nom de sommation d'Abel.

On commence par l'énoncé et la démonstration de cette formule. Ensuite, nous définissons quelques fonctions arithmétiques et nous énonçons quelques propositions sur ces fonctions.

Théorème 8. (La formule de sommation d'Abel) Soient $\sum_{n\geqslant 1} u_n$ et $\sum_{n\geqslant 1} v_n$ deux séries de nombres complexes. Soit $U_n = \sum_{k=1}^{n} u_k$ la somme partielle des u_k, on a alors pour tout $n \geqslant 1$:

$$\sum_{k=1}^{n} u_k v_k = \sum_{i=1}^{n-1} (v_i - v_{i+1}) U_i + v_n U_n$$

Preuve du théorème 8. Méthode 1.

Pour tout $n \geqslant 1$, on a :

$$\begin{aligned}
\sum_{k=1}^{n} u_k v_k &= \sum_{k=1}^{n} u_k (v_k - v_n) + v_n \sum_{k=1}^{n} u_k \\
&= \sum_{k=1}^{n} u_k \left(\sum_{i=k}^{n-1} (v_i - v_{i+1}) \right) + v_n U_n \\
&= \sum_{k=1}^{n} \sum_{i=k}^{n-1} u_k (v_i - v_{i+1}) + v_n U_n \\
&= \sum_{i=1}^{n-1} \sum_{k=1}^{i} u_k (v_i - v_{i+1}) + v_n U_n
\end{aligned}$$

Ainsi,

$$\begin{aligned}
\sum_{k=1}^{n} u_k v_k &= \sum_{i=1}^{n-1} (v_i - v_{i+1}) \left(\sum_{k=1}^{i} u_k \right) + v_n U_n \\
&= \sum_{i=1}^{n-1} (v_i - v_{i+1}) U_i + v_n U_n
\end{aligned}$$

Méthode 2.

Notons pour toute suite $(a_n)_{n\in\mathbb{N}}$, pour tout $n \in \mathbb{N}$:

$$\Delta a_n = a_{n+1} - a_n$$

Alors, pour tout $k \in \mathbb{N}$:

$$\begin{aligned}
\Delta(U.v)_k &= U_{k+1} v_{k+1} - U_k v_k \\
&= \begin{vmatrix} U_{k+1} & U_k \\ v_k & v_{k+1} \end{vmatrix} \\
&= \begin{vmatrix} u_{k+1} & U_k \\ -\Delta v_k & v_{k+1} \end{vmatrix}
\end{aligned}$$

Ainsi,

$$\Delta(U.v)_k = u_{k+1}v_{k+1} + U_k\Delta v_k$$

En sommant de 1 à $n-1$, on obtient :

$$\sum_{k=1}^{n-1}\Delta(U.v)_k = \sum_{k=1}^{n-1}u_{k+1}v_{k+1} + \sum_{k=1}^{n-1}U_k\Delta v_k$$

D'où :

$$U_{n-1}.v_{n-1} - U_1.v_1 = \sum_{k=1}^{n-1}u_{k+1}v_{k+1} + \sum_{k=1}^{n-1}U_k(v_{k+1} - v_k)$$

Ainsi :

$$\sum_{k=1}^{n}u_kv_k = \sum_{i=1}^{n-1}(v_i - v_{i+1})U_i + v_nU_n$$

Définition 3. (La fonction de Möbius) Soit $n \in \mathbb{N}^*$. On note $\mu(n)$ l'entier défini par :

$$\mu(n) = \begin{cases} 0 & \text{si } n \text{ est divisible par le carré d'un nombre premier} \\ (-1)^r & \text{si } r \text{ est le nombre de facteurs premiers distincts de } n, \\ & n \text{ non divisible par le carré d'un nombre premier} \end{cases}$$

Proposition 1. pour tout $n \neq 1$, on a l'égalité

$$\sum_{d/n}\mu(d) = 0$$

Preuve de la proposition 1. Méthode 1.

Soit $n = \prod_{i=1}^{m} p_i^{a_i}$ la décomposition en facteurs premiers de n.

Si $d \in \mathbb{N}$ tel que d divise n. Alors, $\mu(d) \neq 0$ si et seulement si $d = \prod_{i\in J} p_i^{a_i}$ with $J \subset [\![1, m]\!]$

Dans ce cas on a

$$\mu(d) = (-1)^{\#J}$$

On en déduit que :

$$\begin{aligned} \sum_{d/n}\mu(d) &= \sum_{J\subset[\![1,m]\!]}(-1)^{\#J} \\ &= (1-1)^m \\ &= 0 \qquad (\text{car } m > 0) \end{aligned}$$

Méthode 2.

Soit $n \geqslant 2$. D'après le théorème fondamental de l'arithmétique, il existe des entiers premiers $p_1, \ldots, p_r$ et $\alpha_1, \ldots, \alpha_r \geqslant 1$ tels que :

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

On a :

$$\sum_{d/n} \mu(d) = \sum_{k_1=0}^{\alpha_1} \sum_{k_2=0}^{\alpha_2} \cdots \sum_{k_r=0}^{\alpha_r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Par suite :

$$\sum_{d/n} \mu(d) = \sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!] k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) + \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Puisque pour tout $(k_1, \ldots, k_r) \in \prod_{i=1}^{r} [\![0, \alpha_i]\!]$ tel qu'il existe $i_0 \in [\![1, r]\!]$ tel que $k_{i_0} \geqslant 2$, on a

$$\prod_{i=1}^{r} p_i^{k_i} \text{ est divisible par } p_{i_0}^2$$

Alors,

$$\mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$$

D'où

$$\sum_{\substack{(k_1,\ldots,k_r) \in \prod_{i=1}^{r} [\![0,\alpha_i]\!] \\ \exists i_0 \in [\![1,r]\!] k_{i_0} \geqslant 2}} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) = 0$$

Par suite :

$$\sum_{d/n} \mu(d) = \sum_{(k_1,\ldots,k_r) \in [\![0,1]\!]^r} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right)$$

Pour tout $(k_1, \ldots, k_r) \in [\![0, 1]\!]^r$, on a $\sum_{i=1}^{r} k_i$ est le nombre de facteurs premiers distincts de $\prod_{i=1}^{r} p_i^{k_i}$, et $\prod_{i=1}^{r} p_i^{k_i}$ n'est pas divisible par le carré d'un

nombre premier. Alors :

$$\begin{aligned}\sum_{d/n}\mu(d) &= \sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{i=1}^{r}k_i}\\ &= \prod_{i=1}^{r}\left(\sum_{k_1=0}^{1}(-1)^{k_i}\right)\\ &= (1-1)^r\\ &= 0\end{aligned}$$

Théorème 9. (La formule d'inversion de Möbius) Soit H une fonction non nulle de $\mathbb{N}^*$ dans $\mathbb{C}$ telle que pour tout $n, m \in \mathbb{N}^*$

$$H(n.m) = H(n)H(m)$$

On se donne également deux fonctions F et G de$[1, +\infty[$ dans $\mathbb{C}$ telles que :

$$\forall x > 1, \quad G(x) = \sum_{1\leqslant k\leqslant x} F\left(\frac{x}{k}\right)H(k)$$

Alors :

$$\forall x > 1, \quad F(x) = \sum_{1\leqslant k\leqslant x} \mu(k)G\left(\frac{x}{k}\right)H(k)$$

Preuve du théorème 9. On a

$$H(1) = H(1\times 1) = H(1)^2$$

Puisque $H \neq 0$, alors $H(1) = 1$.

De plus, pour tout $x \in [1, +\infty[$, on a :

$$\begin{aligned}
\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k) &= \sum_{1\leqslant k\leqslant x}\mu(k)\sum_{1\leqslant i\leqslant\frac{x}{k}}F\left(\frac{x}{i.k}\right)H(i)H(k)\\
&= \sum_{1\leqslant k\leqslant x}\sum_{1\leqslant i\leqslant\frac{x}{k}}\mu(k)F\left(\frac{x}{i.k}\right)H(i.k)\\
&= \sum_{1\leqslant k.i\leqslant x}\mu(k)F\left(\frac{x}{i.k}\right)H(i.k)\\
&= \sum_{1\leqslant m\leqslant x}\sum_{d|m}\mu(d)F\left(\frac{x}{m}\right)H(m)\\
&= \sum_{1\leqslant m\leqslant x}F\left(\frac{x}{m}\right)H(m)\left(\sum_{d|m}\mu(d)\right)\\
&= F(x)H(1)+\sum_{2\leqslant m\leqslant x}F\left(\frac{x}{m}\right)H(m)\left(\sum_{d|m}\mu(d)\right)
\end{aligned}$$

D'après la proposition 1, on a pour tout $m\geqslant 2$

$$\sum_{d|m}\mu(d)=0$$

d'où :

$$F(x)=\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)H(k)$$

Définition 4. Soit Λ la fonction de $[1,+\infty[$ dans $\mathbb{R}$ qui à p^n associe $\log(p)$ et qui est nulle sur tous les réels qui ne sont pas des entiers de la forme p^n.

Proposition 2. Pour tout entier $m\geqslant 1$, on a :

$$\Lambda(x)=\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right)$$

Preuve de la proposition 2. Méthode 1.

On applique ce qui précède à $F=\Lambda$ et $H=1$ (qui est bien une fonction multiplicative).

Alors, pour tout $x \geqslant 1$ et $k \in \mathbb{N}^*$ $\Lambda\left(\frac{x}{k}\right)$ est non nul si et seulement si x est un entier de la forme $k.p^n$ avec $n \in \mathbb{N}^*$, et nécessairement inférieur à $v_p(x)$.

D'où

$$\begin{aligned} G(x) &= \sum_{1\leqslant k\leqslant x} \Lambda\left(\frac{x}{k}\right) \\ &= 1_{\mathbb{N}}(x) \sum_{p^n\leqslant x} \log(p) \\ &= 1_{\mathbb{N}}(x) \sum_{p/x} v_p(x)\log(p) \\ &= 1_{\mathbb{N}}(x).\log(x) \end{aligned}$$

Ainsi,

$$\Lambda(x) = \sum_{1\leqslant k\leqslant x} \mu(k) 1_{\mathbb{N}}\left(\frac{x}{k}\right) \log\left(\frac{x}{k}\right)$$

En particulier, puisque $\frac{m}{k}$ est un entier si et seulement si k divise m

$$\Lambda(x) = \sum_{d|m} \mu(d) \log\left(\frac{m}{d}\right)$$

Méthode 2.

Pour tout entier $m \in \mathbb{N}^*$, on a

$$\Lambda(1) = 0$$

et

$$\sum_{d|1} \mu(d) \log\left(\frac{1}{d}\right) = \log(1) = 0$$

Dans la suite, on prend $m \geqslant 2$. D'après le théorème fondamental de l'arithmétique, il existe $p_1, \ldots, p_r \in \mathcal{P}^+$ et $\alpha_1, \ldots, \alpha_r \in \mathbb{N}^*$ tels que

$$m = \prod_{i=1}^{r} p_i^{\alpha_i}$$

On a alors :

$$\sum_{d|m} \mu(d) \log\left(\frac{m}{d}\right) = \sum_{(k_1,\ldots,k_r)\in \prod_{i=1}^{r} [\![0,\alpha_i]\!]} \mu\left(\prod_{i=1}^{r} p_i^{k_i}\right) \log\left(\prod_{i=1}^{r} p_i^{\alpha_i - k_i}\right)$$

Avec pour tout $(k_1,\dots,k_r)\in\prod_{i=1}^{r}[\![0,\alpha_i]\!]$, il existe $i_0\in[\![1,r]\!]$ tel que $k_{i_0}\geqslant 2$ alors

$$\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)=0$$

Alors,

$$\sum_{\substack{(k_1,\dots,k_r)\in\prod_{i=1}^{r}[\![0,\alpha_i]\!]\\ \exists i_0\in[\![1,r]\!]k_{i_0}\geqslant 2}}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)\log\left(\prod_{i=1}^{r}p_i^{\alpha_i-k_i}\right)=0$$

Par suite,

$$\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right)=\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}\mu\left(\prod_{i=1}^{r}p_i^{k_i}\right)\log\left(\prod_{i=1}^{r}p_i^{\alpha_i-k_i}\right)$$

Ainsi,

$$\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right)=\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{i=1}^{r}k_i}\sum_{j=1}^{r}(\alpha_j-k_j)\log(p_j)$$

Par suite,

$$\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right)=\log\left(\prod_{i=1}^{r}p_i^{\alpha_i}\right)(1+(-1))^r-\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{i=1}^{r}k_i}\sum_{j=1}^{r}k_j\log(p_j)$$

Ainsi,

$$\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right)=\sum_{j=1}^{r}\log(p_j)\sum_{(k_1,\dots,k_r)\in[\![0,1]\!]^r}(-1)^{\sum_{\substack{i=1\\ i\neq j}}^{r}k_i}\ k_j$$

Ainsi,

$$\begin{aligned}\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right) &= \sum_{j=1}^{r}\log(p_j)\left[\prod_{\substack{i=1\\ i\neq j}}^{r}(1-1)\right](0+1)\\ &= 0^{r-1}\sum_{j=1}^{r}\log(p_j)\\ &= \begin{cases} 0 \text{ si } r\geqslant 2\\ \log(p_1) \text{ si } r=1\end{cases}\\ &= \Lambda(m)\end{aligned}$$

D'où, pour tout $m\in\mathbb{N}^*$

$$\Lambda(m)=\sum_{d|m}\mu(d)\log\left(\frac{m}{d}\right)$$

Par caractère, on entendra toujours caractère de $G(N)$. On dira qu'un caractère $\chi\neq 1$ est non trivial.

On notera encore χ la fonction de $\mathbb{N}$ dans $\mathbb{C}$ définie par

$$\chi(m)=\chi(m \bmod N)$$

si m et N sont premiers entre eux, et $\chi(m)=0$ sinon.

On a la formule

$$\chi(ab)=\chi(a)\chi(b)$$

pour tout a,b.

Définition 5. Soit χ un caractère non trivial. On définit la fonction $f:\mathbb{N}\to\mathbb{C}$ pour tout $n\in\mathbb{N}$ par :

$$f(n)=\sum_{d|n}\chi(d)$$

On définit la fonction g pour tout $x\geqslant 0$, par :

$$g(x)=\sum_{n\leqslant x}\frac{f(n)}{\sqrt{n}}$$

Proposition 3. Soit χ un caractère non trivial. Les séries $\sum_{n\geqslant 1}\frac{\chi(n)}{n}$ et $\sum_{n\geqslant 1}\frac{\chi(n)}{n}\log(n)$ convergent.

On note dans la suite

$$L(\chi)=\sum_{n\geqslant 1}\frac{\chi(n)}{n}$$

et

$$L_1(\chi)=\sum_{n\geqslant 1}\frac{\chi(n)}{n}\log(n)$$

Preuve de la proposition 3. Soit χ un caractère non trivial et $m\in\mathbb{N}^*$. Puisque pour tout entier $n\geqslant 3$, on a

$$\left|\chi(n)\frac{\log(n)}{n}\right|\geqslant\left|\frac{\chi(n)}{n}\right|$$

Il suffit de montrer que la série $\sum_{n\geqslant 1}\chi(n)\frac{\log(n)}{n}$ converge.

D'aprés le théorème 5,

$$\begin{aligned}\sum_{n=1}^{N}\chi(n) &= \sum_{\substack{n=1\\ n\wedge N=1}}^{N}\chi(n)\\ &= \sum_{g\in G(N)}\chi(g)\\ &= 0 \quad (\star)\end{aligned}$$

On a, d'après la formule de sommation d'Abel (le théorème 8)

$$\sum_{n=1}^{m}\chi(n)\frac{\log(n)}{n}=\sum_{n=1}^{m}\chi(n)\frac{\log(m)}{m}+\sum_{n=1}^{m-1}\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)\sum_{i=1}^{n}\chi(i)$$

Par la division euclidienne de m par N, il existe $(q,r)\in\mathbb{N}^2$ tel que $r<N$ et $m=Nq+r$.

On a alors

$$\begin{aligned}\sum_{n=1}^{m}\chi(n) &= \sum_{n=1}^{nq+r}\chi(n)\\ &= \sum_{k=0}^{q-1}\left(\sum_{n=1+k.N}^{(k+1)N}\chi(n)\right)+\sum_{n=1+q.N}^{q.N+r}\chi(n)\\ &= \sum_{k=0}^{q-1}\left(\sum_{n=1}^{N}\chi(n+k.N)\right)+\sum_{n=1}^{r}\chi(n+q.N)\\ &= \sum_{k=0}^{q-1}\left(\sum_{n=1}^{N}\chi(n)\right)+\sum_{n=1}^{r}\chi(n)\\ &= q\sum_{n=1}^{N}\chi(n)+\sum_{n=1}^{r}\chi(n)\end{aligned}$$

D'après $(\star)$,

$$\sum_{n=1}^{N}\chi(n)=0$$

Donc :

$$\sum_{n=1}^{m}\chi(n)=\sum_{n=1}^{r}\chi(n)$$

Ainsi, par l'inégalité triangulaire

$$\left|\sum_{n=1}^{m}\chi(n)\right|\leqslant\sum_{n=1}^{r}|\chi(n)|$$

Donc :

$$\sum_{n=1}^{m}\chi(n)\frac{\log(m)}{m}=O\left(\frac{\log(m)}{m}\right)=o(1)$$

De plus,

$$\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)\sum_{i=1}^{n}\chi(i)=O\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)$$

Avec $\frac{\log(n)}{n}\underset{n\longrightarrow+\infty}{\longrightarrow}0$, alors la serie télescopique $\sum_{n\geqslant1}\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)$ converge.

Ainsi, la série

$$\sum_{n\geqslant1}\left[\left(\frac{\log(n+1)}{n+1}-\frac{\log(n)}{n}\right)\sum_{i=1}^{n}\chi(i)\right]\text{ converge}$$

On en déduit que la série $\sum_{n\geqslant 1}\chi(n)\frac{\log(n)}{n}$ converge.

Par suite $\sum_{n\geqslant 1}\frac{\chi(n)}{n}$ converge.

Proposition 4. La fonction f est arithmétique, et pour tout entier $n\in\mathbb{N}$, on a $f(n)\geqslant 0$.

De plus :

$$f(n)\geqslant 1 \text{ si } n \text{ est un carr é}$$

Preuve de la proposition 4. Soit $(n,m)\in\mathbb{N}^*\times\mathbb{N}^*$, tel que $n\wedge m=1$.

Pour tout d diviseur de n et d' diviseur de m, le produit dd' est un diviseur de $n.m$

Soit D un diviseur de $n.m$. Montrons l'existence et l'unicité d'un couple $(d,d')\in\mathbb{N}^*\times\mathbb{N}^*$, tel que d est un diviseur de n et d' est un diviseur de m et $D=d.d'$

On pose $a=D\wedge n$. On a alors $a|D$ et $a|n$.

Soient $p_1,\dots,p_r,p_{r+1},\dots,p_l$ des nombres premiers deux à deux distincts, et $\alpha_1,\dots,\alpha_l\in\mathbb{N}^*$ tels que :

$$n=\prod_{i=1}^{r}p_i^{\alpha_i} \text{ and } m=\prod_{i=r+1}^{l}p_i^{\alpha_i}$$

On a alors

$$nm=\prod_{i=1}^{l}p_i^{\alpha_i}$$

Comme D est un diviseur de nm, il existe $\lambda_1,\dots,\lambda_l\in\mathbb{N}$ tels que pour tout $i\in[\![1,l]\!]\lambda_i\leqslant\alpha_i$ et $D=\prod_{i=1}^{l}p_i^{\lambda_i}$

On a $a=D\wedge n$, donc

$$a=\prod_{i=1}^{r}p_i^{\min(\lambda_i,\alpha_i)}=\prod_{i=1}^{r}p_i^{\lambda_i}$$

Alors :

$$\frac{D}{a}=\prod_{i=r+1}^{l}p_i^{\lambda_i}$$

Donc $\frac{D}{a} \wedge n = 1$, et $\frac{D}{a}$ divise D, donc divise aussi nm. Via le lemme de Gauss, on en déduit que $\frac{D}{a}$ divise m.

Ainsi, tout diviseur mn est le produit d'un diviseur de n et d'un diviseur de m. Montrons maintenant que cette décomposition est unique.

Soient $d, d', D, D' \in \mathbb{N}^*$ tels que $d.d' = D.D'$ avec d et D (respectivement d' et D') sont des diviseurs de n (respectivement de m).

On a alors d divise $D.D'$, avec $d$est premier à D' (puisque n et m sont premiers entre eux). D'après le lemme de Gauss d divise D.

De même, on trouve Ddivise d, donc $D = d$. De même $D = d'$.

Il vient alors :

$$\begin{aligned} f(n)f(m) &= \left(\sum_{d|n} \chi(d)\right)\left(\sum_{d'|m} \chi(d')\right) \\ &= \sum_{d|n}\sum_{d'|m} \chi(d)\chi(d') \\ &= \sum_{\substack{d|n \\ d'|m}} \chi(d.d') \end{aligned}$$

On utilise ce qu'on a montré, et on a alors :

$$\begin{aligned} f(n)f(m) &= \sum_{d/n.m} \chi(d) \\ &= f(nm) \end{aligned}$$

Si n n'est pas premier à N, on a $\chi(n) = 0$ (par définition).

Sinon, on a $n \in G(N)$, qui est fini. Notons a l'ordre de $n$dans $G(N)$. On a

$$\begin{aligned} 1 &= \chi(1) \\ &= \chi(n^a) \\ &= \chi(n)^a \end{aligned}$$

Et donc $\chi(n)$est une racine a-ème de l'unité. Puisqu'on suppose que χ prend des valeurs réelles, on a $\chi(n)$ est égal à -1 ou 1.

En conclusion χ est à valeurs dans $\{-1, 0, 1\}$.

Soit p un nombre premier, on a pour tout $n \in \mathbb{N}$:

$$\begin{aligned} f(p^n) &= \sum_{k=0}^{n} \chi(p)^k \\ &= \begin{cases} 1 & \text{si } \chi(p) = 0 \\ n+1 & \text{si } \chi(p) = 1 \\ \frac{1+(-1)^n}{2} & \text{si } \chi(p) = -1 \end{cases} \end{aligned}$$

En décomposant n en facteurs premiers, on a

$$f(n) = \prod_{p|n} f(p^{v_p(n)})$$

Chacun des termes est positif, d'après ce qui précède, et même supérieur ou égal à 1 si $v_p(n)$ est pair. On en déduit :

$$f(n) \geqslant 0 \text{ and } f(n) \geqslant 1 \text{ si } n \text{ est un carr é}$$

Proposition 5. On a

$$\lim_{x \to +\infty} g(x) = +\infty$$

Preuve de la proposition 5. D'après ce qui précéde, pour tout $m \in \mathbb{N}^*$ et pour $x \geqslant m^2$, on a :

$$\begin{aligned} g(x) &\geqslant \sum_{k=1}^{m^2} \frac{f(k)}{\sqrt{k}} \\ &\geqslant \sum_{k=1}^{m} \frac{f(k^2)}{k} \\ &\geqslant \sum_{k=1}^{m} \frac{1}{k} \end{aligned}$$

Par divergence de $\sum\limits_{k \geqslant 1} \frac{1}{k}$, on obtient

$$\lim_{x \to +\infty} g(x) = +\infty$$

Proposition 6. Pour tout $x \geqslant 0$, on a

$$g(x) = \sum_{d' \leqslant \sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x} < d \leqslant \frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{d \leqslant \frac{x}{d}} \frac{1}{\sqrt{d'}}$$

Preuve de la proposition 6. L'application $(d, d') \longmapsto (d.d', d)$ de l'ensemble des couples $(d, d') \in \mathbb{N}^* \times \mathbb{N}^*$ vérifiant $n \leqslant x$ et $d|n$ est bien définie et bijective, avec pour réciproque :

$$(n, d) \longmapsto \left(d, \frac{n}{d}\right)$$

On en déduit que :

$$\begin{aligned} g(x) &= \sum_{n \leqslant x} \sum_{d/n} \frac{\chi(d)}{\sqrt{n}} \\ &= \sum_{d.d' \leqslant x} \frac{\chi(d)}{\sqrt{d.d'}} \end{aligned}$$

où la seconde somme est prise sur l'ensemble des couples (d, d') d'entiers $\geqslant 1$, tels que $dd' \leqslant x$. Pour de tels entiers, on a $d \leqslant \frac{x}{d'} \leqslant x$ et $d' \leqslant \frac{x}{d} \leqslant x$, avec $d' \leqslant \sqrt{x}$ si, et seulement si, $d > \sqrt{x}$.

En scindant la somme selon les cas $d < \sqrt{x}$ ou $d \geqslant \sqrt{x}$, on obtient :

$$\begin{aligned} g(x) &= \sum_{\substack{d.d' \leqslant x \\ d > \sqrt{x}}} \frac{\chi(d)}{\sqrt{d.d'}} + \sum_{\substack{d.d' \leqslant x \\ d \leqslant \sqrt{x}}} \frac{\chi(d)}{\sqrt{d.d'}} \\ &= \sum_{d' \leqslant \sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x} < d \leqslant \frac{x}{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \leqslant \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{d \leqslant \frac{x}{d}} \frac{1}{\sqrt{d'}} \end{aligned}$$

Proposition 7. Pour tout $x \geqslant 0$,

$$g(x) - \sqrt{x} L(\chi)$$

est bornée et $L(\chi)$ est non nul.

Preuve de la proposition 7. La fonction g est en escalier par définition, donc continue par morceaux sur son domaine de définition.

La fonction $x \longmapsto g(x) - 2\sqrt{x}L(\chi)$ est également continue par morceaux sur son domaine de définition. Pour montrer qu'elle est bornée, il suffit de montrer qu'elle est bornée au voisinage de $+\infty$.

Pour $m = [x]$, on a $g(x) = g(m)$ (par définition de g). Par conséquent,

$$g(x) - 2\sqrt{x}L(\chi) = g(m) - 2\sqrt{m}L(\chi) - 2L(\chi) - 2L(\chi)\frac{x-m}{\sqrt{x}+\sqrt{m}}$$

Puisque

$$\lim_{x \longmapsto +\infty} \frac{x - [x]}{\sqrt{x} + \sqrt{[x]}} = 0$$

On a alors :

$$g(x) - 2\sqrt{x}L(\chi) = g(m) - 2\sqrt{m}L(\chi) + o(1)$$

On se ramène donc à démontrer que

$$g(x) - 2\sqrt{x}L(\chi) = o(1)$$

dans le cas où x est un entier. Par ailleurs, par définition, on a :

$$\begin{aligned} 2\sqrt{m}L(\chi) &= 2\sqrt{m}\sum_{k=1}^{+\infty}\frac{\chi(k)}{k} \\ &= 2\sum_{k=1}^{+\infty}\frac{\chi(k)}{k}\sqrt{\frac{m}{k}} \end{aligned}$$

Ainsi, $g(m) - 2\sqrt{m}L(\chi)$ est égal à :

$$\sum_{d' \leqslant \sqrt{m}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{m} < d \leqslant \frac{m}{d'}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \leqslant \sqrt{m}} \frac{\chi(d)}{\sqrt{d}} \left(\sum_{d \leqslant \frac{m}{d}} \frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}} \right) - 2\sqrt{m} \sum_{d > \sqrt{m}} \frac{\chi(d)}{d}$$

On va démontrer que chacun des termes du membre de droite de cette égalité est borné par m, ce qui permet de conclure.

On applique le raisonnement de la question 1 avec

$$u_m = \chi(m)$$

On note $U_m = \sum_{d=1}^{m} \chi(d)$. On a vu que la suite $(U_m)_{m \geqslant 1}$ est bornée, et on dispose donc d'un réel positif A tel que

$$|U_m| \leqslant A$$

Supposons que la suite $(v_m)_{m\geqslant 1}$ soit de signe constant de décroissante en valeur absolue. Alors, pour tout $n \leqslant m$, on a :

$$\begin{aligned}\sum_{n<d\leqslant m} v_d u_d &= \sum_{d\leqslant m} v_d u_d - \sum_{d\leqslant n} v_d u_d \\ &= U_m v_m - U_n v_n + \sum_{d=n}^{m-1} U_d(v_d - v_{d+1})\end{aligned}$$

Et par hypothèse de monotonie et de signe sur $(v_m)_{m\geqslant 1}$, on a :

$$\begin{aligned}\left|\sum_{n<d\leqslant m} u_d v_d\right| &\leqslant A\left(|v_m| + |v_n| + \sum_{d=n}^{m-1}(|v_d| - |v_{d+1}|)\right) \\ &= 2A|v_n|\end{aligned}$$

Donc,

$$\sum_{n<d\leqslant m} u_d v_d = O(v_n)$$

Si de plus, la série $\sum u_d v_d$ converge, alors on peut passer à la limite dans l'inégalité précédente, et il vient :

$$\sum_{n<d} u_d v_d = O(v_n)$$

On prend d'abord $v_m = \frac{1}{m}$, qui constitue le terme général d'une suite décroissante et positive. Avec ce qui précéde, et puisque la série définissant $L(\chi)$ converge, il vient :

$$\begin{aligned}\left|-2\sqrt{m}\sum_{d>\sqrt{m}} \frac{\chi(d)}{d}\right| &= \sqrt{m}O\left(\frac{1}{[\sqrt{m}]}\right) \\ &= O(1)\end{aligned}$$

On prend ensuite $v_m = \frac{1}{\sqrt{m}}$, qui est également le terme général d'une suite positive décroissante. Il vient alors :

$$\sum_{\sqrt{m}<d\leqslant \frac{m}{d'}} \frac{\chi(d)}{\sqrt{d}} = O\left(\frac{1}{\sqrt{[\sqrt{m}]}}\right)$$

Or, par comparaison entre une série divergente (de Riemann) et une intégrale dans le cas d'une fonction continue et positive, on a :

$$\sum_{d'<\sqrt{m}} \frac{1}{\sqrt{d'}} \underset{m\to+\infty}{\sim} 2\sqrt{[\sqrt{m}]}$$

Et donc,

$$\sum_{d'<\sqrt{m}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{m}<d\leqslant \frac{m}{d'}} \frac{\chi(d)}{\sqrt{d}} = O(1)$$

Pour étudier le dernier terme, on constate :

$$\sum_{d'\leqslant \frac{m}{d}} \frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}} = \sum_{d'\leqslant \frac{m}{d}} \left(\frac{1}{\sqrt{d'}} - \int_{d'-1}^{d'} \frac{\mathrm{dt}}{\sqrt{t}} \right) + 2\sqrt{\left[\frac{m}{d}\right]} - 2\sqrt{\frac{m}{d}}$$

Or,

$$\begin{aligned} \sqrt{\left[\frac{m}{d}\right]} - \sqrt{\frac{m}{d}} &= \frac{\left[\frac{m}{d}\right] - \frac{m}{d}}{\sqrt{\left[\frac{m}{d}\right]} + \sqrt{\frac{m}{d}}} \\ &= O\left(\sqrt{\frac{d}{m}}\right) \end{aligned}$$

Et donc,

$$\sum_{d\leqslant\sqrt{m}} \frac{\chi(d)}{d} \left(\sum_{d'\leqslant \frac{m}{d}} \frac{1}{\sqrt{d'}} - 2\sqrt{\frac{m}{d}} \right) = \sum_{d\leqslant\sqrt{m}} \left[\int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}} \right) \mathrm{dt} + \frac{\chi(d)}{d} O\left(\sqrt{\frac{d}{m}}\right) \right]$$

On a :

$$\begin{aligned} \sum_{d\leqslant\sqrt{m}} \frac{\chi(d)}{d} O\left(\sqrt{\frac{d}{m}}\right) &= \sum_{d\leqslant\sqrt{m}} O\left(\sqrt{\frac{1}{m}}\right) \\ &= O(1) \end{aligned}$$

et que

$$\int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}} \right) dt < 0$$

On en déduit que la fonction $d \longmapsto \sum_{d'\leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}} \right) dt$ est négative et croissante (i.e décroissante en valeur absolue) en raison de la décroissance de $d \longmapsto \frac{m}{d}$. On pose donc, finalement :

$$v_d = \frac{1}{\sqrt{d}} \sum_{d'\leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}} \right) dt$$

de sorte que la suite $(v_d)_{d\geqslant 1}$ est négative et décroissante en valeur absolue, en tant que produit de deux termes tous deux décroissants en valeur absolue, l'un positif et l'autre négatif. On obtient donc :

$$\sum_{d\leqslant\sqrt{m}} \frac{\chi(d)}{d} \sum_{d'\leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}} \right) \mathrm{dt} = O\left(\int_0^m \frac{\mathrm{dt}}{\sqrt{t}} - \sum_{d'=1}^{m} \frac{1}{\sqrt{d'}} \right)$$

L'intégrale étant entendue comme une limite, et par comparaison entre série et intégrale, on a :

$$\int_1^{m+1} \frac{dt}{\sqrt{t}} \leqslant \sum_{d'=1}^{m} \frac{1}{\sqrt{d'}} \leqslant \int_0^m \frac{dt}{\sqrt{t}}$$

Et donc, puisque $\sqrt{m} - \sqrt{m+1} = \frac{-1}{\sqrt{m}+\sqrt{m+1}} = o(1)$, on en déduit que

$$\sum_{d \leqslant \sqrt{m}} \frac{\chi(d)}{d} \sum_{d' \leqslant \frac{m}{d}} \int_{d'-1}^{d'} \left(\frac{1}{\sqrt{d'}} - \frac{1}{\sqrt{t}} \right) dt = O(1)$$

Ainsi,

$$g(x) - 2\sqrt{x}L(\chi) \text{ est born ée}$$

On en déduit que la fonction $x \longmapsto 2\sqrt{x}L(\chi)$ tend vers l'infini en $-\infty$, et donc que $L(\chi)$est strictement positif. En particulier :

$$L(\chi) \text{ est non nul}$$

Théorème 10. Soit χ un caractère non trivial.

Si $L(\chi) \neq 0$, alors la fonction $x \longmapsto \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n}$ est bornée.

Si $L(\chi) \neq 0$, alors la fonction $x \longmapsto L_1(\chi) \sum_{n \leqslant x} \frac{\mu(n)\chi(n)}{n} + \log(x)$ est bornée.

Preuve du théorème 10. Soit χ un caractère non trivial.
Si $L(\chi) \neq 0$, posons pour tout $x \geqslant 0$,

$$G(x) = \sum_{1 \leqslant n \leqslant x} \frac{x}{n} \chi(n)$$

La fonction G est le produit de l'identité et d'une fonction en escalier, elle est donc continue par morceaux sur son domaine de définition. Il suffit de montrer qu'elle est bornée au voisinage de l'infini.

D'après la proposition 3, la série $\sum_{n\geqslant 1}\frac{\chi(n)}{n}$ converge, il vient par positivité et décroissance de $\left(\frac{1}{n}\right)_{n\geqslant 1}$

$$\begin{aligned} G(x)-x.L(\chi) &= x\sum_{n>x}\frac{\chi(n)}{n} \\ &= O\left(\frac{x}{[x]}\right) \\ &= O(1) \end{aligned}$$

Ainsi, $G(x)-x.L(\chi)$ est bornée.

le caractère χ étant multiplicatif, on applique le théorème 9 avec $F=\mathrm{id}$, $H=\chi$, donc les applications notées G sont identiques. On en déduit que

$$x=\sum_{1\leqslant k\leqslant x}\mu(k)G\left(\frac{x}{k}\right)\chi(k)$$

Donc,

$$\begin{aligned} x-L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k} &= \sum_{1\leqslant k\leqslant x}\mu(k)\chi(k)\left(G\left(\frac{x}{k}\right)-\frac{x}{k}L(\chi)\right) \\ &= O\left(\sum_{1\leqslant k\leqslant x}|\mu(k)\chi(k)|\right) \end{aligned}$$

Or, μ et χ sont bornés par 1 (on a déjà remarqué que χ prend ses valeurs non nulles dans les racines de l'unité), donc

$$x.L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=O(x)$$

Et

$$L(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}=O(1)$$

Par conséquent, si $L(\chi)$ est non nul, et puisque $x\longmapsto\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}$ est une fonction en escalier, donc continue par morceaux sur son domaine de définition, on conclut que

$$\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}\ \text{est born\'ee}$$

Si $L(\chi)=0$, posons pour tout $x>1$,

$$G_1(x)=\sum_{1\leqslant n\leqslant x}\left(\frac{x}{n}\log\left(\frac{x}{n}\right)\right)\chi(n)$$

Par définition et par convergence des séries définissant $L(\chi)$ et $L_1(\chi)$, en tenant compte de $L(\chi)=0$, on a

$$\begin{aligned}G_1(x)+x.L_1(\chi) &= G_1(x)+x.L(\chi)+x.L_1(x)\\ &= -x.\log(x)\sum_{n>x}\frac{\chi(n)}{n}+x\sum_{n>x}\frac{\chi(n)\log(n)}{n}\end{aligned}$$

Or, pour tout $n\geqslant 3$, on a $\log(n)\geqslant 1$, et donc

$$\begin{aligned}\log(n+1) &= \log(n)+\log\left(1+\frac{1}{n}\right)\\ &\leqslant \log(n)+\frac{1}{n}\\ &\leqslant \log\left(1+\frac{1}{n}\right)+\log(n)\frac{n}{n+1}\end{aligned}$$

Les suites $\left(\frac{1}{n}\right)_{n\geqslant 1}$ et $\left(\frac{\log(n)}{n}\right)_{n\geqslant 3}$ sont donc positives et décroissantes. Il résulte alors des relations obtenues en proposition 7 que, pour tout $x>2$,

$$\sum_{n>x}\frac{\chi(n)}{n}=O\left(\frac{1}{x}\right)\text{ and }\sum_{n>x}\frac{\chi(n)\log(n)}{n}=O\left(\frac{\log(x)}{x}\right)$$

D'où

$$G_1(x)=-x.L_1(x)+O(\log(x))$$

On applique le théorème 9, avec $F=\mathrm{id}\times\log$et $H=\chi$. Les applications notées G_1 et G dans le théorème 9 coïncident alors, et on en déduit

$$x.\log(x)=\sum_{1\leqslant k\leqslant x}\mu(k)G_1\left(\frac{x}{k}\right)\chi(k)$$

Et donc,

$$\begin{aligned}x.\log(x)+x.L_1(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k} &= \sum_{1\leqslant k\leqslant x}\mu(k)\chi(k)\left(G_1\left(\frac{x}{k}\right)+\frac{x}{k}L_1(x)\right)\\ &= O\left(\sum_{1\leqslant k\leqslant x}\log\left(\frac{x}{k}\right)\right)\\ &= O(x.\log(x)-\log([x]!))\end{aligned}$$

Ainsi, en utilisant la formule de Stirling :

$$\begin{aligned} O\left(\sum_{1\leqslant k\leqslant x}\log\left(\frac{x}{k}\right)\right) &= O(x.\log(x)-[x]\log([x])+O(x)) \\ &= O\left((x-[x]).\log(x)-[x]\log\left(\frac{x}{[x]}\right)+O(x)\right) \\ &= O(1).\log(x)+O(x).O(1)+O(x) \\ &= O(x) \end{aligned}$$

Donc,

$$\log(x)+L_1(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\tfrac{\chi(k)}{k}=O(1)$$

Ainsi, puisque nous avons affaire à des fonctions continues par morceaux sur leur domaine de définition,

$$\log(x)+L_1(\chi)\sum_{1\leqslant k\leqslant x}\mu(k)\frac{\chi(k)}{k}\text{ est born ée}$$

Théorème 11. On a :

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d}=\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m}+O(1)$$

Preuve du théorème 11. Puisque la suite $\left(\frac{\log(n)}{n}\right)_{n\geqslant 3}$ est positive et décroissante.

En utilisant les relations de la proposition 7, on obtient :

$$\sum_{n>m}\frac{\chi(n)\log(x)}{n}=O\left(\frac{\log(m)}{m}\right)$$

Par définition et par associativité, on a, puisque la seconde somme est finie et par multiplicativité de χ :

$$\begin{aligned} L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d} &= \sum_{d\leqslant x}\left(\sum_{n=1}^{+\infty}\frac{\chi(n)\log(n)}{n}\frac{\mu(d)\chi(d)}{d}\right) \\ &= \sum_{d\leqslant x}\sum_{n\leqslant\frac{x}{d}}\frac{\chi(n)\log(n)}{n}\frac{\mu(d)\chi(d)}{d}+\sum_{d\leqslant x}\sum_{n>\frac{x}{d}}\frac{\chi(n)\log(n)}{n}\frac{\mu(d)\chi(d)}{d} \\ &= \sum_{m\leqslant x}\sum_{d|m}\mu(d).\log\left(\frac{m}{d}\right)\frac{\chi(m)}{m}+\sum_{d\leqslant x}O\left(\frac{d.\log\left(\frac{x}{d}\right)}{x}\right)\frac{\mu(d)\chi(d)}{d} \end{aligned}$$

En utilisant la bijection $(d,n) \longmapsto (n.d,d)$, et la proposition 2, il vient :

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d} = \sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m} + \frac{1}{x}\sum_{d\leqslant x}O\left(\log\left(\frac{x}{d}\right)\right)$$

Or, vu que :

$$\sum_{d\leqslant x}\log\left(\frac{x}{d}\right) = O(x)$$

et donc

$$L_1(\chi)\sum_{d\leqslant x}\frac{\mu(d)\chi(d)}{d} = \sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m} + O(1)$$

Enfin, on a :

$$\begin{aligned}\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m} &= \sum_{p\leqslant x}\log(p)\sum_{n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n}\\ &= \sum_{p\leqslant x}\log(p)\frac{\chi(p)}{p} + \sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n}\end{aligned}$$

Avec

$$\begin{aligned}\sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}\frac{\chi(p)^n}{p^n} &= \sum_{p\leqslant x}\log(p)\sum_{2\leqslant n\leqslant\frac{\log(x)}{\log(p)}}O\left(\frac{1}{p^n}\right)\\ &= \sum_{p\leqslant x}O\left(\frac{1}{p^2}\frac{1}{1-\frac{1}{p}}\right)\log(p)\\ &= O(1)\end{aligned}$$

Ainsi :

$$\sum_{m\leqslant x}\Lambda(m)\frac{\chi(m)}{m} = \sum_{p\leqslant x}\log(p)\frac{\chi(p)}{p} + O(1)$$

Puisque

$$\log(p)\frac{1}{p^2}\frac{1}{1-\frac{1}{p}} \underset{p\to+\infty}{\sim} \frac{\log(p)}{p^2} = O\left(\frac{1}{p^{\frac{3}{2}}}\right)$$

et donc, par comparaison avec une série de Riemann convergente, on a

$$\sum\log(p)\frac{1}{p^2}\frac{1}{1-\frac{1}{p}}$$

est absolument convergente. Il en résulte que

$$L_1(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n} = \sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p} + O(1)$$

Proposition 6. On a :

$$\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p}=\begin{cases}O(1) & \text{si } L(\chi)\neq 0\\ -\log(x)+O(1) & \text{si } L(\chi)=0\end{cases}$$

Preuve de la proposition 6. Il découle, d'après les théorème 10 et 11, que :

$$\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p}=L_1(\chi)\sum_{n\leqslant x}\frac{\mu(n)\chi(n)}{n}+O(1)$$

Ainsi, on obtient :

$$\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p}=\begin{cases}O(1) & \text{si } L(\chi)\neq 0\\ -\log(x)+O(1) & \text{si } L(\chi)=0\end{cases}$$

Théorème 12.

$$\#G(N)\sum_{\substack{p\leqslant x\\ p\equiv 1[N]}}\frac{\chi(p)\log(p)}{p}=\log(x)+O(1)$$

Preuve du théorème 12. Soit T le nombre de caractères non triviaux tels que $L(\chi)=0$. Montrons d'abord que :

$$\#G(N).\sum_{\substack{p\leqslant x\\ p\equiv 1[N]}}\frac{\chi(p)\log(p)}{p}=(1-T)\log(x)+O(1)$$

Ensuite, nous montrerons que $T\leqslant 1$.

D'après la formule de Mertens, si χ est trivial, on a :

$$\begin{aligned}\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p} &= \sum_{p\leqslant x}\frac{\log(p)}{p}\\ &= \log(x)+O(1)\end{aligned}$$

En utilisant le résultat précédent, on obtient :

$$\sum_{\chi\in G(N)}\sum_{p\leqslant x}\frac{\chi(p)\log(p)}{p}=(1-T)\log(x)+O(1)$$

Comme nous avons affaire à des sommes finies, on peut échanger les sommes. Ainsi :

$$\#G(N) \sum_{\substack{p\leqslant x \\ p\equiv 1[N]}} \frac{\chi(p)\log(p)}{p} = (1-T)\log(x) + O(1)$$

Puisque le membre de gauche est positif, étant une somme de termes positifs, le membre de droite l'est également, et donc $T \leqslant 1$.

Montrons maintenant $T = 0$, pour conclure.

Si χ est non trivial et à valeurs réelles, alors $L(\chi) \neq 0$.

D'après la propostion 7, si χ n'est pas à valeurs réelles, alors $\overline{\chi}$est distinct de χ et $L(\overline{\chi}) = \overline{L(\chi)}$, de sorte que les deux sont simultanément nuls ou non. Comme $T \leqslant 1$, aucun des deux n'est nul et finalement

$$T = 0$$

Théorème 13. (Théorème de Dirichlet) Soit l un entier premier à N, Alors

$$\{p \,\text{premier}\, / p \equiv l[N]\} \,\text{est infini}\,.$$

Preuve du théorème 13. On déduit de ce qui précède que, pour un caractère χ non trivial, on a :

$$\sum_{p\leqslant x} \frac{\chi(p)\log(p)}{p} = O(1)$$

Donc,

$$\begin{aligned} \sum_{\chi\in G(N)} \sum_{p\leqslant x} \bar{\chi}(l) \frac{\chi(p)\log(p)}{p} &= \sum_{p\leqslant x} \frac{\log(p)}{p} \\ &= \log(x) + O(1) \end{aligned}$$

Puisque l est premier à N, on dispose d'une relation de Bézout, c'est-à-dire qu'il existe $a, b \in \mathbb{Z}$ tel que

$$a.l + b.N = 1$$

Cela implique que

$$\chi(a)\chi(l) = 1$$

De plus, si d est l'ordre de la classe de l modulo N dans $G(N)$ alors

$$l^d \equiv 1[N]$$

ce qui implique que

$$\chi(l)^d = \chi(1) = 1$$

Ainsi, $\chi(l)$ est une racine de l'unité, et donc

$$\sum_{\chi \in G(N)} \bar{\chi}(l)\chi(p) = \sum_{\chi \in G(N)} \chi(a.p)$$

Cette dernière somme est nulle sauf si $a.p \equiv 1[N]$, auquel cas elle vaut $\#G(N)$.

D'après l'étude des groupes finis, on a :

$$a.p \equiv 1[N] \text{ si and seulement si } p \equiv l[N]$$

et donc

$$\sum_{p \leqslant x} \sum_{\chi \in G(N)} \bar{\chi}(l) \frac{\chi(p)\log(p)}{p} = \#G(N) \sum_{\substack{p \leqslant x \\ p \equiv l[N]}} \frac{\log(p)}{p}$$

Si l'ensemble $\{p \text{ premier } / p \equiv l[N]\}$ est fini, alors la seconde somme est bornée (et même constante) au voisinage de l'infini, et elle ne pourrait donc être équivalente à $\log(x)$

Par conséquent,

$$\{p \text{ premier } / p \equiv l[N]\}$$

est infini.

Généralisations. 1. La conjecture de Bunyakovsky généralise le théorème de Dirichlet aux polynômes de degré supérieur. Par exemple, déterminer si des polynômes simples comme $x^2 + 1$ (connu dans le cadre du quatrième problème de Landau) atteignent une infinité de valeurs premières est un problème ouvert important.

2. La conjecture de Dickson généralise le théorème de Dirichlet à plus d'un polynôme.

3. L'hypothèse de Schinzel (H) généralise ces deux conjectures, c'est-à-dire qu'elle s'applique à plusieurs polynômes, chacun pouvant avoir un degré supérieur à un.

4. Dans la théorie algébrique des nombres, le théorème de Dirichlet se généralise au théorème de densité de Chebotarev.

5. Le théorème de Linnik (1944) concerne la taille du plus petit nombre premier dans une progression arithmétique donnée. Linnik a prouvé que la progression $a + nd$ (pour n variant parmi les entiers positifs) contient un nombre premier de magnitude au plus $c \cdot d^L$, pour certaines constantes absolues c et L. Des recherches ultérieures ont permis de réduire L à 5.

6. Un analogue du théorème de Dirichlet existe dans le cadre des systèmes dynamiques (T. Sunada et A. Katsuda, 1990).

Cinquième partie

Annexe

Dans cette section, nous vous proposons les corrigés détaillés de quatre épreuves de Mathématiques pour la filière MP-MPI, visant à fournir une compréhension approfondie et des techniques de résolution rigoureuses pour les concours de haut niveau. Ces corrigés incluent :

1. Corrigé de l'épreuve Mathématiques A - XLSR - Filière MP-MPI 2024
2. Corrigé de l'épreuve Mathématiques A - XLSR - Filière MP-MPI 2023
3. Épreuve des Écoles Normales Supérieures - Concours d'Admission 2018 - Filière MPI - Composition de Mathématiques C (ULCR)
4. Agrégation Externe 2019 - Autour du théorème de Fermat-Wiles

Ces épreuves constituent une excellente préparation aux concours post-prépas. Elles couvrent de nombreux concepts classiques et approfondissent des notions mathématiques essentielles, permettant ainsi de renforcer la compréhension théorique et les capacités d'analyse.

Corrigé de l'épreuve mathématiques A - XLSR - Filière MP-MPI 2024

SABIR ilyass - ETTOUSY BADR

⋆ ⋆ ⋆

Pramière partie

1.a. Montrons que $-M_0$ est diagonalisable.

Le polynôme caractéristique de $-M_0$ est :

$$\begin{aligned}\chi_{-M_0}(X) &= \det(XI_n + M_0)\\ &= \begin{vmatrix} X & 1 & . & . & . & 1 & 1 \\ 1 & X & & & & . & . \\ 1 & 1 & . & & & . & . \\ . & . & & . & & . & . \\ . & . & & & . & & \\ . & . & & & & X & 1 \\ 1 & 1 & . & . & . & 1 & X \end{vmatrix}\end{aligned}$$

On a alors

$$\chi_{-M_0}(1) = 0$$

Donc 1 est une valeur propre associée à $-M_0$, et le sous-espace propre E_1 de $-M_0$ associé à la valeur propre 1 est :

$$\begin{aligned}E_1 &= \ker(-M_0 - I_n)\\ &= \ker(M_0 + I_n)\end{aligned}$$

Soit $x = \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix} \in \mathbb{R}^n$, on a :

$$\begin{aligned} x \in E_1 &\Leftrightarrow (M_0 + I_n)x = 0 \\ &\Leftrightarrow x_1 + \cdots + x_n = 0 \\ &\Leftrightarrow x \in H := \left\{ \begin{pmatrix} y_1 \\ . \\ . \\ . \\ y_n \end{pmatrix} \in \mathbb{R}^n | y_1, \ldots, y_n \in \mathbb{R} \text{ tel que } \sum_{k=1}^{n} y_k = 0 \right\} \end{aligned}$$

Et cela pour tout $x \in \mathbb{R}^n$, d'où

$$E_1 = H$$

Or, H est un hyperplan, donc $\dim E_1 = \dim H = n - 1$.

Ainsi, 1 est une valeur propre de $-M_0$ d'ordre de multiplicité $n - 1$.

La somme des valeurs propres est la trace de $-M_0$, donc $1 - n$est aussi une valeur propre de $-M_0$.

Pour tout $x = \begin{pmatrix} x_1 \\ . \\ . \\ . \\ x_n \end{pmatrix} \in \mathbb{R}^n$, on a :

$$\begin{aligned} x \in E_{1-n} &\Leftrightarrow (-M_0 + (n-1)I_n)x = 0 \\ &\Leftrightarrow \forall i \in [\![1,n]\!], (n-1)x_i = \sum_{\substack{k=1 \\ k\neq i}}^{n} x_k \\ &\Leftrightarrow x_1 = x_2 = \cdots = x_n \\ &\Leftrightarrow x \in \text{vect} \left(\begin{pmatrix} 1 \\ 1 \\ . \\ . \\ . \\ 1 \end{pmatrix} \right) \end{aligned}$$

Ainsi,

$$E_{1-n} = \text{vect} \left(\begin{pmatrix} 1 \\ 1 \\ . \\ . \\ . \\ 1 \end{pmatrix} \right)$$

Puisque $\dim E_1 + \dim E_{1-n} = n$, alors $-M_0$ est diagonalisable, de valeurs propres 1 et $1-n$.

1.b. Pour tout $x \in \mathbb{R}$, on a, par la définition du déterminant :

$$\det(xI_n + M_0) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} (xI_n + M_0)_{\sigma(i),i}$$

Or, pour tout $i \in [\![1,n]\!]$,

$$(xI_n + M_0)_{\sigma(i),i} = \begin{cases} 1 \text{ si } \sigma(i) \neq i \\ x \text{ si } \sigma(i) = i \end{cases}$$

Alors,

$$\begin{aligned}\det(xI_n + M_0) &= \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \prod_{i\in\boldsymbol{\nu}(\sigma)} x \\ &= \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) x^{\boldsymbol{\nu}(\sigma)}\end{aligned}$$

D'autre part, d'après la question précédente

$$\det(xI_n + M_0) = (x-1)^{n-1}(x-(1-n))$$

D'où

$$\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) x^{\boldsymbol{\nu}(\sigma)} = (x-1)^{n-1}(x+n-1)$$

2. D'après la question précédente, on a
Pour $x = 1$:

$$\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) = 0$$

D'autre part, en dérivant la fonction $x \longmapsto \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) x^{\boldsymbol{\nu}(\sigma)}$, on obtient :

$$\sum_{\substack{\sigma\in\mathcal{S}_n \\ \boldsymbol{\nu}(\sigma)\geqslant 1}} \varepsilon(\sigma)\boldsymbol{\nu}(\sigma) x^{\boldsymbol{\nu}(\sigma)-1} = (n-1)(x-1)^{n-2}(x+n-1) + (x-1)^{n-1}$$

Au point $x = 1$, on a :

$$\sum_{\substack{\sigma\in\mathcal{S}_n \\ \boldsymbol{\nu}(\sigma)\geqslant 1}} \varepsilon(\sigma)\boldsymbol{\nu}(\sigma) = \begin{cases} 0 \text{ si } n \geqslant 3 \\ 2 \text{ si } n = 2 \end{cases}$$

D'où

$$\begin{aligned}\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma)\boldsymbol{\nu}(\sigma) &= \sum_{\substack{\sigma\in\mathcal{S}_n \\ \boldsymbol{\nu}(\sigma)\geqslant 1}} \varepsilon(\sigma)\boldsymbol{\nu}(\sigma) \\ &= \begin{cases} 0 \text{ si } n \geqslant 3 \\ 2 \text{ si } n = 2 \end{cases}\end{aligned}$$

De plus, pour tout $x \in \mathbb{R}$, on a :

$$\int_0^x \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) t^{\boldsymbol{\nu}(\sigma)} dt = \int_0^x (t-1)^{n-1}(t+n-1)dt$$

Or

$$\begin{aligned}\int_0^x \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) t^{\boldsymbol{\nu}(\sigma)} dt &= \sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) \int_0^x t^{\boldsymbol{\nu}(\sigma)} dt \\ &= \sum_{\sigma\in\mathcal{S}_n} \frac{\varepsilon(\sigma)}{1+\boldsymbol{\nu}(\sigma)} x^{\boldsymbol{\nu}(\sigma)+1}\end{aligned}$$

Et

$$\begin{aligned}\int_0^x (t-1)^{n-1}(t+n-1)dt &= \int_0^x (t-1)^n + n(t-1)^{n-1} dt \\ &= \frac{(x-1)^{n+1}}{n+1} + (x-1)^n + (-1)^{n-1}\frac{n}{n+1}\end{aligned}$$

D'où

$$\sum_{\sigma\in\mathcal{S}_n} \frac{\varepsilon(\sigma)}{1+\boldsymbol{\nu}(\sigma)} x^{\boldsymbol{\nu}(\sigma)+1} = \frac{(x-1)^{n+1}}{n+1} + (x-1)^n + (-1)^{n-1}\frac{n}{n+1}$$

Au point $x = 1$, on a

$$\sum_{\sigma\in\mathcal{S}_n} \frac{\varepsilon(\sigma)}{1+\boldsymbol{\nu}(\sigma)} = (-1)^{n-1}\frac{n}{n+1}$$

3. On a :

$$\begin{aligned}\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) &= \sum_{\substack{\sigma\in\mathcal{S}_n \\ \varepsilon(\sigma)=1}} \varepsilon(\sigma) + \sum_{\substack{\sigma\in\mathcal{S}_n \\ \varepsilon(\sigma)=-1}} \varepsilon(\sigma) \\ &= \mathrm{Card}\{\sigma\in\mathcal{S}_n : \varepsilon(\sigma)=1\} - \mathrm{Card}\{\sigma\in\mathcal{S}_n : \varepsilon(\sigma)=-1\}\end{aligned}$$

D'après la question précédente, on a $\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) = 0$.

Par suite,

$$\mathrm{Card}\{\sigma\in\mathcal{S}_n : \varepsilon(\sigma)=1\} = \mathrm{Card}\{\sigma\in\mathcal{S}_n : \varepsilon(\sigma)=-1\}$$

D'où la probabilité qu'une permutation de $\mathcal{S}_n$ tirée uniformément au hasard, soit de signature donnée est $\frac{1}{2}$.

4. Soit $\sigma\in\mathcal{S}_n$.

On a $\sigma\in\mathcal{D}_n$ si et seulement si $\boldsymbol{\nu}(\sigma) = 0$.

Et

$$\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma) x^{\boldsymbol{\nu}(\sigma)} = \sum_{\sigma\in\mathcal{D}_n} \varepsilon(\sigma) + \sum_{\sigma\in\mathcal{S}_n\setminus\mathcal{D}_n} \varepsilon(\sigma) x^{\boldsymbol{\nu}(\sigma)}$$

Au point $x = 0$, on a

$$\begin{aligned}\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma)x^{\boldsymbol{\nu}(\sigma)}\Big|_{x=0} &= \sum_{\sigma\in\mathcal{D}_n} \varepsilon(\sigma) \\ &= \mathrm{Card}\{\sigma \in \mathcal{D}_n : \varepsilon(\sigma) = 1\} - \mathrm{Card}\{\sigma \in \mathcal{D}_n : \varepsilon(\sigma) = -1\}\end{aligned}$$

D'autre part,

$$\begin{aligned}\sum_{\sigma\in\mathcal{S}_n} \varepsilon(\sigma)x^{\boldsymbol{\nu}(\sigma)}\Big|_{x=0} &= (x-1)^{n-1}(x+n-1)|_{x=0} \\ &= (-1)^{n-1}(n-1)\end{aligned}$$

Ainsi,

$$\mathrm{Card}\{\sigma \in \mathcal{D}_n : \varepsilon(\sigma) = 1\} - \mathrm{Card}\{\sigma \in \mathcal{D}_n : \varepsilon(\sigma) = -1\} = (-1)^{n-1}(n-1)$$

D'où le résultat.

5.a. Soit $m \in \mathbb{N}$. On a $(1, X, \dots, X^m)$ (resp. $(1, (X-1), \dots, (X-1)^m)$) est une famille de polynômes non nuls échelonnée en degré. Donc, elle est libre, avec un cardinal égal à $m + 1 = \dim(\mathbb{R}_m[X])$.

Ainsi, elle est une base de $\mathbb{R}_m[X]$.

5.b. Il suffit de montrer que M est la matrice de passage de la base $(1, (X-1), \dots, (X-1)^m)$ à la base $(1, X, \dots, X^m)$.

On a, pour tout $k \in [\![0, m]\!]$,

$$X^k = ((X-1)+1)^k = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} (X-1)^i$$

D'où le résultat.

5.c. Puisque M est une matrice de passage, alors elle est inversible, et son inverse M^{-1} est la matrice de passage de la base $(1, X, \dots, X^m)$ à la base $(1, (X-1), \dots, (X-1)^m)$.

On a, pour tout $k \in [\![0, m]\!]$,

$$(X-1)^k = \sum_{i=0}^{k} \begin{pmatrix} k \\ i \end{pmatrix} (-1)^{k-i} X^i$$

D'où

$$M^{-1} = \left(\begin{pmatrix} k \\ i \end{pmatrix} (-1)^{k-i} \right)_{(i,k) \in [\![1,n]\!]^2}$$

5.d. Soient $(u_0, \ldots, u_m), (v_0, \ldots, v_m) \in \mathbb{R}^{m+1}$, tels que pour tout $k \leqslant m$,

$$u_k = \sum_{l=0}^{k} \begin{pmatrix} k \\ l \end{pmatrix} v_l$$

Montrons que pour tout $k \leqslant m$, on a

$$v_k = \sum_{l=0}^{k} (-1)^{k-l} \begin{pmatrix} k \\ l \end{pmatrix} u_l$$

On a

$$\begin{pmatrix} u_0 \\ . \\ . \\ . \\ u_m \end{pmatrix} = \begin{pmatrix} \sum_{l=0}^{m} \begin{pmatrix} 0 \\ l \end{pmatrix} v_l \\ . \\ . \\ . \\ \sum_{l=0}^{m} \begin{pmatrix} m \\ l \end{pmatrix} v_l \end{pmatrix}$$

$$= M \begin{pmatrix} v_0 \\ . \\ . \\ . \\ v_m \end{pmatrix}$$

Donc

$$\begin{pmatrix} v_0 \\ . \\ . \\ . \\ v_m \end{pmatrix} = M^{-1} \begin{pmatrix} u_0 \\ . \\ . \\ . \\ u_m \end{pmatrix} = \begin{pmatrix} \sum_{l=0}^{m} (-1)^{0-l} \begin{pmatrix} 0 \\ l \end{pmatrix} u_l \\ . \\ . \\ . \\ \sum_{l=0}^{m} (-1)^{m-l} \begin{pmatrix} m \\ l \end{pmatrix} u_l \end{pmatrix}$$

D'où le résultat.

6. Soit $n \in \mathbb{N}^*$. Soit $k \in [\![0, n]\!]$,

Notons, pour tout $l \in [\![0, k]\!]$, $\mathcal{F}_l$: l'ensemble des permutations de $\mathcal{S}_k$ ayant exactement l points fixes.

On a $\{\mathcal{F}_0, \ldots, \mathcal{F}_k\}$ forme une partition de $\mathcal{S}_k$, en particulier :

$$\sum_{l=0}^{k} \mathrm{Card}(\mathcal{F}_l) = k!$$

D'autre part :

$$\begin{aligned} \mathrm{Card}(\mathcal{F}_l) &= \begin{pmatrix} k \\ l \end{pmatrix} \mathrm{Card}(\mathcal{D}_k) \\ &= \begin{pmatrix} k \\ l \end{pmatrix} D_{l-k} \\ &= \begin{pmatrix} k \\ l-k \end{pmatrix} D_{l-k} \end{aligned}$$

Avec la convention

$$D_0 = \mathrm{Card}(\mathcal{D}_0) = 1$$

D'où :

$$\sum_{l=0}^{k} \begin{pmatrix} k \\ l \end{pmatrix} D_k = k!$$

En utilisant la question précédente, on a :

$$\begin{aligned} D_n &= \sum_{k=0}^{n}(-1)^{n-k}\left(\begin{array}{c} n \\ k \end{array}\right)k! \\ &= n!\sum_{k=0}^{n}\frac{(-1)^{n-k}}{(n-k)!} \\ &= n!\sum_{k=0}^{n}\frac{(-1)^{k}}{k!} \end{aligned}$$

7.a. Soit $n \geqslant 2$, on a

$$Y_n(\mathcal{D}_n) = \{-1, 1\}$$

Pour $\varepsilon \in \{-1, 1\}$, on a

$$\mathbb{P}(Y_n = \varepsilon) = \frac{\text{card}\{\sigma \in \mathcal{D}_n : \varepsilon(\sigma) = \varepsilon\}}{D_n}$$

Or, d'après la question 4, on a

$$\mathbb{P}(Y_n = 1) = \mathbb{P}(Y_n = -1) + \frac{(-1)^{n-1}(n-1)}{D_n}$$

Donc,

$$\mathbb{P}(Y_n = 1) = \frac{1}{2} + \frac{(-1)^{n-1}(n-1)}{2D_n}$$

Et

$$\mathbb{P}(Y_n = -1) = \frac{1}{2} - \frac{(-1)^{n-1}(n-1)}{2D_n}$$

D'où

$$\mathbb{P}(Y_n = \varepsilon) = \frac{1}{2} + \varepsilon\frac{(-1)^{n-1}(n-1)}{2D_n}$$

7.b. Soit $\varepsilon \in \{-1, 1\}$, on a pour tout $n \geqslant 2$:

$$\frac{(-1)^{n-1}(n-1)}{2D_n} = \frac{(-1)^{n-1}(n-1)}{n!\sum\limits_{k=0}^{n}\frac{(-1)^k}{k!}}$$

Or,

$$\sum_{k=0}^{n}\frac{(-1)^{k}}{k!} \underset{n\to+\infty}{\sim} \frac{1}{e}$$

Donc

$$\frac{(-1)^{n-1}(n-1)}{2D_n} \underset{n\to+\infty}{\sim} \frac{(-1)^{n-1}(n-1)}{2en!}$$

Avec

$$\lim_{n\to+\infty} \frac{(-1)^{n-1}(n-1)}{2en!} = 0$$

D'où

$$\lim_{n\to+\infty} \frac{(-1)^{n-1}(n-1)}{2D_n} = 0$$

Ainsi, $\lim_{n\to+\infty} \mathbb{P}(Y_n = \varepsilon)$ existe et on a :

$$\lim_{n\to+\infty} \mathbb{P}(Y_n = \varepsilon) = \frac{1}{2}$$

8.a. On a

$$Z_n(\mathcal{S}_n) = [\![0, n]\!]$$

Et pour tout $k \in [\![0, n]\!]$, on a :

$$\begin{aligned}
\mathbb{P}(Z_n = k) &= \frac{\mathrm{Card}\{\sigma \in \mathcal{S}_n : \boldsymbol{\nu}(\sigma) = k\}}{n!} \\
&= \frac{\begin{pmatrix} n \\ k \end{pmatrix} D_{n-k}}{n!} \\
&= \frac{1}{k!} \sum_{l=0}^{n-k} \frac{(-1)^l}{l!}
\end{aligned}$$

8.b. On a

$$\lim_{n\to+\infty} \mathbb{P}(Z_n = k) = \frac{1}{ek!}$$

8.c. Le nombre moyen de points fixes d'une permutation aléatoire est l'espérence de Z_n.

Et on a :

$$\begin{aligned}
\mathbb{E}[Z_n] &= \sum_{k=0}^{n} k\mathbb{P}(Z_n = k) \\
&= \sum_{k=0}^{n} k \frac{1}{k!} \sum_{l=0}^{n-k} \frac{(-1)^l}{l!} \\
&= \sum_{k=1}^{n} \frac{1}{(k-1)!} \sum_{l=0}^{n-k} \frac{(-1)^l}{l!}
\end{aligned}$$

Or, pour tout $k \in \mathbb{N}$, on a :

$$\lim_{n\to+\infty} k\mathbb{P}(Z_n = k) = \begin{cases} \frac{1}{e(k-1)!} & \text{si } k > 0 \\ 0 & \text{si } k = 0 \end{cases}$$

D'autre part, on a :

$$\sum_{k=0}^{n} k\mathbb{P}(Z_n = k) = \sum_{k=0}^{+\infty} k\mathbb{P}(Z_n = k)\mathbf{1}_{[n,+\infty[}(k)$$

La somme est finie à termes positifs, donc :

$$\begin{aligned}\lim_{n\to+\infty}\sum_{k=0}^{+\infty} k\mathbb{P}(Z_n = k)\mathbf{1}_{[n,+\infty[}(k) &= \sum_{k=0}^{+\infty}\lim_{n\to+\infty} k\mathbb{P}(Z_n = k)\mathbf{1}_{[n,+\infty[}(k)\\ &= \sum_{k=1}^{+\infty}\frac{1}{e(k-1)!}\\ &= 1\end{aligned}$$

D'où

$$\lim_{n\to+\infty}\mathbb{E}[Z_n] = 1$$

9. Par un calcul simple, on obtient :

$$\begin{cases}\frac{1}{2!}\sum\limits_{\sigma\in\mathcal{S}_2}\omega(\sigma) = \frac{3}{2}\\ \frac{1}{3!}\sum\limits_{\sigma\in\mathcal{S}_3}\omega(\sigma) = \frac{11}{6}\\ \frac{1}{4!}\sum\limits_{\sigma\in\mathcal{S}_4}\omega(\sigma) = \frac{50}{24}\end{cases}$$

10. Soit $n \geqslant 2$, on a $s(n,n)$, est le nombre de permutations σ de $\mathcal{S}_n$tel que $\omega(\sigma) = n$, donc $l_{\omega(\sigma)} = 1$.

D'où $\sigma = \mathrm{id}_{\mathcal{S}_n}$, par conséquent :

$$s(n,n) = 1$$

Et $s(n,1)$ est le nombre de permutations σ de $\mathcal{S}_n$tel que $\omega(\sigma) = 1$, c'est-à-dire $l_{\omega(\sigma)} = n$.

Il existe $(n-1)!$ permutations σ de $\mathcal{S}_n$telles que $\omega(\sigma) = 1$ (cycle de longueur n).

D'où

$$s(n,1) = (n-1)!$$

Pour tout $k \in [\![2, n-1]\!]$, on a $s(n,k)$ est le nombre de permutations σ de $\mathcal{S}_n$telles que $\omega(\sigma) = k$.

Montrons que

$$s(n,k) = s(n-1,k-1) + (n-1)s(n-1,k)$$

Si $\omega(\sigma) = k$ et sans déplacer n, donc n est fixé par σ, alors la restriction de σ à $\mathcal{S}_{n-1}$ vérifie $\omega(\sigma') = k-1$, donc il y a $s(n-1,k-1)$ permutations qui vérifient cette condition.

Si $\omega(\sigma) = k$ par déplacement de n, alors il y a $(n-1)$possibilités pour la position de $\sigma(n)$. Après avoir choisi la position de n, les $n-1$ autres éléments forment une bijection isomorphe à une permutation σ' de $\mathcal{S}_{n-1}$ tel que $\omega(\sigma') = k$.

Donc il y a $(n-1)s(n-1,k)$ permutations qui vérifient cette condition.

D'où

$$s(n,k) \quad = \quad s(n-1,k-1) + (n-1)s(n-1,k)$$

11. Soit $x \in \mathbb{R}$. Posons, pour tout $j \in \mathbb{N}^*$,

$$\kappa_j(x) = \sum_{k=1}^{j} s(j,k)x^k$$

On a pour tout $n \in \mathbb{N}^*$:

$$\begin{aligned}
\kappa_n(x) &= S(n,n)x^n + S(n,1)x + \sum_{k=2}^{n-1}(s(n-1,k-1) + (n-1)s(n-1,k))x^k \\
&= x^n + (n-1)!x + \sum_{k=2}^{n-1} s(n-1,k-1)x^k + (n-1)\sum_{k=2}^{n-1} s(n-1,k)x^k \\
&= x^n + (n-1)!x + x\sum_{k=1}^{n-2} s(n-1,k)x^k + (n-1)\sum_{k=2}^{n-1} s(n-1,k)x^k \\
&= x^n + (n-1)!x + x(\kappa_{n-1}(x) - s(n-1,n-1)x^{n-1}) + (n-1)(\kappa_{n-1}(x) - s(n-1,1)x) \\
&= (x+n-1)\kappa_{n-1}(x)
\end{aligned}$$

Par téléscopage, on en déduit :

$$\begin{aligned}
\kappa_n(x) &= \kappa_1(x)\prod_{i=2}^{n}(x+i-1) \\
&= x\prod_{i=1}^{n-1}(x+i) \\
&= \prod_{i=0}^{n-1}(x+i)
\end{aligned}$$

12. On a, pour tout $n \in \mathbb{N}^*$:

$$\begin{aligned}\mathbb{E}[X_n] &= \sum_{k=0}^{n} k\mathbb{P}(X_n = k) \\ &= \frac{1}{n!}\sum_{k=0}^{n} k \,\mathrm{Card}\{\sigma \in \mathcal{S}_n : \omega(\sigma) = k\} \\ &= \frac{1}{n!}\sum_{k=0}^{n} k s(n,k)\end{aligned}$$

Or, d'après la question précédente, pour tout $x \in \mathbb{R}$,

$$\sum_{k=1}^{n} k s(n,k) x^{k-1} = \sum_{k=0}^{n-1}\prod_{\substack{i=0 \\ i\neq k}}^{n-1} (x+i)$$

En particulier, pour $x = 1$, on a :

$$\begin{aligned}\sum_{k=1}^{n} k s(n,k) &= \sum_{k=0}^{n-1}\prod_{\substack{i=0 \\ i\neq k}}^{n-1} (1+i) \\ &= \sum_{k=0}^{n-1} \frac{n!}{k+1} \\ &= n!\sum_{k=1}^{n} \frac{1}{k}\end{aligned}$$

Par suite,

$$\mathbb{E}[X_n] = \sum_{k=1}^{n} \frac{1}{k}$$

Or,

$$\sum_{k=1}^{n} \frac{1}{k} \underset{n\to+\infty}{=} \ln(n) + \gamma + O\left(\frac{1}{n}\right)$$

Alors,

$$\mathbb{E}[X_n] \underset{n\to+\infty}{=} \ln(n) + \gamma + O\left(\frac{1}{n}\right)$$

13.a. D'après la question 11, pour tout $n \in \mathbb{N}^*$,

$$\sum_{k=2}^{n} k(k-1) s(n,k) x^{k-2} = \sum_{k=0}^{n-1}\sum_{\substack{j=0 \\ j\neq k}}^{n-1}\prod_{\substack{i=0 \\ i\neq k,j}}^{n-1} (x+i)$$

En particulier,

$$\begin{aligned}\sum_{k=2}^{n} k(k-1)s(n,k) &= \sum_{k=0}^{n-1}\sum_{\substack{j=0\\ j\neq k}}^{n-1}\prod_{\substack{i=0\\ i\neq k,j}}^{n-1}(1+i)\\ &= \sum_{k=0}^{n-1}\sum_{\substack{j=0\\ j\neq k}}^{n-1}\frac{n!}{(k+1)(j+1)}\\ &= n!\sum_{k=0}^{n-1}\left(\sum_{j=0}^{n-1}\frac{1}{(k+1)(j+1)}-\frac{1}{(k+1)^2}\right)\\ &= n!\left(\sum_{k=1}^{n}\sum_{j=1}^{n}\frac{1}{kj}-\sum_{k=1}^{n}\frac{1}{k^2}\right)\end{aligned}$$

D'où le résultat.

13.b. Pour tout $n \in \mathbb{N}^*$, on a :

$$\begin{aligned}\sum_{k=2}^{n} k^2 s(n,k) &= \sum_{k=2}^{n} k(k-1)s(n,k) + \sum_{k=1}^{n} ks(n,k)\\ &= \mathbb{E}[X_n] + \sum_{k=1}^{n}\sum_{j=1}^{n}\frac{1}{kj} - \sum_{k=1}^{n}\frac{1}{k^2}\end{aligned}$$

14.a. On a, pour tout $n \in \mathbb{N}^*$,

$$\begin{aligned}\frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\omega(\sigma)^2 &= \frac{1}{n!}\sum_{k=1}^{n} k^2 s(n,k)\\ &= \mathbb{E}[X_n] + \sum_{k=1}^{n}\sum_{j=1}^{n}\frac{1}{kj} - \sum_{k=1}^{n}\frac{1}{k^2}\end{aligned}$$

Or,

$$\begin{aligned}\sum_{k=1}^{n}\sum_{j=1}^{n}\frac{1}{kj} &= \left(\sum_{k=1}^{n}\frac{1}{k}\right)^2\\ &\underset{n\to+\infty}{=} \left(\ln(n)+\gamma+O\left(\frac{1}{n}\right)\right)^2\\ &\underset{n\to+\infty}{=} \ln(n)^2+\gamma^2+O\left(\frac{1}{n}\right)^2+2\gamma\ln(n)+2O\left(\frac{\ln(n)}{n}\right)+2\gamma O\left(\frac{1}{n}\right)\end{aligned}$$

On a l'existence des suites $(\varepsilon_{j,n})_{n\in\mathbb{N}}$ bornées pour tout $j=1,2,3$ telles que :

$$\begin{cases} O\left(\frac{1}{n}\right)^2 = \frac{\varepsilon_{1,n}}{n^2} \\ O\left(\frac{1}{n}\right) = \frac{\varepsilon_{2,n}}{n} \\ O\left(\frac{\ln(n)}{n}\right) = \frac{\ln(n)}{n}\varepsilon_{3,n} \end{cases}$$

Donc,

$$\begin{aligned} \sum_{k=1}^{n}\sum_{j=1}^{n}\frac{1}{kj} &\underset{n\to+\infty}{=} \ln(n)^2+\gamma^2+2\gamma\ln(n)+\frac{\varepsilon_{1,n}}{n^2}+2\frac{\varepsilon_{2,n}}{n}+2\frac{\ln(n)}{n}\varepsilon_{3,n} \\ &\underset{n\to+\infty}{=} \ln(n)^2+\gamma^2+2\gamma\ln(n)+\frac{\ln(n)}{n}\left(\frac{\varepsilon_{1,n}}{n\ln(n)}+2\frac{\varepsilon_{2,n}}{\ln(n)}+2\varepsilon_{3,n}\right) \end{aligned}$$

Avec $\left(\frac{\varepsilon_{1,n}}{n\ln(n)}+2\frac{\varepsilon_{2,n}}{\ln(n)}+2\varepsilon_{3,n}\right)_{n\in\mathbb{N}}$ est une suite bornée. Alors,

$$\sum_{k=1}^{n}\sum_{j=1}^{n}\frac{1}{kj} \underset{n\to+\infty}{=} \ln(n)^2+\gamma^2+2\gamma\ln(n)+O\left(\frac{\ln(n)}{n}\right)$$

Or,

$$\begin{aligned} \mathbb{E}[X_n] &\underset{n\to+\infty}{=} \ln(n)+\gamma+O\left(\frac{1}{n}\right) \\ &\underset{n\to+\infty}{=} \ln(n)+\gamma+O\left(\frac{\ln(n)}{n}\right) \end{aligned}$$

Et,

$$\begin{aligned} \sum_{k=1}^{n}\frac{1}{k^2} &\underset{n\to+\infty}{=} \frac{\pi^2}{6}+o(1) \\ &\underset{n\to+\infty}{=} \frac{\pi^2}{6}+O\left(\frac{\ln(n)}{n}\right) \end{aligned}$$

D'où,

$$\frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\omega(\sigma)^2 \underset{n\to+\infty}{=} (2\gamma+1)\ln(n)+\gamma^2+\gamma-\frac{\pi^2}{6}+\ln(n)^2+O\left(\frac{\ln(n)}{n}\right)$$

D'où,

$$c=\gamma^2+\gamma-\frac{\pi^2}{6}$$

14.b. On a :

$$\begin{aligned} \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}(\omega(\sigma)-\ln(n))^2 &= \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\omega(\sigma)^2-2\frac{\ln(n)}{n!}\sum_{\sigma\in\mathcal{S}_n}\omega(\sigma)+\ln(n)^2 \\ &= \frac{1}{n!}\sum_{\sigma\in\mathcal{S}_n}\omega(\sigma)^2-2\ln(n)\mathbb{E}[X_n]+\ln(n)^2 \\ &\underset{n\to+\infty}{=} \ln(n)+c+O\left(\frac{\ln(n)}{n}\right) \end{aligned}$$

15. D'après l'inégalité de Markov :

$$\begin{aligned}
\mathbb{P}(|X_n - \ln(n)| > \varepsilon \ln(n)) &\leqslant \frac{\mathbb{E}[(X_n - \ln(n))^2]}{\varepsilon^2 \ln(n)^2} \\
&= \frac{1}{\varepsilon^2 \ln(n)^2} \cdot \frac{1}{n!} \sum_{\sigma \in \mathcal{S}_n} (\omega(\sigma) - \ln(n))^2 \\
&\underset{n\to+\infty}{=} \frac{1}{\varepsilon^2 \ln(n)} \left(1 + \frac{c}{\ln(n)} + O\left(\frac{1}{n}\right)\right) \\
&\underset{n\to+\infty}{=} \frac{1}{\varepsilon^2 \ln(n)}(1 + o(1))
\end{aligned}$$

Or, il existe une constante $C > 0$ telle que

$$1 + o(1) \leqslant C$$

D'où

$$\mathbb{P}(|X_n - \ln(n)| > \varepsilon \ln(n)) \leqslant \frac{C}{\varepsilon^2 \ln(n)}$$

Deuxième partie

16. Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$, on a

$$\begin{aligned}
\sum_{k=2}^{n} a_k b(k) &= \sum_{k=2}^{n} (A(k) - A(k-1)) b(k) \\
&= \sum_{k=2}^{n} A(k)b(k) - \sum_{k=3}^{n} A(k-1)b(k) \\
&= \sum_{k=2}^{n} A(k)b(k) - \sum_{k=2}^{n-1} A(k)b(k+1) \\
&= A(n)b(n) + \sum_{k=2}^{n-1} A(k)(b(k) - b(k+1)) \\
&= A(n)b(n) - \sum_{k=2}^{n-1} A(k) \int_k^{k+1} b'(t)dt \\
&= A(n)b(n) - \sum_{k=2}^{n-1} \int_k^{k+1} A(k)b'(t)dt
\end{aligned}$$

Or, pour tout $k \in [\![2, n-1]\!]$et pour tout $t \in [k, k+1]$, on a

$$A(t) = A(k)$$

D'où,

$$\begin{aligned}\sum_{k=2}^{n} a_k b(k) &= A(n)b(n) - \sum_{k=2}^{n-1} \int_k^{k+1} A(t)b'(t)dt \\ &= A(n)b(n) - \int_2^n A(t)b'(t)dt\end{aligned}$$

17.a.

Pour $n = 1$

$$\prod_{\substack{p \leqslant n \\ p \text{ premier}}} p = 1$$

Pour $n = 2$

$$\prod_{\substack{p \leqslant n \\ p \text{ premier}}} p = 2$$

Pour $n = 3$

$$\prod_{\substack{p \leqslant n \\ p \text{ premier}}} p = 6$$

17.b. Si $n$est pair et $n > 2$, alors n n'est pas premier. Par suite,

$$\begin{aligned}\prod_{\substack{p \leqslant n \\ p \text{ premier}}} p &= \prod_{\substack{p \leqslant n-1 \\ p \text{ premier}}} p \\ &\leqslant 4^{n-1} \\ &\leqslant 4^n\end{aligned}$$

17.c. Soit $n = 2m + 1$ avec $m \in \mathbb{N}$. On a :

$$\begin{aligned}m! \begin{pmatrix} 2m+1 \\ m \end{pmatrix} &= \prod_{k=m+1}^{2m+1} k \\ &= \prod_{\substack{m+1 \leqslant k \leqslant 2m+1 \\ kn' \text{ est pas premier}}} k \times \prod_{\substack{m+1 \leqslant p \leqslant 2m+1 \\ p \text{ premier}}} p\end{aligned}$$

D'où :

$$\prod_{\substack{m+1 \leqslant p \leqslant 2m+1 \\ p \text{ premier}}} p \,\text{divise}\, m! \begin{pmatrix} 2m+1 \\ m \end{pmatrix}$$

Or, pour tout p premier tel que $m + 1 \leqslant p \leqslant 2m + 1$, on a :

$$p \wedge m! = 1$$

Donc :

$$\prod_{\substack{m+1\leqslant p\leqslant 2m+1\\ p\,\text{premier}}} p\wedge m!=1$$

Ainsi :

$$\prod_{\substack{m+1\leqslant p\leqslant 2m+1\\ p\,\text{premier}}} p\,\text{divise}\left(\begin{array}{c}2m+1\\ m\end{array}\right)$$

D'autre part, on a :

$$\begin{aligned}\left(\begin{array}{c}2m+1\\ m\end{array}\right) &= \frac{1}{2}\left[\left(\begin{array}{c}2m+1\\ m\end{array}\right)+\left(\begin{array}{c}2m+1\\ m+1\end{array}\right)\right]\\ &\leqslant \frac{1}{2}\sum_{k=0}^{2m+1}\left(\begin{array}{c}2m+1\\ k\end{array}\right)\\ &= \frac{1}{2}\times 2^{2m+1}\\ &= 4^m\end{aligned}$$

17.d. D'après ce qui précède, on a :

$$\prod_{\substack{m+1\leqslant p\leqslant 2m+1\\ p\,\text{premier}}} p\,\text{divise}\left(\begin{array}{c}2m+1\\ m\end{array}\right)$$

Et

$$\left(\begin{array}{c}2m+1\\ m\end{array}\right)\leqslant 4^m$$

Donc,

$$\begin{aligned}\prod_{\substack{m+1\leqslant p\leqslant 2m+1\\ p\,\text{premier}}} p &\leqslant \left(\begin{array}{c}2m+1\\ m\end{array}\right)\\ &\leqslant 4^m\end{aligned}$$

Par suite,

$$\begin{aligned}\prod_{\substack{p\leqslant n\\ p\,\text{premier}}} p &= \prod_{\substack{p\leqslant m\\ p\,\text{premier}}} p\times\prod_{\substack{m+1\leqslant p\leqslant 2m+1\\ p\,\text{premier}}} p\\ &\leqslant 4^m\times 4^m\\ &\leqslant 4^{2m+1}\\ &= 4^n\end{aligned}$$

D'où, par récurrence forte, pour tout $n \geqslant 1$,

$$\prod_{\substack{p \leqslant n \\ p \text{ premier}}} p \leqslant 4^n$$

18. Soit $n \in \mathbb{N}^*$ et $p$un nombre premier.

On a :

$$\begin{aligned} \boldsymbol{\nu}_p(n!) &= \sum_{k=1}^{n} \boldsymbol{\nu}_p(k) \\ &= \sum_{k=1}^{n} \sum_{j=1}^{+\infty} \delta_{j,k} \end{aligned}$$

Avec, pour tous $j, k \in \mathbb{N}$,

$$\delta_{j,k} := \begin{cases} 1 & \text{si } p^j \text{ divise } k \\ 0 & \text{sinon} \end{cases}$$

Or, la somme $\sum_{k=1}^{n} \sum_{j=1}^{+\infty} \delta_{j,k}$ est finie. Ainsi,

$$\begin{aligned} \boldsymbol{\nu}_p(n!) &= \sum_{j=1}^{+\infty} \sum_{k=1}^{n} \delta_{j,k} \\ &= \sum_{j=1}^{+\infty} \text{Card}\{k \in [\![1, n]\!] | kp^j \leqslant n\} \\ &= \sum_{j=1}^{+\infty} E\left(\frac{n}{p^j}\right) \end{aligned}$$

Par suite,

$$\begin{aligned} \frac{n}{p} - 1 &\leqslant E\left(\frac{n}{p}\right) \\ &= \boldsymbol{\nu}_p(n!) \\ &= \sum_{j=1}^{+\infty} E\left(\frac{n}{p^j}\right) \\ &\leqslant \sum_{j=1}^{+\infty} \frac{n}{p^j} \\ &= \frac{n}{p} \frac{1}{1 - \frac{1}{p}} \\ &= \frac{n}{p} + \frac{n}{p(p-1)} \end{aligned}$$

D'où le résultat.

19.a. Soit $n \in \mathbb{N}^*$,

On sait que la fonction $t \longmapsto \ln(t)$ est croissante et continue sur $[1, +\infty[$, donc :

$$\sum_{k=1}^{n-1} \ln(k) \leqslant \sum_{k=1}^{n-1} \int_k^{k+1} \ln(t)dt \leqslant \sum_{k=1}^{n-1} \ln(k+1)$$

Avec

$$\begin{aligned} \sum_{k=1}^{n-1} \int_k^{k+1} \ln(t)dt &= \int_1^n \ln(t)dt \\ &= n\ln(n) - n + 1 \end{aligned}$$

Donc,

$$n\ln(n) - n + 1 \leqslant \sum_{k=1}^{n} \ln(k) \leqslant n\ln(n) + \ln(n) - n + 1$$

D'où,

$$\sum_{k=1}^{n} \ln(k) \underset{n\to+\infty}{=} n\ln(n) - n + O(\ln(n))$$

19.b. D'après le théorème fondamental de l'arithmétique et par définition de la valuation,on a

$$n! = \prod_{p \text{ premier}} p^{\boldsymbol{\nu}_p(n!)}$$

Avec pour tout $p > n$ premier $v_p(n!) = 0$ (car $p \wedge n! = 1$).

D'où

$$n! = \prod_{\substack{p \leqslant n \\ p \text{ premier}}} p^{\boldsymbol{\nu}_p(n!)}$$

Par suite

$$\ln(n!) = \sum_{\substack{p \leqslant n \\ p \text{ premier}}} \boldsymbol{\nu}_p(n!)\ln(p)$$

D'une part, on a

$$\begin{aligned} \sum_{\substack{p \leqslant n \\ p \text{ premier}}} \boldsymbol{\nu}_p(n!)\ln(p) &\leqslant \sum_{\substack{p \leqslant n \\ p \text{ premier}}} \left(\frac{n}{p} + \frac{n}{p(p-1)}\right)\ln(p) \\ &\leqslant n \sum_{\substack{p \leqslant n \\ p \text{ premier}}} \frac{\ln(p)}{p} + n \sum_{\substack{p \leqslant n \\ p \text{ premier}}} \frac{\ln(p)}{p(p-1)} \end{aligned}$$

D'autre part,

$$\begin{aligned}\sum_{\substack{p\leqslant n\\ p\,\text{premier}}} \boldsymbol{\nu}_p(n!)\ln(p) &\geqslant \sum_{\substack{p\leqslant n\\ p\,\text{premier}}} \left(\frac{n}{p}-1\right)\ln(p)\\ &\geqslant n\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p} - \sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\ln(p)\\ &= n\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p} - \ln\left(\prod_{\substack{p\leqslant n\\ p\,\text{premier}}} p\right)\\ &\geqslant n\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p} - n\ln(4)\end{aligned}$$

D'où

$$n\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p} - n\ln(4) \leqslant \ln(n!) \leqslant n\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p} + n\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p(p-1)}$$

19.c. On a

$$\frac{\ln(k)}{k(k-1)} \underset{k\to+\infty}{=} o\left(\frac{1}{k^{3/2}}\right)$$

D'où, par le critère de comparaison avec une série de Riemann, la série $\sum_{k\geqslant 2}\frac{\ln(k)}{k(k-1)}$ converge.

19.d. D'après ce qui précède, on a :

$$\frac{\ln(n!)}{n} - \sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p(p-1)} \leqslant \sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p} \leqslant \frac{\ln(n!)}{n} + \ln(4)$$

D'après la formule de Stirling :

$$\frac{\ln(n!)}{n} \underset{n\to+\infty}{=} \ln(n) + O(1)$$

Puisque $\sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{\ln(p)}{p(p-1)}$ converge (car $\sum_{k\geqslant 2}\frac{\ln(k)}{k(k-1)}$ converge).

On en déduit que :

$$\sum_{\substack{p\leqslant n\\ p\text{ premier}}} \frac{\ln(p)}{p} \underset{n\to+\infty}{=} \ln(n)+O(1)$$

20.a. Soit $n\geqslant 2$,

Pour

$$b : t\in[2,+\infty[\longmapsto \frac{1}{\ln(t)}$$

et

$$A : t\in[2,+\infty[\longmapsto \sum_{\substack{p\leqslant t\\ p\text{ premier}}} \frac{\ln(p)}{p} = \sum_{2\leqslant k\leqslant t} \frac{\ln(k)}{k}(\omega(k)-\omega(k-1))$$

D'après la question 16, pour tout $n\in\mathbb{N}$,

$$\sum_{2\leqslant k\leqslant n} \frac{\ln(k)}{k}(\omega(k)-\omega(k-1))\frac{1}{\ln(k)} = \frac{1}{\ln(n)}(R(n)+\ln(n))+\int_2^n \frac{1}{t(\ln t)^2}(R(t)+\ln(t))dt$$

Par suite,

$$\sum_{\substack{p\leqslant n\\ p\text{ premier}}} \frac{1}{p} = 1+\frac{R(n)}{\ln(n)}+\ln_2(n)-\ln_2(2)+\int_2^n \frac{R(t)}{t(\ln t)^2}dt$$

20.b. On a la fonction $t\longmapsto \frac{R(t)}{t(\ln(t))^2}$ est continue par morceaux sur $t\in[2,+\infty[$.

De plus, pour tout $t\in[2,+\infty[$:

$$\frac{R(t)}{t(\ln(t))^2} = \frac{1}{t(\ln(t))^2}\left(\sum_{\substack{p\leqslant t\\ p\text{ premier}}} \frac{\ln(p)}{p}\right)-\frac{1}{t\ln(t)}$$

Or, d'après la question 19.d, on a :

$$\begin{aligned}\sum_{\substack{p\leqslant t\\ p\text{ premier}}} \frac{\ln(p)}{p} &= \sum_{\substack{p\leqslant E(t)\\ p\text{ premier}}} \frac{\ln(p)}{p}\\ &\underset{t\to+\infty}{=} \ln(E(t))+O(1)\\ &\underset{t\to+\infty}{=} \ln(t)+O(1)\end{aligned}$$

Par suite :

$$\begin{aligned}\frac{R(t)}{t(\ln(t))^2} &\underset{t\to+\infty}{=} \frac{\ln(t)+O(1)}{t(\ln(t))^2} - \frac{1}{t\ln(t)} \\ &\underset{t\to+\infty}{=} \frac{O(1)}{t(\ln(t))^2} \\ &\underset{t\to+\infty}{=} O\left(\frac{1}{t(\ln(t))^2}\right)\end{aligned}$$

Puisque pour tout $t \geqslant 2$,

$$\int_2^t \frac{du}{u(\ln(u))^2} = \frac{1}{\ln(2)} - \frac{1}{\ln(t)}$$

Ainsi, la fonction $t \longmapsto \int_2^t \frac{du}{u(\ln(u))^2}$ admet une limite en $+\infty$.

En particulier, la fonction $t \longmapsto \int_2^t \frac{R(u)}{u(\ln(u))^2}du$ est intégrable.

20.c. D'après la question 20.a, on a :

$$\sum_{\substack{p\leqslant n \\ p\text{ premier}}} \frac{1}{p} = 1 + \frac{R(n)}{\ln(n)} + \ln_2(n) - \ln_2(2) + \int_2^n \frac{R(t)}{t(\ln t)^2}dt$$

Or, d'après la question précédente :

$$\frac{R(t)}{t(\ln(t))^2} \underset{t\to+\infty}{=} O\left(\frac{1}{t(\ln(t))^2}\right)$$

Et

$$\int_2^n \frac{1}{t(\ln(t))^2}dt \underset{n\to+\infty}{=} O\left(\frac{1}{\ln(n)}\right)$$

Alors :

$$\int_2^n \frac{R(t)}{t(\ln t)^2}dt \underset{n\to+\infty}{=} O\left(\frac{1}{\ln(n)}\right)$$

De plus, on a :

$$\begin{aligned}R(n) &= \sum_{\substack{p\leqslant t \\ p\text{ premier}}} \frac{\ln(p)}{p} - \ln(t) \\ &= \sum_{\substack{p\leqslant E(t) \\ p\text{ premier}}} \frac{\ln(p)}{p} - \ln(t) \\ &\underset{t\to+\infty}{=} \ln(E(t)) - \ln(t) + O(1) \\ &\underset{t\to+\infty}{=} O(1)\end{aligned}$$

D'où

$$\sum_{\substack{p\leqslant n\\ p\,\text{premier}}} \frac{1}{p} \underset{n\to+\infty}{=} \ln_2(n)+1-\ln_2(2)+O\left(\frac{1}{\ln(n)}\right)$$

D'où le résultat avec

$$c_1 = 1-\ln_2(2)$$

21.a. Soit $x\in[1,+\infty[$ et $q\in\mathbb{N}^*$.

On a

$$\begin{aligned}\text{Card}\{n\in\mathbb{N}\cap[1,x] : n\equiv 0(\text{mod}\,q)\} &= \text{Card}\left\{n\in\mathbb{N}\cap[1,x] : \frac{n}{q}\in\mathbb{N}\right\}\\ &= E\left(\frac{x}{q}\right)\end{aligned}$$

D'où

$$\left|\text{Card}\{n\in\mathbb{N}\cap[1,x] : n\equiv 0(\text{mod}\,q)\}-\frac{x}{q}\right|\leqslant 1$$

D'où le résultat.

21.b. On a, via la question 16 :

$$\begin{aligned}\frac{1}{E(x)}\sum_{2\leqslant n\leqslant x}\omega(n) &= \sum_{2\leqslant n\leqslant x}\frac{\omega(n)-\omega(n-1)}{n}-\int_2^{E(x)}\frac{1}{t^2}\sum_{2\leqslant n\leqslant t}\omega(n)dt\\ &= \sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{1}{p}-\int_2^{E(x)}\frac{1}{t^2}\sum_{2\leqslant n\leqslant t}\omega(n)dt\\ &\leqslant \sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{1}{p}-\int_2^{E(x)}\frac{dt}{t}\\ &= \sum_{\substack{p\leqslant n\\ p\,\text{premier}}}\frac{1}{p}-\ln(E(x))+\ln(2)\\ &\underset{x\to+\infty}{=} \ln_2(E(x))+1+\ln(2)-\ln_2(2)+O\left(\frac{1}{\ln(E(x))}\right)\\ &\underset{x\to+\infty}{=} \ln_2(x)+O(1)\end{aligned}$$

D'où :

$$\begin{aligned}\frac{1}{x}\sum_{2\leqslant n\leqslant x}\omega(n) &= \frac{E(x)}{x}\frac{1}{E(x)}\sum_{2\leqslant n\leqslant x}\omega(n)\\ &\underset{x\to+\infty}{=} \ln_2(x)+O(1)\end{aligned}$$

22.a. Pour tout $x \geqslant 2$, on a :

$$\begin{aligned}\frac{1}{x}\sum_{n\leqslant x}(\omega(n)-\ln_2(x))^2 &= \frac{1}{x}\sum_{n\leqslant x}\omega(n)^2 - 2\frac{\ln_2(x)}{x}\sum_{n\leqslant x}\omega(n) + \frac{E(x)}{x}(\ln_2(x))^2 \\ &\underset{x\to+\infty}{=} \frac{1}{x}\sum_{n\leqslant x}\omega(n)^2 - 2(\ln_2(x))^2 + O(\ln_2(x)) + (\ln_2(x))^2 \\ &\underset{x\to+\infty}{=} \frac{1}{x}\sum_{n\leqslant x}\omega(n)^2 - (\ln_2(x))^2 + O(\ln_2(x))\end{aligned}$$

22.b. Soit $x \geqslant 2$, on a :

$$\begin{aligned}\sum_{n\leqslant x}\omega(n)^2 &= \sum_{n\leqslant x}\left(\sum_{\substack{p|n\\ p\text{ premier}}} 1\right)^2 \\ &= \sum_{n\leqslant x}\sum_{\substack{p_1|n\\ p_1\text{ premier}}}\sum_{\substack{p_2|n\\ p_2\text{ premier}}} 1 \\ &= \sum_{\substack{p_1\leqslant x\\ p_1\text{ premier}}}\sum_{\substack{p_2\leqslant x\\ p_2\text{ premier}}}\left(\sum_{\substack{n\leqslant x\\ p_1|n\text{ et }p_2|n}} 1\right) \\ &= \sum_{\substack{p_1\leqslant x\\ p_1\text{ premier}}}\sum_{\substack{p_2\leqslant x\\ p_2\text{ premier}}} \operatorname{Card}\{n\in\mathbb{N}^* : n\leqslant x, p_1|n \text{ and } p_2|n\}\end{aligned}$$

22.c. Pour tout $x \geqslant 2$, on a :

$$\sum_{\substack{p_1,p_2\leqslant x\\ p_1\neq p_2\text{ premiers}}} \operatorname{Card}\{n\in\mathbb{N}^*, n\leqslant x, p_1|n \text{ and } p_2|n\} = \sum_{\substack{p_1,p_2\leqslant x\\ p_1\neq p_2\text{ premiers}}} \operatorname{Card}\{n\in\mathbb{N}^* : n\leqslant x, p_1p_2|n\}$$

Or, d'après la question 21.a, on a pour tous $p_1 \neq p_2$ premiers :

$$\operatorname{Card}\{n\in\mathbb{N}^*, n\leqslant x, p_1p_2|n\} - \frac{x}{p_1p_2} \text{ est bornée}$$

Donc

$$\operatorname{Card}\{n\in\mathbb{N}^*, n\leqslant x, p_1p_2|n\} \underset{x\to+\infty}{=} \frac{x}{p_1p_2} + O(1)$$

Ainsi,

$$\sum_{\substack{p_1,p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \text{Card}\{n\in\mathbb{N}^* : n\leqslant x, p_1|n, p_2|n\} \underset{x\to+\infty}{=} \sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \frac{x}{p_1p_2}+O(1)$$

$$\underset{x\to+\infty}{=} \sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \frac{x}{p_1p_2} + \sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} O(1)$$

Or,

$$\sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} 1 \underset{x\to+\infty}{=} \sum_{p\leqslant x} 1$$

$$\underset{x\to+\infty}{=} O(\ln_2(x)) \quad (\text{cf } 20.a)$$

Donc

$$\sum_{\substack{p_1,p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \text{Card}\{n\in\mathbb{N}^* : n\leqslant x, p_1|n, p_2|n\} = \sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \frac{x}{p_1p_2}+O(\ln_2(x))$$

Or, puisque la série $\sum_{p\geqslant 2}\frac{1}{p}$ diverge, on a

$$\sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \frac{x}{p_1p_2} \underset{x\to+\infty}{=} \sum_{\substack{p_1,p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \frac{x}{p_1p_2}$$

$$\underset{x\to+\infty}{=} \sum_{\substack{p_1,p_2\leqslant x\\ p_1p_2 \text{ premiers}}} \frac{x}{p_1p_2} - x\sum_{\substack{p\leqslant x\\ p \text{ premier}}}\frac{1}{p^2}$$

$$\underset{x\to+\infty}{=} x\left(\sum_{\substack{p\leqslant x\\ p \text{ premier}}}\frac{1}{p}\right)^2 - xO(1)$$

$$\underset{x\to+\infty}{=} x\left(\ln_2(E(x))+c_1+O\left(\frac{1}{\ln(E(x))}\right)\right)^2 - O(x)$$

$$\underset{x\to+\infty}{=} x(\ln_2(x))^2 + O(x\ln_2(x))$$

D'où

$$\sum_{\substack{p_1,p_2\leqslant x\\ p_1\neq p_2 \text{ premiers}}} \text{Card}\{n\in\mathbb{N}^*, n\leqslant x, p_1|n \text{ and } p_2|n\} - x(\ln_2(x))^2 \underset{x\to+\infty}{=} O(x\ln_2(x))$$

22.d. D'après ce qui précède, pour tout $x \geqslant 2$, on a :

$$\begin{aligned}
\frac{1}{x}\sum_{n\leq x}\Big(\omega(n)-\ln_2(x)\Big)^2 &\xrightarrow[x\to+\infty]{} \frac{1}{x}\sum_{n\leq x}\omega(n)^2-\big(\ln_2(x)\big)^2+O\big(\ln_2(x)\big)\\
&\xrightarrow[x\to+\infty]{} \frac{1}{x}\sum_{\substack{p_1\neq p_2\\ p_1,p_2\leq x\\ \text{premiers}}}\mathrm{Card}\Big\{n\leq x : p_1\mid n \text{ et } p_2\mid n\Big\}\\
&\quad+\frac{1}{x}\sum_{\substack{p_1\leq x\\ \text{premier}}}\mathrm{Card}\Big\{n\leq x : p_1\mid n\Big\}-\big(\ln_2(x)\big)^2+O\big(\ln_2(x)\big)\\
&\xrightarrow[x\to+\infty]{} \ln_2(x)^2+O\big(\ln_2(x)\big)+\frac{1}{x}\sum_{\substack{p\leq x\\ \text{premier}}}\frac{x}{p}-\big(\ln_2(x)\big)^2+O\big(\ln_2(x)\big)\\
&\xrightarrow[x\to+\infty]{} \ln_2(x)+c_1+O\Big(\frac{1}{\ln x}\Big)+O\big(\ln_2(x)\big)\\
&\xrightarrow[x\to+\infty]{} O\big(\ln_2(x)\big)
\end{aligned}$$

23. On pose

$$\varphi=\left\{n\geqslant 3 : \left|\frac{\omega(n)-\ln_2(n)}{\sqrt{\ln_2(n)}}\right|\geqslant (\ln_2(n))^{1/4}\right\}$$

Montrons que

$$\lim_{x\to+\infty}\frac{1}{x}\,\mathrm{Card}\{n\leqslant x : n\in\varphi\}=0$$

On a pour tout x assez grand,

$$\begin{aligned}
\mathrm{Card}\{\varphi\cap[1,x]\} &= \mathrm{Card}\left\{\varphi\cap\left[\sqrt{x},x\right]\right\}+\mathrm{Card}\left\{\varphi\cap\left[1,\sqrt{x}\right[\right\}\\
&= \mathrm{Card}\left\{\varphi\cap\left[\sqrt{x},x\right]\right\}+O\left(\sqrt{x}\right)
\end{aligned}$$

Pour tout $n\in\varphi\cap[\sqrt{x},x]$

$$\tfrac{(\omega(n)-\ln_2(n))^2}{\ln_2(n)}\geqslant(\ln_2(n))^{1/2} \text{ and } x\geqslant n\geqslant\sqrt{x}$$

On a également :

$$\begin{aligned}
\frac{(\omega(n)-\ln_2(x))^2}{\ln_2(n)} &= \frac{(\omega(n)-\ln_2(n)+\ln_2(n)-\ln_2(x))^2}{\ln_2(n)}\\
&= \frac{(\omega(n)-\ln_2(n))^2}{\ln_2(n)}+\frac{(\ln_2(x)-\ln_2(n))^2}{\ln_2(n)}+2\frac{(\omega(n)-\ln_2(n))(\ln_2(x)-\ln_2(n))}{\ln_2(n)}
\end{aligned}$$

Par suite, on a :

$$\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{\big(\omega(n)-\ln_2(x)\big)^2}{\ln_2(n)}=\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{\big(\omega(n)-\ln_2(n)\big)^2}{\ln_2(n)}+\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{\big(\ln_2(x)-\ln_2(n)\big)^2}{\ln_2(n)}$$
$$+2\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{\big(\omega(n)-\ln_2(n)\big)\big(\ln_2(x)-\ln_2(n)\big)}{\ln_2(n)}$$

Avec

$$\begin{aligned}\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{(\ln_2(x)-\ln_2(n))^2}{\ln_2(n)} &\underset{x\to+\infty}{=} \frac{x-\sqrt{x}}{\ln_2(x)}o(1)\\ &\underset{x\to+\infty}{=} \frac{x}{\ln_2(x)}o(1)\end{aligned}$$

Et

$$\begin{aligned}\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{\big(\omega(n)-\ln_2(n)\big)\big(\ln_2(x)-\ln_2(n)\big)}{\ln_2(n)} &\underset{x\to+\infty}{\leqslant} \frac{o(1)}{\ln_2\Big(\sqrt{x}\Big)}\sum_{n\in\varphi\cap[\sqrt{x},x]}\Big(\omega(n)-\ln_2(n)\Big)\\ &\underset{x\to+\infty}{\leqslant} \frac{o(1)}{\ln_2(x)}\left[\sum_{n\leq x}\Big(\omega(n)-\ln_2(n)\Big)-\sum_{n\leq\sqrt{x}}\Big(\omega(n)-\ln_2(n)\Big)\right.\\ &\underset{x\to+\infty}{\leqslant} \frac{o(1)}{\ln_2(x)}\Big(\ln_2(x)-\ln_2\big(\sqrt{x}\big)+O(1)\Big)\\ &\underset{x\to+\infty}{\leqslant} \frac{o(1)}{\ln_2(x)}\end{aligned}$$

Et

$$\begin{aligned}\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{(\omega(n)-\ln_2(n))^2}{\ln_2(n)} &\leqslant \sum_{n\in[\sqrt{x},x]}\frac{(\omega(n)-\ln_2(n))^2}{\ln_2(n)}\\ &\leqslant \frac{1}{\ln_2\left(\sqrt{x}\right)}\left(\sum_{n\leqslant x}(\omega(n)-\ln_2(n))^2-\sum_{n\leqslant\sqrt{x}}(\omega(n)-\ln_2(n))^2\right)\\ &\underset{x\to+\infty}{\leqslant} xO(1)-\sqrt{x}O(1)\\ &\underset{x\to+\infty}{\leqslant} xO(1)\end{aligned}$$

Ainsi,

$$\begin{aligned}\sum_{n\in\varphi\cap[\sqrt{x},x]}\frac{(\omega(n)-\ln_2(x))^2}{\ln_2(n)} &\underset{x\to+\infty}{\leqslant} \frac{x}{\ln_2(x)}o(1)+\frac{o(1)}{\ln_2(x)}+xO(1)\\ &\underset{x\to+\infty}{\leqslant} xO(1)\end{aligned}$$

Or,

$$\begin{aligned}\sum_{n\in\varphi\cap\left[\sqrt{x},x\right]}\frac{(\omega(n)-\ln_2(x))^2}{\ln_2(n)} &\geqslant \sum_{n\in\varphi\cap\left[\sqrt{x},x\right]}(\ln_2(n))^{1/2}\\ &\geqslant \operatorname{Card}\left(\varphi\cap\left[\sqrt{x},x\right]\right)\left(\ln_2\left(\sqrt{x}\right)\right)^{1/2}\end{aligned}$$

Par suite,

$$\begin{aligned}0 &\leqslant \frac{1}{x}\operatorname{Card}\left(\varphi\cap\left[\sqrt{x},x\right]\right)\\ &\underset{x\to+\infty}{\leqslant} \frac{1}{x\left(\ln_2\left(\sqrt{x}\right)\right)^{1/2}}\sum_{n\in\varphi\cap\left[\sqrt{x},x\right]}\frac{(\omega(n)-\ln_2(x))^2}{\ln_2(n)}\\ &\underset{x\to+\infty}{\leqslant} \frac{O(1)}{\left(\ln_2\left(\sqrt{x}\right)\right)^{1/2}}\end{aligned}$$

Avec $\lim\limits_{x\to+\infty}\frac{O(1)}{\left(\ln_2\left(\sqrt{x}\right)\right)^{1/2}}=0$. Alors

$$\lim_{x\to+\infty}\frac{1}{x}\operatorname{Card}\left(\varphi\cap\left[\sqrt{x},x\right]\right)=0$$

Par suite,

$$\lim_{x\to+\infty}\frac{1}{x}\operatorname{Card}(\varphi\cap[0,x])=0$$

D'où le résultat.

Corrigé de l'épreuve mathématiques A - XLSR - Filière MP-MPI 2023

SABIR ilyass - ETTOUSY BADR

⋆ ⋆ ⋆

1. Préliminaires

1.a. Montrons que $\mathbb{H}$ est un sous-$\mathbb{R}$ algèbre de $M_2(\mathbb{C})$ stable par $Z \longmapsto Z^*$.

On a $E = Z(1,0) \in \mathbb{H}$, et pour tout $z_1, z_2, z_3, z_4 \in \mathbb{C}$ et $\lambda \in \mathbb{R}$, on a :

$$\begin{aligned} Z(z_1,z_2) + \lambda Z(z_3,z_4) &= \begin{pmatrix} z_1+\lambda z_3 & -(\overline{z_2+\lambda z_4}) \\ z_2+\lambda z_4 & \overline{z_1+\lambda z_3} \end{pmatrix} \\ &= Z(z_1+\lambda z_3, z_2+\lambda z_4) \\ &\in \mathbb{H} \end{aligned}$$

De plus,

$$Z(z_1,z_2) \times Z(z_3,z_4) = \begin{pmatrix} z_1z_3 - \bar{z}_2 z_4 & -(\overline{z_2z_3 + \bar{z}_1 z_4}) \\ z_2z_3 + \bar{z}_1 z_4 & \overline{z_1z_3 - \bar{z}_2 z_4} \end{pmatrix} \in \mathbb{H}.$$

Donc, $\mathbb{H}$est un sous $\mathbb{R}$-algèbre de $M_2(\mathbb{C})$.

Ensuite, on a

$$\begin{aligned} Z(z_1,z_2)^* &= \begin{pmatrix} \overline{z_1} & \bar{z}_2 \\ -z_2 & z_1 \end{pmatrix} \\ &= Z(\overline{z_1}, -z_2) \\ &\in \mathbb{H} \end{aligned}$$

D'où $\mathbb{H}$ est stable par $Z \longmapsto Z^*$.

1.b. Soit $Z \in \mathbb{H}$, notons $Z = Z(z_1,z_2)$ où $z_1, z_2 \in \mathbb{C}$.

On a

$$\begin{aligned} Z(z_1,z_2)Z(z_1,z_2)^* &= \begin{pmatrix} z_1 & -\bar{z}_2 \\ z_2 & \overline{z_1} \end{pmatrix}\begin{pmatrix} \overline{z_1} & \bar{z}_2 \\ -z_2 & z_1 \end{pmatrix} \\ &= \begin{pmatrix} |z_1|^2+|z_2|^2 & 0 \\ 0 & |z_1|^2+|z_2|^2 \end{pmatrix} \\ &= (|z_1|^2+|z_2|^2)E \end{aligned}$$

De plus, on a

$$\begin{aligned} Z^*Z &= Z(\overline{z_1},-z_2)Z(\overline{z_1},-z_2)^* \\ &= (|\overline{z_1}|^2+|-z_2|^2)E \\ &= (|z_1|^2+|z_2|^2)E \end{aligned}$$

Si $Z(z_1,z_2)$ est non nul, alors $(z_1,z_2)\neq(0,0)$, en particulier $|z_1|^2+|z_2|^2>0$, d'où Z est inversible.

1.c. Soit $Z(z_1,z_2)\in\mathbb{H}$, avec $z_1,z_2\in\mathbb{C}$.
Si $Z\in\mathbb{R}_{\mathbb{H}}$, alors il existe $a\in\mathbb{R}$ tel que $Z=aE$.
On a, pour tout $Z'\in\mathbb{H}$,

$$\begin{aligned} Z.Z' &= aZ' \\ &= Z'.Z \end{aligned}$$

Réciproquement, si pour tout $Z'\in\mathbb{H}$, on a $Z.Z'=Z'.Z$,
Donc, pour tout $z_3,z_4\in\mathbb{C}$, on a

$$Z(z_1z_3-\bar{z}_2z_4,z_2z_3+\bar{z}_1z_4)=Z(z_3z_1-\bar{z}_4z_2,z_4z_1+\bar{z}_3z_2)$$

Ainsi,

$$\begin{cases} z_1z_3-\bar{z}_2z_4=z_3z_1-\bar{z}_4z_2 \\ z_2z_3+\bar{z}_1z_4=z_4z_1+\bar{z}_3z_2 \end{cases}$$

Par suite, pour tout $z_4\in\mathbb{R}$, on a

$$z_4(\bar{z}_2-z_2)=0$$

et pour tout $z_4\in i\mathbb{R}$, on a

$$z_4(\bar{z}_2+z_2)=0$$

En particulier, $z_2 \in \mathbb{R} \cap i\mathbb{R} = \{0\}$, donc $z_2 = 0$.
Et $z_4(z_1 - \bar{z}_1) = 0$, et ça pour tout $z_4 \in \mathbb{C}$, donc $z_1 \in \mathbb{R}$.
D'où

$$Z = z_1.E \in \mathbb{R}_{\mathbb{H}}$$

D'où l'équivalence.

2.a. Pour tout $Z = (z_1, z_2) \in \mathbb{H}$ et $Z' = (z_3, z_4) \in \mathbb{H}$. On a :

$$\begin{aligned} N(ZZ') &= N(Z(z_1z_3 - \bar{z}_2z_4, z_2z_3 + \bar{z}_1z_4)) \\ &= |z_1z_3 - \bar{z}_2z_4|^2 + |z_2z_3 + \bar{z}_1z_4|^2 \\ &= |z_1z_3|^2 - 2z_1z_3\overline{\bar{z}_2z_4} + |\bar{z}_2z_4|^2 + |z_2z_3|^2 + 2z_2z_3\overline{\bar{z}_1z_4} + |\bar{z}_1z_4|^2 \\ &= |z_1|^2|z_3|^2 + |z_2|^2|z_4|^2 + |z_2|^2|z_3|^2 + |z_1|^2|z_4|^2 \\ &= (|z_1|^2 + |z_2|^2)(|z_3|^2 + |z_4|^2) \\ &= N(Z)N(Z') \end{aligned}$$

2.b. Montrons que S est un sous groupe de $\mathbb{H}^\times$.
On a $N(E) = 1$, donc $E \in S$.
Soient $Z, Z' \in S$. On a $Z, Z' \in \mathbb{H}$ tels que

$$\begin{aligned} N(Z) &= N(Z') \\ &= 1 \end{aligned}$$

D'après la question 1.b, on a Z et Z' sont inversibles.
Or, d'après la question précédente, on a :

$$\begin{aligned} N\left(Z'^{-1}\right) &= N(Z').N\left(Z'^{-1}\right) \\ &= N\left(Z'Z'^{-1}\right) \\ &= N(E) \\ &= 1 \end{aligned}$$

Donc,

$$\begin{aligned} N\left(Z.Z'^{-1}\right) &= N(Z)N\left(Z'^{-1}\right) \\ &= 1 \end{aligned}$$

Ainsi, $Z.Z'^{-1} \in S$. Donc S est un sous-groupe de $\mathbb{H}^\times$.

De plus, pour tout $Z = (z_1, z_2) \in \mathbb{H}^\times$, on a $N(Z) > 0$, et

$$\begin{aligned} N\left(\frac{1}{\sqrt{N(Z)}}Z\right) &= \left|\frac{z_1}{\sqrt{N(Z)}}\right|^2 + \left|\frac{z_2}{\sqrt{N(Z)}}\right|^2 \\ &= \frac{1}{N(Z)}N(Z) \\ &= 1 \end{aligned}$$

Donc $\frac{1}{\sqrt{N(Z)}}Z \in S$.

3.a. Soient $x, y, z, t \in \mathbb{R}$, on a :

$$\begin{aligned} N(xE + yI + zJ + tK) &= N\left(\begin{pmatrix} x+iy & z-it \\ -z+it & x-iy \end{pmatrix}\right) \\ &= |x+iy|^2 + |-z+it|^2 \\ &= x^2 + y^2 + z^2 + t^2 \end{aligned}$$

3.b. Soit $U \in \mathbb{H}^{\text{im}}$, on a alors l'existence de $x, y, z \in \mathbb{R}$ tels que $U = xI + yJ + zK$. On a alors :

$$\begin{aligned} U^2 &= -(x^2 + y^2 + z^2)E \\ &= -N(U)E \end{aligned}$$

On a donc

$$\mathbb{H}^{\text{im}} \subset \{U \in \mathbb{H} | U^2 \in]-\infty, 0]E\}$$

Soit $U \in \mathbb{H}$ tel que $U^2 \in]-\infty, 0]E$. Montrons que $U \in \mathbb{H}^{\text{im}}$.

On a l'existence de $x, y, z, t \in \mathbb{R}$ tels que

$$U = xE + yI + zJ + tK$$

On a :

$$U^2 = (x^2 - y^2 - z^2 - t^2)E + 2xyI + 2xzJ + 2xtK$$

On a $U^2 \in]-\infty, 0]E$, donc $xy = xz = xt = 0$ et $x^2 \leqslant y^2 + z^2 + t^2$.

Si $x \neq 0$, alors $y = z = t = 0$. Par suite $x^2 \leqslant 0$, donc $x = 0$, ce qui est absurde.

D'où $x = 0$. Par suite

$$U = yI + zJ + tK \in \mathbb{H}^{\text{im}}$$

4. On a $Z \in \mathbb{H} \to \sqrt{N(Z)}$ est une norme sur $\mathbb{H}$ associée au produit scalaire $\langle ., . \rangle$.

On a S est la sphére unité centrée en 0 de l'espace vectoriel normé $\left(\mathbb{H}, \sqrt{N}\right)$.

Ainsi, S est un fermé de $\mathbb{H}$, et on a

$$\psi(\{(x, y, z, t) \in \mathbb{R}^4 | x^2 + y^2 + z^2 + t^2 = 1\}) = S$$

Or, $\{(x, y, z, t) \in \mathbb{R}^4 | x^2 + y^2 + z^2 + t^2 = 1\}$ est la sphére unité centrée en 0 de $\mathbb{R}^4$, qui est donc connexe par arcs.

De plus, ψ est 1-lipschitzienne, donc en particulier qu'elle est continue.

Ainsi, S est connexe par arc, comme étant l'image directe par une application continue d'une partie connexe par arcs.

5. Soient $U, V \in H^{\text{im}}$.

5.a. Montrons que U et V sont orthogonaux si et seulement si $UV+VU = 0$.

Supposons que U et V sont orthogonaux. On a

$$\begin{aligned} UV + VU &= (U + V)^2 - U^2 - V^2 \\ &= -(N(U + V) - N(U) - N(V))E \end{aligned}$$

Donc, U et V sont orthogonaux si et seulement si

$$N(U + V) = N(U) + N(V)$$

ce qui est équivalent à $UV + VU = 0$.

Dans ce cas, on a

$$\begin{aligned} (UV)^2 &= -UV^2U \\ &= N(V)U^2 \\ &= -N(U)N(V)E \end{aligned}$$

avec

$$-N(U)N(V) \leqslant 0$$

Donc $UV \in H^{\text{im}}$.

Notons

$$U = x_1 I + y_1 J + z_1 K$$

et

$$V = x_2 I + y_2 J + z_2 K$$

avec $x_1, x_2, y_1, y_2, z_1, z_2 \in \mathbb{R}$.

On obtient alors

$$UV \quad = \quad (y_1 z_2 - z_1 y_2)I + (z_1 x_2 - x_1 z_2)J + (x_1 y_2 - y_1 x_2)K$$

(car U et V sont orthogonaux).

Ainsi, la matrice de (U, V, UV) dans la base (I, J, K) est

$$\begin{pmatrix} x_1 & x_2 & y_1 z_2 - z_1 y_2 \\ y_1 & y_2 & z_1 x_2 - x_1 z_2 \\ z_1 & z_2 & x_1 y_2 - y_1 x_2 \end{pmatrix}$$

Avec

$$\begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix} \wedge \begin{pmatrix} x_2 \\ y_2 \\ z_2 \end{pmatrix} = \begin{pmatrix} y_1 z_2 - z_1 y_2 \\ y_1 z_2 - z_1 y_2 \\ x_1 y_2 - y_1 x_2 \end{pmatrix}$$

Donc, le déterminant de $\begin{pmatrix} x_1 & x_2 & y_1 z_2 - z_1 y_2 \\ y_1 & y_2 & z_1 x_2 - x_1 z_2 \\ z_1 & z_2 & x_1 y_2 - y_1 x_2 \end{pmatrix}$ est positif ou nul.

5.b. Supposons que (U, V) est une famille orthonormée dans $\mathbb{H}^{\text{im}}$.

Montrons que (U, V, UV) est une base orthonormée directe de $\mathbb{H}^{\text{im}}$.

Et on a

$$N(U + V) = N(U) + N(V) \text{ and } N(U) = N(V) = 1$$

De plus,

$$\begin{aligned}\langle U, UV\rangle &= \frac{1}{2}(N(U(U+V)) - N(UV) - N(U)) \\ &= \frac{1}{2}[N(U)(N(U+V) - N(V)) - N(U)] \\ &= \frac{1}{2}[N(U)(N(U)) - N(U)] \\ &= \frac{1}{2}[1-1] \\ &= 0\end{aligned}$$

Par symétrie, $\langle V, UV\rangle = 0$, et

$$N(UV) = N(U)N(V) = 1$$

Ainsi, (U, V, UV) est une famille orthonormée. D'après la question précédente, cette famille a un déterminant positif ou nul ; comme elle est orthogonale, elle est donc libre. En particulier, son déterminant non nul et donc strictement positif.

En conclusion, (U, V, UV) est une base orthonormée directe de $\mathbb{H}^{\text{im}}$.

2. Automorphismes de $\mathbb{H}$ and rotations.

6. Montrons que α est un morphisme de groupes.

Soient $(u, v), (u', v') \in S \times S$, on a pour tout $Z \in \mathbb{H}$:

$$\begin{aligned}\alpha((u,v)\times(u',v'))(Z) &= \alpha(uu', vv')(Z) \\ &= uu'Z(vv')^{-1} \\ &= u\left(u'Zv'^{-1}\right)v^{-1} \\ &= u(\alpha(u',v')(Z))v^{-1} \\ &= \alpha(u,v)\circ\alpha(u',v')(Z)\end{aligned}$$

Donc,

$$\alpha((u,v)\times(u',v')) = \alpha(u,v)\circ\alpha(u',v')$$

Ainsi, α est un morphisme de groupes.

Soit $(u, v) \in \ker \alpha$, alors pour tout $Z \in \mathbb{H}$, on a $\alpha(u, v)(Z) = Z$, donc

$$uZv^{-1} = Z$$

Ainsi,

$$uZ = Zv$$

En particulier,

$$\begin{aligned} E &= u.u^* \\ &= u^*v \end{aligned}$$

Avec $u^* = u^{-1}$ (cf. la question 1.b), donc $u = v$.

Ainsi, pour tout $Z \in \mathbb{H}$, on a

$$uZ = Zu$$

d'où $Z \in \mathbb{R}_{\mathbb{H}}$(d'après la question 1.c).

Et $N(u) = 1$, donc $u = \pm 1$.

Réciproquement, si $u = v = \pm 1$, on a pour tout $Z \in \mathbb{H}$:

$$uZv^{-1} = Z$$

D'où

$$(u, v) \in \ker \alpha$$

On en déduit que

$$\ker \alpha = \{(-1, -1), (1, 1)\}$$

7. Montrons que α est continue.

L'application $(u, v) \in \mathbb{H}^2 \longmapsto (Z \longmapsto uZv)$ est bilinéaire en dimension finie, donc elle est continue sur $\mathbb{H}^2$, en particulier, elle est continue sur $S \times S$.

De plus, $v \longmapsto v^{-1}$ est continue sur S (car pour tout $v \in S$, l'application $v \to v^{-1}$ est polynômiale en v d'après le thèorème de Cayley-Hamilton).

Ainsi, α est continue comme étant le composé de deux fonctions continues.

Pour tout $(u,v) \in S \times S$, on a :

$$\begin{aligned} N(\alpha(u,v)(Z)) &= N(uZv^{-1}) \\ &= N(u)N(Z)N(v^{-1}) \\ &= N(Z) \end{aligned}$$

En particulier, $\sqrt{N(\alpha(u,v)(Z))} = \sqrt{N(Z)}$ et $\sqrt{N}$ est une norme euclidienne (cf. partie I).

Alors, $\alpha(u,v) \in O(H)$.

Pour tout $(u,v) \in S \times S$, on a

$$\det(\alpha(u,v)) \neq 0$$

Puisque det est continue sur $\mathrm{GL}(\mathbb{H})$ et α est continue, alors $\det \circ \alpha$ est continue.

D'autre part, $S \times S$ est connexe par arcs en tant que produit de deux parties connexes par arcs, donc $\det \circ \alpha$ gadre un signe constant sur $S \times S$, avec

$$\det(\alpha(E,E)) = 1 > 0$$

Ainsi, pour tout $(u,v) \in S \times S$, on a $\det(\alpha(u,v)) > 0$.

En conclusion, l'image de α est contenue dans $\mathrm{SO}(\mathbb{H})$.

8. Soient $\theta \in \mathbb{R}$ et $v \in \mathbb{H}^{\mathrm{im}} \cap S$, et soit $u = (\cos\theta)E + (\sin\theta)v$.

8.a. Montrons que $u \in S$.

On a $v \in \mathbb{H}^{\mathrm{im}} = \mathrm{vect}_{\mathbb{R}}(I,J,K)$. Notons $v = xI + yJ + zK$avec $x,y,z \in \mathbb{R}$.

Donc

$$u = (\cos\theta)E + (\sin\theta)xI + (\sin\theta)yJ + (\sin\theta)zK$$

Donc

$$\begin{aligned} N(u) &= (\cos\theta)^2 + (\sin\theta)^2x^2 + (\sin\theta)^2y^2 + (\sin\theta)^2z^2 \\ &= 1 \end{aligned}$$

car $x^2 + y^2 + z^2 = 1$.

Donc, $u \in S$.

Or, $N(u) > 0$ et $N(v) > 0$, donc d'après la question 1.b de la partie I, u et v sont inversibles et on a

$$u^{-1} = N(u)u^* = u^* \text{ and } v^* = N(v)v^{-1} = v^{-1}$$

Or, $u^* = ((\cos\theta)E + (\sin\theta)v)^*$, avec $Z \to Z^*$ est $\mathbb{R}-$linéaire.
Donc

$$u^* = (\cos\theta)E + (\sin\theta)v^*$$

Puisque $v \in \mathbb{H}^{\text{im}}$, et d'après la question 3.b

$$\begin{aligned} v^2 &= -N(v)E \\ &= -E \end{aligned}$$

donc

$$\begin{aligned} v^* &= -v^2v^* \\ &= -v \end{aligned}$$

Ainsi,

$$\begin{aligned} u^{-1} &= u^* \\ &= (\cos\theta)E - (\sin\theta)v \end{aligned}$$

8.b. Soit $\omega \in \mathbb{H}^{\text{im}} \cap S$ un vecteur orthogonal à v.
On a :

$$\begin{aligned} C_u(v) &= uvu^{-1} \\ &= ((\cos\theta)E + (\sin\theta)v)v((\cos\theta)E - (\sin\theta)v) \end{aligned}$$

Or, $(\cos\theta)E + (\sin\theta)v$, v et $(\cos\theta)E - (\sin\theta)v$ commutent, donc :

$$\begin{aligned} C_u(v) &= (\cos\theta)^2v - (\sin\theta)^2v^3 \\ &= v \end{aligned}$$

Car $v^2 = -E$

Et :

$$\begin{aligned} C_u(w) &= uwu^{-1} \\ &= ((\cos\theta)E + (\sin\theta)v)w((\cos\theta)E - (\sin\theta)v) \\ &= (\cos\theta)^2 w\cos(\theta)\sin(\theta)wv + \sin(\theta)\cos(\theta)vw(\sin\theta)^2 v \\ &= ((\cos\theta)^2(\sin\theta)^2)w + \cos\theta\sin\theta(vwwv) \\ &= \cos(2\theta)w + \sin(2\theta)vw \end{aligned}$$

Car $v, w \in \mathbb{H}^{\text{im}}$, via la question 5.b on a

$$wv + vw = 0$$

Pour $C_u(vw)$:

$$\begin{aligned} C_u(vw) &= uvwu^{-1} \\ &= ((\cos\theta)E + (\sin\theta)v)vw((\cos\theta)E - (\sin\theta)v) \\ &= ((\cos\theta)vw + (\sin\theta)v^2 w)((\cos\theta)E - (\sin\theta)v) \\ &= ((\cos\theta)vw - (\sin\theta)w)((\cos\theta)E - (\sin\theta)v) \\ &= (\cos\theta)^2 vw - \cos\theta\sin\theta(vwv + w) + (\sin\theta)^2 wv \\ &= (\cos\theta)^2 vw - \cos\theta\sin\theta(-v^2 w + w) + (\sin\theta)^2 wv \\ &= (\cos\theta)^2 vw - 2\cos\theta\sin\theta w + (\sin\theta)^2 wv \\ &= ((\cos\theta)^2 - (\sin\theta)^2)vw - 2\cos\theta\sin\theta w \\ &= \cos(2\theta)vw - \sin(2\theta)w \end{aligned}$$

Donc :

$$\text{mat}_{(v,w,vw)} C_u = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\theta) & -\sin(2\theta) \\ 0 & \sin(2\theta) & \cos(2\theta) \end{pmatrix}$$

9. Montrons que l'application $\varphi : u \longmapsto C_u$ induit un morphisme surjectif de groupes $S \to SO(\mathbb{H}^{\text{im}})$.

Pour tous $u, v \in S$ et $Z \in \mathbb{H}^{\text{im}}$, on a :

$$\begin{aligned} \varphi(uv)(Z) &= uvZ(uv)^{-1} \\ &= u(vZv^{-1})u^{-1} \\ &= u(C_v(Z))u^{-1} \\ &= C_u \circ C_v(Z) \\ &= \varphi(u) \circ \varphi(v)(Z) \end{aligned}$$

Donc

$$\varphi(uv) = \varphi(u) \circ \varphi(v)$$

Ainsi, $u \longmapsto C_u$ est un morphisme de groupes.

La surjectivité de φ est déduite de la question précédente et de la définition de $\mathrm{SO}(\mathbb{H}^{\mathrm{im}})$.

Pour tout $x \in \operatorname{Ker}\varphi$, pour tout $Z \in \mathbb{H}^{\mathrm{im}}$, on a $uZu^{-1} = Z$.

Puisque $\mathbb{H} = \mathrm{vect}(E) + \mathbb{H}^{\mathrm{im}}$, avec E la matrice identité, alors pour tout $Z \in \mathbb{H}$, on a u commute avec Z. Par conséquent, $u \in \mathbb{R}_{\mathbb{H}}$ (via la question 1.c).

Or„ $N(u) = 1$, donc $u = \pm 1$.

Réciproquement, $u = \pm 1$ vérifie $uZu^{-1} = Z$pour tout $Z \in \mathbb{H}$.

Ainsi

$$\ker\varphi = \{-1, 1\}$$

10.a. Pour tout $u \in \mathrm{SO}(\mathbb{H})$, on a :

$$\begin{aligned} \alpha(\overline{u(E)}, E)(u(E)) &= \overline{u(E)}u(E)E \\ &= E \end{aligned}$$

Donc $\mathbb{H}^{\mathrm{im}}$ est stable par $\alpha(\overline{u(E)}, E)$. L'orthogonalité assure l'existence d'un $v \in \mathbb{H}$ tel que

$$\alpha(\overline{u(E)}, E) \circ u = \alpha(v, v)$$

Ainsi,

$$\begin{aligned} u &= \alpha(\overline{u(E)}, E)^{-1} \circ \alpha(v, v) \\ &= \alpha(u(E)v, v) \end{aligned}$$

D'où le résultat.

10.b. $S \times \{E\}$ est un groupe en tant que produit de deux groupes, et α est un morphisme. Alors $N := \alpha(S \times \{E\}) \subset \mathrm{SO}(\mathbb{H})$ est un sous-groupe de $\mathrm{SO}(\mathbb{H})$ en tant qu'image directe d'un sous-groupe par un morphisme de groupes.

Soit $n \in N$ et $g \in \mathrm{SO}(\mathbb{H})$. Il existe donc $x \in S$ tel que $n = \alpha(x, E)$ et $(u, v) \in \mathbb{H}^2$ tel que $g = \alpha(u, v)$.

On a, pour tout $Z \in \mathbb{H}$

$$\begin{aligned} gng^{-1}(Z) &= gxZg^{-1} \\ &= \alpha(uxu^{-1}, E)(Z) \end{aligned}$$

Donc,

$$gng^{-1} = \alpha(uxu^{-1}, E) \in N$$

Pour $n = \pm id = \alpha(\pm 1, 1)$ et $g = \mathrm{id} = \alpha(1, 1)$, on a

$$\{\pm \mathrm{id}\} \subset N \subset \mathrm{SO}(\mathbb{H})$$

Or, d'après la question précédente, $\mathbb{H}^{\mathrm{im}}$ est stable par tous les éléments de N, d'où on en déduit que

$$N \not= \mathrm{SO}(\mathbb{H})$$

Il suffit de prendre $\alpha(I, 1) \in N$, avec $\alpha(I, 1) \neq \pm \mathrm{id}$, d'où le résultat.

11. Puisque $\mathrm{id}_{\mathbb{H}} \in \mathrm{Aut}(\mathbb{H})$, alors pour tous $\varphi, \psi \in \mathrm{Aut}(H)$, et pour tous $z, z' \in \mathbb{H}$,

$$\varphi \circ \psi^{-1}_{|\mathbb{R}_{\mathbb{H}}} = \mathbb{R}_{\mathbb{H}}$$

On a

$$\begin{aligned} \varphi(\varphi^{-1}(zz^{'})) &= zz' \\ &= \varphi(\varphi^{-1}(z))\varphi(\varphi^{-1}(z')) \\ &= \varphi(\varphi^{-1}(z)\varphi^{-1}(z')) \end{aligned}$$

Donc,

$$\varphi^{-1}(zz^{'}) = \varphi^{-1}(z)\varphi^{-1}(z')$$

Et pour tous $z, z' \in \mathbb{H}$, on a

$$\begin{aligned} \varphi \circ \psi(zz') &= \varphi(\psi(z)\psi(z')) \\ &= \varphi(\psi(z))\varphi(\psi(z')) \\ &= \varphi \circ \psi(z)\varphi \circ \psi(z') \end{aligned}$$

Ainsi, Aut($\mathbb{H}$) est un sous-groupe de GL($\mathbb{H}$).

Soit $u \in S$, on a alors pour tout $Z \in \mathbb{R}_{\mathbb{H}}$,

$$\begin{aligned} \alpha(u,u)(Z) &= uZu^{-1} \\ &= Z \end{aligned}$$

Donc $\alpha_{|\mathbb{R}_{\mathbb{H}}} = \mathrm{id}_{\mathbb{H}}$.

Et pour tout $Z, Z' \in \mathbb{H}$, on a

$$\begin{aligned} \alpha(u,u)(Z.Z') &= (uZu^{-1})(uZ'u^{-1}) \\ &= \alpha(u,u)(Z)\alpha(u,u)(Z') \end{aligned}$$

Ainsi, $\alpha(u,u) \in \mathrm{Aut}(\mathbb{H})$.

D'où le résultat.

12. Soit $f \in \mathrm{Aut}(\mathbb{H})$.

On a

$$\begin{aligned} f(I)^2 &= f(I^2) \\ &= f(-E) \\ &= -E \end{aligned}$$

De même, on trouve $f(J^2) = -E$, donc d'après la question 3.b, on a $f(I), f(J) \in \mathbb{H}^{\mathrm{im}}$.

Et

$$\begin{aligned} f(I)f(J) + f(J)f(I) &= f(IJ + JI) \\ &= f(0) \\ &= 0 \end{aligned}$$

D'après la question 5.a, on a $f(I)$ et $f(J)$ sont orthogonaux. Par conséquent, via la question 5.b, on a alors $(f(I), f(J), f(K) = f(I)f(J))$ est une base orthonormée directe de $\mathbb{H}^{\mathrm{im}}$.

13.a. Montrons que la restriction à $\mathbb{H}^{\mathrm{im}}$ induit un isomorphisme de groupes.

D'après les questions 8 et 11, l'application $u \in \mathrm{Aut}(\mathbb{H}) \to u_{|\mathbb{H}^{\mathrm{im}}} \in \mathrm{SO}(\mathbb{H}^{\mathrm{im}})$ est surjective.

Si $u_{|\mathbb{H}^{\mathrm{im}}} = \mathrm{id}_{\mathbb{H}^{\mathrm{im}}}$, alors pour tout $Z \in \mathbb{H}$, on a $u(Z) = Z$ (car $u_{|\mathbb{R}_{\mathbb{H}}} = \mathrm{id}_{\mathbb{R}_{\mathbb{H}}}$).

Par suite, $u_{|\mathbb{H}} = \mathrm{id}_{\mathbb{H}}$.

Ainsi, l'application $u \in \mathrm{Aut}(\mathbb{H}) \to u_{|\mathbb{H}^{\mathrm{im}}} \in \mathrm{SO}(\mathbb{H}^{\mathrm{im}})$ est injective.

D'où le résultat.

13.b. Montrons que

$$\mathrm{Aut}(\mathbb{H}) = \{\alpha(u,u), u \in S\}$$

D'après la question 11,

$$\{\alpha(u,u), u \in S\} \subset \mathrm{Aut}(\mathbb{H})$$

Et pour tout $u \in \mathrm{Aut}(\mathbb{H})$, il existe $v \in S$ tel que $u_{|\mathbb{H}^{\mathrm{im}}} = \alpha(v,v)_{|\mathbb{H}^{\mathrm{im}}}$ (d'après la question 9).

Or,

$$\mathbb{H} = \mathbb{H}^{\mathrm{im}} \oplus \mathbb{R}_{\mathbb{H}}$$

Donc $u = \alpha(v,v)$.

D'où

$$\mathrm{Aut}(\mathbb{H}) \subset \{\alpha(u,u), u \in S\}$$

D'où le résultat.

3. Normes euclidiennes sur $\mathbb{R}^2$.

14.a. Montrons que $\mathcal{K}$ est une partie compacte et convexe de $M_2(\mathbb{R})$.

En dimension finie, toutes les normes sont équivalentes ; en particulier, il existe $\alpha > 0$ tel que, pour tout $x \in \mathbb{R}^2$ on a $\|x\|_2 \leqslant \alpha\|x\|$. Donc, pour tout $A \in \mathcal{K}$, on a

$$\sup_{x \neq 0} \frac{\|Ax\|}{\|x\|} \leqslant \alpha$$

Ainsi, $\mathcal{K}$ est bornée (pour la norme subordonnée de $\|.\|$). En dimension finie, elle est bornée pour n'importe quelle norme.

Soit $(A_n)_{n\in\mathbb{N}}$une suite de matrices de $\mathcal{K}$qui converge vers $A \in M_2(\mathbb{R})$. On a, pour tout $n \in \mathbb{N}$, et pour tout $x \in \mathbb{R}^2$,

$$\|x\|_2 \geqslant \|A_n x\|$$

De plus, pour tout $B \in M_2(\mathbb{R})$, la fonction $x \in \mathbb{R}^2 \longmapsto \|Bx\|$ est lipschitzienne. En effet, pour tous $x_1, x_2 \in \mathbb{R}^2$, on a

$$\begin{aligned} |\|Bx_1\| - \|Bx_2\|| &\leqslant \|B(x_1 - x_2)\| \\ &\leqslant \alpha\|x_1 - x_2\| \end{aligned}$$

Avec $\alpha > 0$ défini dans la question précédente. En particulier, la fonction $x \in \mathbb{R}^2 \longmapsto \|Bx\|$ est continue. Par conséquent, $\lim\limits_{n\to+\infty} \|A_n x\| = \|Ax\|$, donc $\|x\|_2 \geqslant \|Ax\|$.

Ainsi, $A \in \mathcal{K}$, et $\mathcal{K}$ est donc fermée. Par conséquent, $\mathcal{K}$ est compacte.

Montrons maintenant que $\mathcal{K}$ est convexe dans $M_2(\mathbb{R})$.

Soient $A, B \in \mathcal{K}$ et $\lambda \in [0, 1]$. On a

$$\begin{aligned} \|\lambda Ax + (1-\lambda)Bx\| &\leqslant \lambda\|Ax\| + (1-\lambda)\|Bx\| \\ &\leqslant \|x\|_2 \end{aligned}$$

Ainsi, $\lambda Ax + (1-\lambda)Bx \in \mathcal{K}$, et donc $\mathcal{K}$ est convexe.

14.b. Montrons qu'il existe $A \in \mathcal{K}$ tel que

$$\det A = \sup_{B\in\mathcal{K}} \det B$$

On a $B \in \mathcal{K} \to \det B$ est continue sur le compact $\mathcal{K}$. Ainsi, det est bornée sur $\mathcal{K}$ et atteint ses bornes. En particulier, il existe $A \in \mathcal{K}$ tel que $\det A = \sup\limits_{B\in\mathcal{K}} \det B$.

15. En dimension finie, toutes les normes sont équivalentes. En particulier, il existe une constante $\beta > 0$ telle que pour tout $x \in \mathbb{R}^2$, on a $\|x\|_2 \geqslant \beta\|x\|$.

Donc, $\|x\|_2 \geqslant \|\beta E.x\|$, ce qui implique que $\beta E \in \mathcal{K}$.

Ainsi,

$$\begin{aligned}\det A &\geqslant \det(\beta E)\\ &= \beta^2\\ &> 0\end{aligned}$$

Montrons qu'il existe un élément $x \in \mathcal{C}$ tel que $\|Ax\| = 1$. Supposons par l'absurde que pour tout $x \in \mathcal{C}$, on ait $\|Ax\| < 1$.

L'application $x \longmapsto \|Ax\|$ est continue, car elle est le composé de deux fonctions continues $x \longmapsto xA$, qui est linéaire en dimension finie, et $x \longmapsto \|x\|$, qui est 1-lipschitizienne (d'après l'inégalité triangulaire).

Sur le compact $\mathcal{K}$, $\|Ax\|$ est bornée et atteint ses bornes,

$$\sup_{x\in\mathcal{C}}\|Ax\| < 1$$

Posons $C = \frac{A}{\sup\limits_{x\in\mathcal{C}}\|Ax\|}$, alors pour tout $y \in \mathbb{R}$.

$$\begin{aligned}\|Cy\| &= \frac{1}{\sup\limits_{x\in\mathcal{C}}\|Ax\|}\|Ay\|\\ &= \frac{\|y\|_2}{\sup\limits_{x\in\mathcal{C}}\|Ax\|}\left\|A\frac{y}{\|y\|_2}\right\|\end{aligned}$$

Avec $\frac{y}{\|y\|_2} \in \mathcal{C}$, on a donc $\|Cy\| \leqslant \|y\|_2$, ainsi $C \in \mathcal{K}$.

Par suite, $\det(C) \leqslant \det(A)$, donc

$$\frac{1}{\left(\sup\limits_{x\in\mathcal{C}}\|Ax\|\right)^2}\det(A) \leqslant \det(A)$$

avec $\det(A) > 0$. Alors, $\sup\limits_{x\in\mathcal{C}}\|Ax\| \geqslant 1$.

ce qui est absurde.

D'où le résultat.

16. Soit $B \in \mathrm{SO}(\mathbb{R}^2)$ une matrice telle que $x = B\begin{pmatrix}1\\0\end{pmatrix}$.

16.a. Soit $r \in]0,1[$. Pour montrer qu'il existe $x_r \in \mathcal{C}$ tel que

$$\left\|AB\begin{pmatrix}r & 0\\ 0 & \frac{1}{r}\end{pmatrix}x_r\right\| > 1$$

il suffit de montrer que

$$AB\begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} \notin \mathcal{K}$$

Par l'absurde, supposons que $AB\begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} \in \mathcal{K}$.

On a $A \in \mathcal{K}$, et pour tout $x \in \mathbb{R}^2$,

$$\begin{aligned} \|Bx\|_2 &= \|x\|_2 \\ &\leqslant \|ABx\| \end{aligned}$$

Ainsi, $AB \in \mathcal{K}$. Donc, par convexité de $\mathcal{K}$, on a $\frac{1}{2}\left[AB + AB\begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix}\right] \in \mathcal{K}$.

Or,

$$\begin{aligned} \det\left(\frac{1}{2}\left[AB + AB\begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix}\right]\right) &= \frac{1}{4}\det(A)\det(B)\det\begin{pmatrix} r+1 & 0 \\ 0 & \frac{1}{r}+1 \end{pmatrix} \\ &\leqslant \det(A) \end{aligned}$$

Puisque $\det A = \sup_{B \in \mathcal{K}} \det B$.

Or, $\det(B) = 1$, alors $(r+1)\left(\frac{1}{r}+1\right) \leqslant 4$, ce qui implique $\frac{1}{r} + r \leqslant 2$, donc $\left(\frac{1}{r} - r\right)^2 \leqslant 0$.

Ainsi, $r = \frac{1}{r}$, ce qui est absurde avec $0 < r < 1$.

D'où le résultat.

16.b. Soit $r \in]0,1[$, on a d'après la question précédente :

$$\begin{aligned} \left\| AB\begin{pmatrix} ry_r \\ \frac{z_r}{r} \end{pmatrix} \right\| &= \left\| AB\begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} x_r \right\| \\ &> 1 \end{aligned}$$

Donc

$$\left\| \begin{pmatrix} ry_r \\ \frac{z_r}{r} \end{pmatrix} \right\|_2 \geqslant \left\| AB\begin{pmatrix} ry_r \\ \frac{z_r}{r} \end{pmatrix} \right\|$$

Car $\dfrac{\begin{pmatrix} ry_r \\ \frac{z_r}{r} \end{pmatrix}}{\left\| \begin{pmatrix} ry_r \\ \frac{z_r}{r} \end{pmatrix} \right\|_2} \in \mathcal{C}$ et $AB \in \mathcal{K}$.

Donc

$$\left\| \begin{pmatrix} ry_r \\ \frac{z_r}{r} \end{pmatrix} \right\|_2 > 1$$

Par suite

$$r^2 y_r^2 + \frac{z_r^2}{r^2} > 1 \text{ and } y_r^2 + z_r^2 = 1$$

Par conséquent,

$$z_r^2 \left(\frac{1}{r^2} - r^2 \right) > 1 - r^2$$

Ainsi,

$$\begin{aligned} z_r^2 &> \frac{1 - r^2}{\frac{1}{r^2} - r^2} \\ &= \frac{r^2}{r^2 + 1} \end{aligned}$$

D'où le résultat.

17. Montrons qu'il existe une base (e_1, e_2)de $\mathbb{R}^2$telle que $\|Ax\| = \|x\|_2$ pour $x \in \{e_1, e_2\}$.

D'après la question 15, il existe $e_1 \in \mathcal{C}$ tel que $\|Ae_1\| = 1$ avec $\|e_1\|_2 = 1$.

Pour tout $n \in \mathbb{N}$ tel que $n \geqslant 2$, puisque $\frac{n-1}{n} \in]0, 1[$, alors il d'après la question 16.a, il existe $t_n \in \mathcal{C}$ tel que

$$\left\| AB \begin{pmatrix} \frac{n-1}{n} & 0 \\ 0 & \frac{n}{n-1} \end{pmatrix} t_n \right\| > 1$$

Comme $\mathcal{C}$ est compact, alors la suite $\left(t_n := \begin{pmatrix} c_n \\ d_n \end{pmatrix} \right)_{n \geqslant 2}$ admet une sous-suite convergente.

Il existe donc une application strictement croissante $\varphi : \mathbb{N} \to \mathbb{N}$ telle que $(t_{\varphi(n)})_{n \in \mathbb{N}}$ converge vers une limite que nous notons $t \in \mathcal{C}$.

Puisque φ diverge vers $+\infty$, car l'ouvert de $\mathbb{N}$ est vide.

Or, $x \to \|x\|$ est continue (1-lipschitzienne d'après l'inégalité triangulaire), alors

$$\lim_{n\to+\infty} \begin{pmatrix} \frac{\varphi(n)-1}{\varphi(n)} & 0 \\ 0 & \frac{\varphi(n)}{\varphi(n)-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Donc

$$\lim_{n\to+\infty} \begin{pmatrix} \frac{n-1}{n} & 0 \\ 0 & \frac{n}{n-1} \end{pmatrix} x_{\varphi(n)} = t$$

En passant à la limite, on obtient

$$\|ABt\| \geqslant 1$$

Comme $t \in \mathcal{C}$ et $AB \in \mathcal{K}$, on a $\|ABt\| \leqslant 1$. Donc, $\|ABt\| = 1$.

Notons $e_2 = Bt \in \mathcal{C}$.

On a bien $\|e_2\| = 1 = \|e_2\|_2$.

Il reste à montrer que (e_1, e_2) est une famille libre pour conclure.

Soient $\alpha, \beta \in \mathbb{R}$ tels que

$$\alpha e_1 + \beta e_2 = 0$$

Donc,

$$B\left(\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}\right) = 0$$

avec $e_2 := \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$.

Puisque B est inversible, cela implique :

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} = 0$$

On a alors $\beta w_2 = 0$.

Or, d'après la question précédente, pour tout $n \in \mathbb{N}$,

$$d_{\varphi(n)} > \frac{\varphi(n)^2}{\varphi(n)^2 + 1}$$

En passant à la limite, on obtient

$$w_2 \geqslant \frac{1}{2}$$

Donc $\beta = 0$, ce qui entraîne $\alpha = 0$.

D'où le résultat.

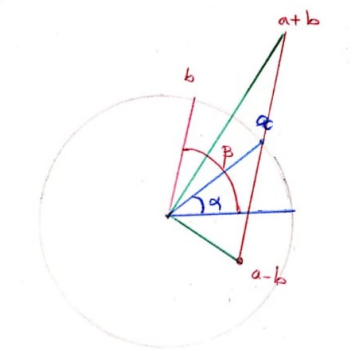
18. Notons α et β respectivement l'angle entre x et l'axe des abscisses, (respectivement entre y et l'axe des abscisses).

On a

$$\alpha - \beta \not\in \pi\mathbb{Z}$$

Notons Θ l'ensemble des angles entre les $x \in T$ et l'axe des abscisses.

Puisque $\frac{x-y}{\|x-y\|} \in T$ and $\frac{x+y}{\|x+y\|} \in T$.
Alors $\frac{\alpha+\beta}{2} \in \Theta$, et $\frac{\alpha-\beta+\pi}{2} \in \Theta$.



Puisque

$$\frac{\alpha - \left(\frac{\alpha+\beta}{2}\right)}{2} = \frac{\alpha - \beta}{4} \not\in \pi\mathbb{Z}$$

On a donc $\frac{\alpha-\beta}{4} \in \Theta$.

Ainsi, par récurrence, pour tous $k, l \in \mathbb{Z}$ et pour tout $n \in \mathbb{N}^*$

$$\frac{k\alpha + l\beta}{2^n} \in \Theta$$

Avec $\alpha \neq 0$ ou $\beta \neq 0$, alors la suite $\left(\frac{k\alpha+l\beta}{2^n}\right)_{k,l\in\mathbb{Z},n\in\mathbb{N}^*}$ est dense dans $\mathbb{R}$.

Donc, pour tout angle γ, il existe une suite de vecteurs unitaires qui converge vers le vecteur unitaire d'angle γ.

Par fermeture, T contient tous les vecteurs de tous les angles.

Ainsi, $\mathcal{C} \subset T$.

Par suite,

$$T = \mathcal{C}$$

19. On définie, $\varphi : (x, y) \longmapsto \langle A^{-1}x, A^{-1}y\rangle$, avec $\langle ., .\rangle$ le produit scalaire associé à $\|.\|_2$.

On a bien que φ est définie, et il s'agit bien d'un produit scalaire.

Il suffit de montrer que pour tout $x \in \mathbb{R}^2$, on a $\varphi(x, x) = \|x\|^2$ pour conclure.

Notons

$$\Re = \{x \in \mathcal{C} | \|Ax\| = 1\}$$

Il s'agit d'une partie fermée de $\mathcal{C}$.

D'après la question 17, on a $(e_1, e_2) \in \Re$, qui est une base de $\mathbb{R}^2$, avec $e_1 \not= \pm e_2$.

Pour tout $a, b \in \Re$,

$$\|A(a + b)\|^2 + \|A(a - b)\|^2 \geqslant 4.$$

Avec $a, b \in \mathcal{C}$, alors $\|A(a + b)\| \leqslant \|a + b\|_2$ et $\|A(a - b)\| \leqslant \|a - b\|_2$.

Avec

$$\begin{aligned} \|a + b\|_2^2 + \|a - b\|_2^2 &= 2(\|a\|_2^2 + \|b\|_2^2) \\ &= 4 \end{aligned}$$

.

Alors,

$$(\|a + b\|_2^2 - \|A(a + b)\|^2) + (\|a - b\|_2^2 - \|A(a - b)\|^2) \leqslant 0$$

Avec $A \in \mathcal{K}$, donc $\|a+b\|^2-\|A(a+b)\|^2 \geqslant 0$ et $\|a-b\|^2-\|A(a-b)\|^2 \geqslant 0$.

Ainsi, $\|a - b\|_2 = \|A(a - b)\|$ et $\|a - b\|_2 = \|A(a - b)\|$.

Par suite, $\frac{a-b}{\|a-b\|_2} \in \Re$ et $\frac{a+b}{\|a+b\|_2} \in \Re$.

Ainsi, d'après la question précédente, $\Re = \mathcal{C}$.

D'où, pour tout $x \in \mathbb{R}^2$,

$$\|Ax\| = \|x\|_2$$

Par suite,

$$\begin{aligned}\varphi(x,x) &= \|A^{-1}x\|_2^2\\ &= \|A^{-1}(Ax)\|^2\\ &= \|x\|^2\end{aligned}$$

D'où le résultat.

4. Algèbres valuées

20.a. Soit $x \in A$, alors par définition, il existe $n \in \mathbb{N}^*$ et $a_0, \dots, a_{n-1} \in \mathbb{R}$ tels que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

Par décomposition en éléments simples dans $\mathbb{R}$ du polynôme $X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$. il existe $b_1, \dots, b_r, \alpha_1, \dots, \alpha_l, \beta_1, \dots, \beta_l \in \mathbb{R}$ tels que

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 = \prod_{i=1}^{r}(X - b_i)\prod_{i=1}^{l}(X^2 - \alpha_i X - \beta_i)$$

Donc,

$$\prod_{i=1}^{r}(x - b_i)\prod_{i=1}^{l}(x^2 - \alpha_i x - \beta_i) = 0$$

Puisque A est sans diviseur de zéro, il existe $i \in [\![1, r]\!]$ tel que $x = b_i$ ou bien il existe $i \in [\![1, l]\!]$ tel que $x^2 = \alpha_i x + \beta_i$.

Dans le premier cas, on a $x^2 = b_i x \in x + \mathbb{R}x$.

Dans le deuxième cas, on a $x^2 \in x + \mathbb{R}x$.

Ainsi, dans tous les cas, $x^2 \in x + \mathbb{R}x$.

D'où le résultat.

20.b. Puisque $A \neq \mathbb{R}$, il existe $a, b \in \mathbb{R}$ tels que $x^2 = ax + b$ avec $a^2 + 4b < 0$.

Ainsi,

$$\begin{aligned}\left(x - \frac{a}{2}\right)^2 &= b + \frac{a^2}{4}\\ &= \frac{a^2 + 4b}{4}\end{aligned}$$

On pose

$$y = \frac{2}{\sqrt{-a^2-4b}}\left(x - \frac{a}{2}\right)$$

On a

$$\mathbb{R} + \mathbb{R}x = \mathbb{R} + \mathbb{R}y$$

car $(y, 1)$ est $\mathbb{R}$-libre.

Définissons $\varphi : a + yb \in \mathbb{R} + \mathbb{R}x \longmapsto a + ib$. On a φ est bien définie et bijective (par la libérté de $(1, y)$), et de plus, pour tous $a+by, c+dy \in \mathbb{R}+\mathbb{R}x$, on a :

$$\begin{aligned}\varphi((a+by)+(c+dy)) &= (a+c)+i(b+d)y \\ &= \varphi(c+dy)+\varphi(c+dy)\end{aligned}$$

et

$$\begin{aligned}\varphi((a+by)(c+dy)) &= \varphi(ac+(bc+ad)y-bd) \\ &= ac-bd+i(bc+ad) \\ &= \varphi(a+by)\varphi(c+dy)\end{aligned}$$

Donc φ est un morphisme d'algèbre bijectif.

21. Montrons qu'il existe $i_A \in A$ tel que $i_A^2 = -1$.

Pour tout $x \in A$, on a $x^2 \in \mathbb{R} + \mathbb{R}x$, donc il existe $a_x, b_x \in \mathbb{R}$ tels que $x^2 = a_x x + b_x$.

Supposons que pour tout $x \in A$, $a_x^2 + 4b_x \geqslant 0$.

Alors

$$\left(x - \frac{a_x - \sqrt{a_x^2+4b_x}}{2}\right)\left(x - \frac{a_x + \sqrt{a_x^2+4b_x}}{2}\right) = 0$$

Or, A est sans diviseur de zéro, donc soit $x = \frac{a_x-\sqrt{a_x^2+4b_x}}{2} \in \mathbb{R}$, soit $x = \frac{a_x+\sqrt{a_x^2+4b_x}}{2} \in \mathbb{R}$.

Cela implique que $A = \mathbb{R}$, ce qui est absurde.

Ainsi, il existe $x \in \mathbb{R}$ et $a, b \in \mathbb{R}$ tels que $x^2 - ax - b = 0$,avec $a^2 + 4b < 0$.

On a alors

$$\begin{aligned}\left(x - \frac{a}{2}\right)^2 &= b + \frac{a^2}{4} \\ &= \frac{a^2+4b}{4}\end{aligned}$$

On pose

$$i_A = \frac{2}{\sqrt{-a^2-4b}}\left(x - \frac{a}{2}\right)$$

On a alors $i_A^2 = -1$.

22.a. Soient $x, y \in A$, on a :

$$\begin{aligned} T(xy) &= i_A x y i_A \\ &= -i_A x (i_A i_A) y i_A \\ &= -(i_A x i_A)(i_A y i_A) \\ &= -T(x)T(y) \end{aligned}$$

22.b. On a, pour tout $x \in A$,

$$\begin{aligned} T \circ T(x) &= i_A (i_A x i_A) i_A \\ &= x \\ &= \mathrm{id}(x) \end{aligned}$$

Donc $T \circ T = \mathrm{id}$, et ainsi

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

est un polynôme annulateur de T. De plus, $X+1$ et $X-1$ sont premiers entre eux. D'après le théorème de décomposition des noyaux, on a :

$$A = \ker(T - \mathrm{id}) \oplus \ker(T + \mathrm{id})$$

23. Montrons que $\ker(T + \mathrm{id}) = U$

Soit $x \in \mathrm{Ker}(T + \mathrm{id}) \backslash \{0\}$. Alors $T(x) = -x$, donc $x = -i_A x i_A$, ainsi $i_A x = x i_A$.

Donc x et i_A commutent. Par suite,

$$(i_A x)^2 = -x^2$$

En particulier, $i_A x \not\in \mathbb{R}$, ce qui implique que $(i_A x, 1)$ est une base de $\mathbb{R} + \mathbb{R}x$.

Ainsi, il existe $a, b \in \mathbb{R}$ tels que

$$x = a + b i_A \in U$$

Réciproquement, si $x \in U$, alors il existe $(a, b) \in \mathbb{R}^2$ tel que

$$x = a + bi_A$$

Donc

$$\begin{aligned} T(x) &= i_A(a + bi_A)i_A \\ &= i_A a i_A - i_A b \\ &= a i_A i_A - b i_A \\ &= -a - b i_A \\ &= -x \end{aligned}$$

Donc

$$x \in \mathrm{Ker}(T + \mathrm{id})$$

Ainsi, $\ker(T + \mathrm{id}) = U$, et puisque A n'est pas isomorphe à $\mathbb{C}$ et que Ker(T+id) est de dimension 2, alors Ker(T-id) n'est pas réduit à zéro.

24. Fixons $\beta \in \mathrm{Ker}(T - \mathrm{id}) \backslash \{0\}$.

24.a. Montrons que l'application $x \longmapsto \beta x$ envoie $\ker(T - \mathrm{id})$ dans $\ker(T + \mathrm{id})$.

Soit $x \in \mathrm{Ker}(T - \mathrm{id})$, donc $T(x) = x$.

Or, $\beta \in \mathrm{Ker}(T - \mathrm{id})$, donc $T(\beta) = \beta$.

D'après la question 22.a, on a :

$$\begin{aligned} T(\beta x) &= -T(\beta)T(x) \\ &= -\beta x \end{aligned}$$

Par suite, $\beta x \in \ker(T + \mathrm{id})$, donc $x \longmapsto \beta x$ envoie $\ker(T - \mathrm{id})$ dans $\ker(T + \mathrm{id})$.

D'après la question précédente, on a $\beta \ker(T - \mathrm{id}) \subset U$.

Ainsi, $\dim_{\mathbb{R}} \ker(T - \mathrm{id}) \leqslant \dim_{\mathbb{R}} U$

De même $x \longmapsto \beta x$ envoie $\ker(T+\mathrm{id})$ dans $\ker(T-\mathrm{id})$, donc $\dim_{\mathbb{R}}(\ker(T-\mathrm{id})) \geqslant \dim_{\mathbb{R}} U$.

On en déduit que

$$\dim_{\mathbb{R}} U = \dim_{\mathbb{R}} \ker(T - \mathrm{id})$$

Par suite, $U = \ker(T - \mathrm{id})$.

24.b. Montrons que $\beta^2 \in]-\infty, 0[$.

D'après ce qui précéde, on a $\beta \ker(T - \mathrm{id}) \subset U$.

Donc, $\beta^2 \ker(T - \mathrm{id}) \subset \beta U = \ker(T - \mathrm{id})$.

Comme $\ker(T - \mathrm{id}) \not= \{0\}$, il en résulte que $\beta^2 \in \mathbb{R}$.

Supposons par l'absurde que $\beta^2 > 0$. Alors, $\beta = \sqrt{\beta^2} \in \mathbb{R}$, donc $\beta U = U$.

Ainsi,

$$\begin{aligned} A &= U + \beta U \\ &= U \end{aligned}$$

Or, U est isomorphe à $\mathbb{C}$, ce qui est absurde, car A n'est pas isomorphe à $\mathbb{R}$ ni à $\mathbb{C}$.

D'où le résultat.

24.c. On a $i_A \in \mathrm{Ker}(T + \mathrm{id})$, donc $\beta i_A \in \beta U$. Ainsi, $(\beta, \beta i_A)$ est une base de βU, et $(1, i_A)$ est une base de U. Par somme directe, on a $(1, i_A, \beta, \beta i_A)$ est une base de A.

Donc A est isomorphe à $\mathbb{H}$. (car $\dim_{\mathbb{R}} \mathbb{H} = 4$)

25. Soient $x, y \in A$ tels que $xy = yx$ et tels que $V = \mathbb{R}x + \mathbb{R}y$ soit de dimension 2 sur $\mathbb{R}$.

Montrons que pour tout $u, v \in V$, on a

$$\|u + v\|^2 + \|u - v\|^2 \geqslant 4\|u\|.\|v\|$$

Soient $u, v \in \mathbb{R}x + \mathbb{R}y$. Puisque x, y commutent, alors u, v commutent également, en tant que polynômes $x$et y. Or,

$$\|u + v\|^2 = \|(u + v)^2\| \text{ and } \|u - v\|^2 = \|(u - v)^2\|$$

Par l'inégalité triangulaire inverse, on a

$$\begin{aligned} \|u + v\|^2 + \|u - v\|^2 &\geqslant \|(u + v)^2 - (u - v)^2\| \\ &\geqslant 4\|u\|.\|v\| \end{aligned}$$

Montrons que la restriction de $\|.\|$ à V provient d'un produit scalaire sur V.

On a $V = x\mathbb{R} + y\mathbb{R}$ de dimension 2, donc V est isomorphe à $\mathbb{R}^2$.

Il existe un isomorphisme d'espaces vectoriels $\varphi : \mathbb{R}^2 \to V$.

On a, pour tout $x, y \in \mathbb{R}^2$,

$$\|\varphi(x) + \varphi(y)\|^2 + \|\varphi(x) - \varphi(y)\|^2 \geqslant 4\|\varphi(x)\|.\|\varphi(y)\|$$

Ainsi,

$$\|\varphi(x + y)\|^2 + \|\varphi(x - y)\|^2 \geqslant 4\|\varphi(x)\|.\|\varphi(y)\|$$

Avec $\psi : x \in \mathbb{R}^2 \longmapsto \|\varphi(x)\|$ est une norme sur $\mathbb{R}^2$, en effet, pour tout $x, y \in \mathbb{R}^2$ et $\lambda \in \mathbb{R}$, on a

Si $\|\varphi(x)\| = 0$, alors $\varphi(x) = 0$, et par injectivité, on a $x = 0$.

De plus, $\|\varphi(\lambda x)\| = |\lambda|\|\varphi(x)\|$ et $\|\varphi(x+y)\| = \|\varphi(x)+\varphi(y)\| \leqslant \|\varphi(x)\| + \|\varphi(y)\|$.

D'après le théorème A, on a $x \longmapsto \|\varphi(x)\|$ provient d'un produit scalaire $\langle .|. \rangle$.

Notons

$$\zeta : (u, v) \in V \longmapsto \langle \varphi^{-1}(u), \varphi^{-1}(v) \rangle$$

.

On a ζ est symétrique. De plus, pour tout $u \in V$,

$$\begin{aligned} \zeta(u, u) &= \|\varphi(\varphi^{-1}(u))\| \\ &= \|u\| \\ &\geqslant 0 \end{aligned}$$

Donc ζ est positif.

Par linéarité de φ^{-1}, on a ζ est bilinéaire.

Et par injectivité, ζ est définie.

Donc ζ définie un produit scalaire sur V.

$\|.\|$ provient de ζ.

D'où le résultat.

26. Soit $x \in A$. Si $x \in \mathbb{R}$, il est évident que

$$x^2 \in \mathbb{R} + \mathbb{R}x$$

Supposons que $x \in A\backslash\mathbb{R}$, alors $V = x + \mathbb{R}x$ est de dimension 2.

D'après la question précédente, $\|.\|$ provient d'un produit scalaire sur V.

Notons y un vecteur orthogonal non nul à 1 dans V.

Ainsi, on a $(1, y)$ forme une base de V.

Donc il existe $a, b \in \mathbb{R}$ tels que $x = a + by$.

Ainsi,

$$x^2 = a^2 + 2aby + y^2$$

Avec :

$$\begin{aligned}
\langle 1, y^2\rangle &= \frac{1}{2}(\|y^2\|^2 + 1 - \|y^2 - 1\|^2) \\
&= \frac{1}{2}(\|y^2\|^2 + 1 - \|y - 1\|^2\|y + 1\|^2) \\
&= \frac{1}{2}(\|y\|^4 + 1 - (\|y\|^2 + 1)^2) \\
&= \frac{1}{2}(\|y\|^4 + 1 - \|y\|^4 - 2\|y\|^2 - 1\Big) \\
&= -\|y^2\| \\
&= -\|1\|^2\|y^2\|
\end{aligned}$$

Et donc, d'après le cas d'égalité dans l'inégalité de Cauchy-Schwarz, on a $y^2 \in \mathbb{R}$.

D'où :

$$\begin{aligned}
x^2 &\in \mathbb{R} + \mathbb{R}_y \\
&= \mathbb{R} + \mathbb{R}_x
\end{aligned}$$

27. D'après la question précédente, on a A est algébrique (car Pour tout $x \in \mathbb{R}$, il existe $a, b \in \mathbb{R}$ tels que $x^2 = ax + b$).

De plus, A est sans diviseur de zéro : en effet, pour $x, y \in A$ tels que $xy = 0$, on alors

$\|x\|\|y\| = \|xy\| = 0$

Par conséquent $\|x\| = 0$ ou $\|y\| = 0$.

Par suite $x = 0$ou $y = 0$.

Ainsi, d'après le théorème B, A est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$.

D'où le théorème C.

ÉCOLES NORMALES SUPÉRIEURES
CONCOURS D'ADMISSION 2018
FILIÈRE MPI

Composition de mathématiques - C - (ULCR)

Corrigé par : SABIR ILYASS.

⋆ ⋆ ⋆

Partie I

Dans cette partie, E est un ensemble fini ou dénombrable. L'ensemble des probabilités sur E est l'ensemble

$$\mathcal{P}(E) = \left\{ \mu : E \to [0,1] | \sum_{x \in E} \mu(x) = 1 \right\}$$

Une matrice de transition sur E est une application $P : E \times E \to [0,1]$ telle que, pour tout $x \in E$, on a

$$\sum_{y \in E} P(x,y) = 1$$

Le produit PQde deux matrices de transition P et Q est défini par

$$\forall (x,z) \in E \times E, (PQ)(x,z) = \sum_{y \in E} P(x,y)Q(y,z)$$

On notera I la matrice de transition définie par

$$I(x,y) = \begin{cases} 1 \text{ si } x = y \\ 0 \text{ si } x \not= y \end{cases}$$

1.1. (a) **Vérifier que si P et Q sont des matrices de transition, alors PQ est aussi une matrice de transition.**

Soient P, Q deux matrices de transition, on a pour tout $x \in E$

$$\sum_{y \in E} (PQ)(x,y) = \sum_{y \in E} \sum_{z \in E} P(x,z)Q(z,y)$$

Avec, la famille $(P(x,z)Q(z,y))_{(y,z)\in E\times E}$ est à termes positifs, donc via le théorème de Fubini-Tonelli on a :

$$\begin{aligned}\sum_{y\in E}(PQ)(x,y) &= \sum_{z\in E}\sum_{y\in E}P(x,z)Q(z,y)\\ &= \sum_{z\in E}P(x,z)\sum_{y\in E}Q(z,y)\end{aligned}$$

Puisque Q est une matrice de transition, alors $\sum\limits_{y\in E}Q(z,y)=1$,

Ensuite, $\sum\limits_{y\in E}(PQ)(x,y) = \sum\limits_{z\in E}P(x,z) = 1$, car P est une matrice de transition, d'où le résultat.

(b) **Vérifier que si P, Q et R sont des matrices de transition, on a $(PQ)R = P(QR)$.**

Pour tout $(x,y)\in E\times E$. On a

$$\begin{aligned}(PQ)R(x,y) &= \sum_{z\in E}(PQ)(x,z)R(z,y)\\ &= \sum_{z\in E}\sum_{t\in E}P(x,t)Q(t,z)R(z,y)\end{aligned}$$

La famille $(P(x,t)Q(t,z)R(z,y))_{(z,t)\in E\times E}$ est à termes positifs, donc d'après le théorème de Fubini-Tonelli, on peut permuter les sommes. Ainsi, on a :

$$\begin{aligned}(PQ)R(x,y) &= \sum_{t\in E}\sum_{z\in E}P(x,t)Q(t,z)R(z,y)\\ &= \sum_{t\in E}P(x,t)\sum_{z\in E}Q(t,z)R(z,y)\\ &= \sum_{t\in E}P(x,t)(\mathrm{QR})(t,y)\\ &= P(QR)(x,y)\end{aligned}$$

Et ceci est vrai pour tout $(x,y)\in E\times E$, donc $(PQ)R = P(QR)$.

(c) Pour tout entier $n\geqslant 0$ et toute matrice de transition P, on définit P^n par $P^0 = I$ et la relation de récurrence $P^{n+1} = P^nP$ si $n\geqslant 0$. **Vérifier que P^n est bien une matrice de transition.**

Par récurrence sur $n\in\mathbb{N}$, on a pour $n=0$, $P^0 = I$, qui est bien une matrice de transition.

Soit $n \in \mathbb{N}$. Supposons que P^nest une matrice de transition. Puisque Pest une matrice de transition, alors d'après la question **1.1.a**, le produit $P^{n+1} = P^n P$ est une matrice de transition,

D'où le résultat.

Étant donnés $\mu \in \mathcal{P}(E)$, une matrice de transition$P$, et des fonctions bornées $f : E \to \mathbb{R}$ et$g : E \to \mathbb{R}$, on définit les nombres réels suivants

$$\begin{aligned} \mu[f] &= \sum_{x\in E} \mu(x)f(x). \\ \mu P(y) &= \sum_{x\in E} \mu(x)P(x,y), o\grave{u} y \in E. \\ Pf(x) &= \sum_{y\in E} P(x,y)f(y), o\grave{u} x \in E. \\ \langle f, g\rangle_\mu &= \mu[fg]. \end{aligned}$$

1.2. Soit $\mu \in \mathcal{P}(E)$, soient P et Q des matrices de transition et soit $f : E \to \mathbb{R}$ une fonction bornée.

(a) **Montrer que $\mu P \in \mathcal{P}(E)$ et que $(\mu P)Q = \mu(PQ)$.**

Montrons d'abord que $\mu P \in \mathcal{P}(E)$.

On a, pour tout $x \in E$

$$\sum_{x\in E} \mu P(x) = \sum_{x\in E}\sum_{y\in E} \mu(y)P(y,x)$$

La famille $(\mu(y)P(y,x))_{(x,y)\in E\times E}$ est à termes positifs, donc via le théorème de Fubini-Tonelli, on a :

$$\begin{aligned} \sum_{x\in E} \mu P(x) &= \sum_{y\in E}\sum_{x\in E} \mu(y)P(y,x) \\ &= \sum_{y\in E} \mu(y)\left(\sum_{x\in E} P(y,x)\right) \\ &= \sum_{y\in E} \mu(y)(\text{car } P \text{ est une matrice de transition}) \\ &= 1(\text{car } \mu \in \mathcal{P}(E)) \end{aligned}$$

De plus, pour tout $x \in E$, on a

$$0 \leqslant \mu P(x) \leqslant \sum_{x\in E} \mu P(x) = 1$$

Donc, $\mu P \in \mathcal{P}(E)$.

Montrons maintenant que $(\mu P)Q = \mu(PQ)$.

On a, pour tout $y \in E$,

$$\begin{aligned}(\mu P)Q(x) &= \sum_{x\in E}(\mu P)(x)Q(x,y)\\ &= \sum_{x\in E}\sum_{z\in E}\mu(z)P(z,x)Q(x,y)\end{aligned}$$

Avec la famille $(\mu(z)P(z,x)Q(x,y))_{(x,z)\in E\times E}$ est à termes positifs, donc, via le théorème de Fubini-Tonelli, on a :

$$\begin{aligned}(\mu P)Q(x) &= \sum_{z\in E}\sum_{x\in E}\mu(z)P(z,x)Q(x,y)\\ &= \sum_{z\in E}\mu(z)\left(\sum_{x\in E}P(z,x)Q(x,y)\right)\\ &= \sum_{z\in E}\mu(z)(PQ)(z,y)\\ &= \mu(PQ)(y)\end{aligned}$$

D'où le résultat.

(*b*) **Montrer que $Pf : E \to \mathbb{R}$ est une fonction bornée et que $\mu P[f] = \mu[Pf]$.**

On a pour tout $x \in E$:

$$\begin{aligned}|Pf(x)| &= \left|\sum_{y\in E}P(x,y)f(y)\right|\\ &\leqslant \sum_{y\in E}P(x,y)|f(y)|\\ &\leqslant \max_{z\in E}|f(z)|\sum_{y\in E}P(x,y)\\ &\leqslant \max_{z\in E}|f(z)|\\ &< +\infty \quad (\text{car } f \text{ est born\'ee})\end{aligned}$$

D'où Pf est bornée. Montrons maintenant que $\mu P[f] = \mu[Pf]$

On a

$$\begin{aligned}\mu P[f] &= \sum_{x\in E}\mu P(x)f(x)\\ &= \sum_{x\in E}\sum_{y\in E}\mu(y)P(y,x)f(x)\end{aligned}$$

La famille $(\mu(y)P(y,x)f(x))_{(x,y)\in E\times E}$ est sommable, en effet, on a

$$\begin{aligned}\sum_{y\in E}\sum_{x\in E}|\mu(y)P(y,x)f(x)| &= \sum_{y\in E}\mu(y)\sum_{x\in E}P(y,x)|f(x)|\\ &\leqslant \|f\|_\infty\sum_{y\in E}\mu(y)\sum_{x\in E}P(y,x)\\ &= \|f\|_\infty\sum_{y\in E}\mu(y)\\ &= \|f\|_\infty\\ &< +\infty\end{aligned}$$

Donc, d'après le théorème de Fubini-Tonelli, la famille $(\mu(y)P(y,x)f(x))_{(x,y)\in E\times E}$ est sommable.

Et on a

$$\begin{aligned}\mu P[f] &= \sum_{x\in E}\sum_{y\in E}\mu(y)P(y,x)f(x)\\ &= \sum_{y\in E}\mu(y)\left(\sum_{x\in E}P(y,x)f(x)\right)\\ &= \sum_{y\in E}\mu(y)Pf(y)\\ &= \mu[Pf]\end{aligned}$$

(c)**Montrer que** $(PQ)f = P(Qf)$**.**

Pour tout $x\in E$, on a

$$\begin{aligned}(PQ)f(x) &= \sum_{y\in E}(PQ)(x,y)f(y)\\ &= \sum_{y\in E}\sum_{z\in E}P(x,z)Q(z,y)f(y)\end{aligned}$$

La famille $(P(x,z)Q(z,y)f(y))_{(y,z)\in E\times E}$ est sommable, en effet

$$\begin{aligned}\sum_{z\in E}\sum_{y\in E}|P(x,z)Q(z,y)f(y)| &= \sum_{z\in E}\sum_{y\in E}P(x,z)Q(z,y)|f(y)|\\ &\leqslant \|f\|_\infty\sum_{z\in E}P(x,z)\left(\sum_{y\in E}Q(z,y)\right)\\ &= \|f\|_\infty\sum_{z\in E}P(x,z)\\ &= \|f\|_\infty\\ &< +\infty\end{aligned}$$

Et donc, via le thèoréme de Fubini-Tonelli, on a

$$\begin{aligned}(PQ)f(x) &= \sum_{z\in E}\sum_{y\in E} P(x,z)Q(z,y)f(y)\\ &= \sum_{z\in E} P(x,z)\left(\sum_{y\in E} Q(z,y)f(y)\right)\\ &= \sum_{z\in E} P(x,z)(Qf)(z)\\ &= P(Qf)(x)\end{aligned}$$

Et cela pour tout $x \in E$. D'où $(PQ)f = P(Qf)$.

Une matrice de transition P est dite **réversible** par rapport à un élément π de $\mathcal{P}(E)$ si pour tout $(x, y) \in E^2$, on a

$$\pi(x)P(x,y) = \pi(y)P(y,x).$$

Une matrice de transition P est dite **irréductible** si, pour tout $(x, y) \in E^2$, il existe un entier $n \geqslant 1$ tel que $P^n(x, y) > 0$.

On se donne, sur un espace probabilisé $(W, \mathcal{A}, \mathbb{P})$, une suite $(U_n)_{n\geqslant 1}$ de variables aléatoires réelles indépendantes et identiquement distribuées, et une variable aléatoireX_0 à valeurs dans E, indépendante de la suite $(U_n)_{n\geqslant 1}$. On se donne une fonction $F : E \times \mathbb{R} \to E$ et on définit une suite $(X_n)_{n\geqslant 1}$ de variables aléatoires à valeurs dans E en posant, pour tout entier $n \geqslant 1$,

$$X_n = F(X_{n-1}, U_n)$$

La loi de X_n est notéeμ_n. On rappelle que c'est l'élément de $\mathcal{P}(E)$ défini par $\mu_n(x) = \mathbb{P}[X_n = x]$ pour tout $x \in E$.

L'espérance d'une variable aléatoire réelle bornée X sera notée $\mathbb{E}[X]$.

Pour tout $(x, y) \in E^2$, on pose $P(x, y) = \mathbb{P}[F(x, U_1) = y]$.

1.3. (a) Vérifier que P est une matrice de transition et que, pour tout entier $n \geqslant 0$ et tout $(x_0, \ldots, x_n) \in E^{n+1}$, on a

$$\mathbb{P}[X_0 = x_0, \ldots, X_n = x_n] = \mu_0(x_0)\prod_{i=1}^{n} P(x_{i-1}, x_i).$$

Vérifiant d'abord que P est une matrice de transition. On a pour tout $x \in E$:

$$\begin{aligned}\sum_{y\in E} P(x,y) &= \sum_{y\in E} \mathbb{P}[F(x,U_1)=y] \\ &= 1\end{aligned}$$

D'où P est une matrice de transition.

On a pour tout $n \in \mathbb{N}$

$$\begin{aligned}\mathbb{P}[X_0=x_0,...,X_n=x_n] &= \mathbb{P}[X_0=x_0,...,X_{n-1}=x_{n-1},X_n=x_n] \\ &= \mathbb{P}[X_0=x_0,...,X_{n-1}=x_{n-1},F(X_{n-1},U_n)=x_n] \\ &= \mathbb{P}[X_0=x_0,...,X_{n-1}=x_{n-1},F(x_{n-1},U_n)=x_n]\end{aligned}$$

Par itération, on obtient

$$\mathbb{P}[X_0=x_0,...,X_n=x_n] = \mathbb{P}[X_0=x_0,F(x_0,U_n)=x_1...,,F(x_{n-1},U_n)=x_n]$$

Avec $(U_n)_{n\geqslant 1}$ est une suite de variables aléatoires réelles indépendantes et identiquement distribuées, alors pour tout $x \in \mathbb{R}$, $(F(x,U_k))_{k\geqslant 1}$ est une suite de variables aléatoires indépendantes et identiquement distribuées. Par ailleurs, X_0 est indépendante de la suite $(U_n)_{n\geqslant 1}$. Ainsi, X_0est également indépendante de la suite $(F(x,U_k))_{k\geqslant 1}$, où $x \in E$.

On a alors

$$\begin{aligned}\mathbb{P}[X_0=x_0,...,X_n=x_n] &= \mathbb{P}[X_0=x_0]\prod_{k=1}^{n}\mathbb{P}[F(x_{k-1},U_n)=x_k] \\ &= \mathbb{P}[X_0=x_0]\prod_{k=1}^{n}\mathbb{P}[F(x_{k-1},U_1)=x_k] \\ &= \mu_0(x_0)\prod_{k=1}^{n}P(x_{k-1},x_k)\end{aligned}$$

(b)**Montrer que pour tout entier $n \geqslant 0$ et tout $(x_0,...,x_n) \in E^{n+1}$ tel que $\mathbb{P}[X_0=x_0,...,X_n=x_n]>0$, on a, pour tout $x \in E$,**

$$\mathbb{P}[X_{n+1}=x|X_0=x_0,...,X_n=x_n]=P(x_n,x)$$

Soit $n \in \mathbb{N}$, $x \in E$ et soit $(x_0,...,x_n) \in E^{n+1}$ tel que $\mathbb{P}[X_0=x_0,...,X_n=x_n]>0$.

Posons $x_{n+1} = x$. En utilisant la question précédente, on a

$$\begin{aligned}
\mathbb{P}[X_{n+1} = x_{n+1} | X_0 = x_0, ..., X_n = x_n] &= \frac{\mathbb{P}[X_0 = x_0, ..., X_n = x_n, X_{n+1} = x_{n+1}]}{\mathbb{P}[X_0 = x_0, ..., X_n = x_n]} \\
&= \frac{\mu_0(x_0) \prod_{k=1}^{n+1} P(x_{k-1}, x_k)}{\mu_0(x_0) \prod_{k=1}^{n} P(x_{k-1}, x_k)} \\
&= P(x_n, x_{n+1}) \\
&= P(x_n, x)
\end{aligned}$$

D'où le résultat.

(*c*)**Montrer que pour tout**$n \geqslant 0$, **on a** $\mu_n = \mu_0 P^n$ **et que si** $\mu_0 P = \mu_0$, **alors** $\mu_n = \mu_0$ **pour tout** $n \geqslant 0$**.**

Soit $n \in \mathbb{N}$, pour tout $x \in E$, on a, par formule de probabilité totale, en utilisant la question 1.3.a, et en posant $x_n = x$:

$$\begin{aligned}
\mu_n(x) &= \mathbb{P}[X_n = x] \\
&= \sum_{x_0 \in E} \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \mathbb{P}[X_n = x, X_0 = x_0, ..., X_{n-1} = x_{n-1}] \\
&= \sum_{x_0 \in E} \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \mathbb{P}[X_0 = x_0, ..., X_{n-1} = x_{n-1}, X_n = x] \\
&= \sum_{x_0 \in E} \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \mu_0(x_0) \prod_{k=1}^{n} P(x_{k-1}, x_k) \\
&= \sum_{x_0 \in E} \mu_0(x_0) \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \prod_{k=1}^{n} P(x_{k-1}, x_k)
\end{aligned}$$

Par une simple récurrence, on peut montrer la formule qui donne le produit fini de plusieurs matrices de transitions :

$$\sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \prod_{k=1}^{n} P(x_{k-1}, x_k) = P^n(x_0, x_n)$$

D'où

$$\begin{aligned}
\mu_n(x) &= \sum_{x_0 \in E} \mu_0(x_0) P^n(x_0, x_n) \\
&= \mu_0 P^n(x_n) \\
&= \mu_0 P^n(x)
\end{aligned}$$

Et ça pour tout $x \in E$, alors

$$\mu_n = \mu_0 P^n$$

Supposons maintenant que $\mu_0 P = \mu_0$, Et montrons par récurrence que $\mu_n = \mu_0$ pour tout $n \geqslant 0$.

Pour $n = 0$, on a bien $\mu_0 P^0 = \mu_0 I = \mu_0$.

Soit $n \in \mathbb{N}$, supposons que $\mu_n = \mu_0 P^n$, et montrons que $\mu_n = \mu_0 P^{n+1}$.

On a par hypothèse de récurrence

$$\mu_n P^{n+1} = (\mu_0 P^n) P = \mu_0 P = \mu_0$$

D'où le résultat.

(*d*) **Montrer que pour tout** $n \geqslant 0$ **et tout** $x \in E$ **tel que** $\mu_0(x) > 0$**, on a**

$$\mathbb{P}[X_n = y | X_0 = x] = P^n(x, y) \text{ pour tout } y \in E.$$

Soit $n \in \mathbb{N}$. On a, pour tout $x, y \in E$, tel que $\mu_0(x) > 0$

$$\begin{aligned} \mathbb{P}[X_n = y | X_0 = x] &= \frac{\mathbb{P}[X_n = y, X_0 = x]}{\mathbb{P}[X_0 = x]} \\ &= \frac{1}{\mu_0(x)} \mathbb{P}[X_n = y, X_0 = x] \end{aligned}$$

Notons $x_0 = x$, et $x_n = y$. On a alors :

$$\begin{aligned} \mathbb{P}[X_n = y | X_0 = x] &= \frac{1}{\mu_0(x)} \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \mathbb{P}[X_0 = x_0, ..., X_{n-1} = x_{n-1}, X_n = x] \\ &= \frac{1}{\mu_0(x)} \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \mu_0(x_0) \prod_{k=1}^{n} P(x_{k-1}, x_k) \\ &= \sum_{x_1 \in E} \cdots \sum_{x_{n-1} \in E} \prod_{k=1}^{n} P(x_{k-1}, x_k) \\ &= P^n(x_0, x_n) \\ &= P^n(x, y) \end{aligned}$$

D'où le résultat.

(*e*) **Montrer que pour toute fonction** $f : E \to \mathbb{R}$ **bornée, on a**

$$\mathbb{E}[f(X_n)] = \mu_0[P^n f].$$

On a

$$\begin{aligned}
\mathbb{E}[f(X_n)] &= \sum_{x\in E} f(x)\mathbb{P}[X_n = x] \\
&= \sum_{x\in E} f(x)\mu_n(x) \\
&= \sum_{x\in E} \mu_0 P^n(x) f(x) \\
&= \mu_0 P^n[f] \\
&= \mu_0[P^n f] \quad (d'\text{apr}\grave{\text{e}}s \text{ la question } 1.2.c)
\end{aligned}$$

À partir de maintenant, on supposera que

• P est réversible par rapport à une probabilité $\pi \in \mathcal{P}(E)$,

• il existe $a \in E$ tel que $\pi(a) > 0$ et tel que, pour tout $x \in E$, il existe un entier$n \geqslant 1$ pour lequel $P^n(a, x) > 0$.

1.4. Montrer que $\pi P = \pi$**.**

On a, pour tout $x \in E$

$$\begin{aligned}
\pi P(x) &= \sum_{y\in E} \pi(y)P(y, x) \\
&= \sum_{y\in E} \pi(x)P(x, y) \\
&= \pi(x)\sum_{y\in E} P(x, y) \\
&= \pi(x)
\end{aligned}$$

Et ça pour tout $x \in E$, alors $\pi P = \pi$.

1.5. (*a*) **Montrer que pour tout** $n \geqslant 1$**, la matrice de transition** P^n**est réversible par rapport à** π**.**

Essayons de montrer le résultat par récurrence sur $n \in \mathbb{N}^*$.

Pour $n = 1$, par définition de P, P est réversible par rapport à π.

Soit $n \in \mathbb{N}^*$. Supposons que P^nest réversible par rapport à π, et montrons que P^{n+1}est réversible par rapport àπ.

On a

$$\begin{aligned}
\pi(x)P^{n+1}(x,y) &= \pi(x)(P^nP)(x,y) \\
&= \sum_{z\in E}\pi(x)P^n(x,z)P(z,y) \\
&= \sum_{z\in E}\pi(z)P^n(z,x)P(z,y) \\
&= \sum_{z\in E}\pi(z)P(z,y)P^n(z,x) \\
&= \sum_{z\in E}\pi(y)P(y,z)P^n(z,x) \\
&= \pi(y)\sum_{z\in E}P(y,z)P^n(z,x) \\
&= \pi(y)(PP^n)(y,x) \\
&= \pi(y)P^{n+1}(y,x)
\end{aligned}$$

Ainsi P^{n+1}est réversible par rapport àπ, d'où le résultat par récurrence sur $n \geqslant 1$.

(b)**Soit**$n \geqslant 1$ **et soit** $x \in E$**. Montrer que si** $P^n(a,x) > 0$**, alors** $P^n(x,a) > 0$**et** $\pi(x) > 0$.

D'après la question précédente, on a

$$\pi(a)P^n(a,x) = \pi(x)P^n(x,a)$$

Puisque $\pi(a) > 0$, et $P^n(a,x) > 0$, on en déduit que $\pi(x)P^n(x,a) > 0$.

Comme $\pi(x) \geqslant 0$, on obtient alors $P^n(x,a) > 0$et $\pi(x) > 0$.

(c) Montrer que $\pi(x) > 0$ **pour tout** $x \in E$**.**

On a pour tout $x \in E$, il existe un entier$n \geqslant 1$ pour lequel $P^n(a,x) > 0$. D'après la question précédente, on en conclut que $\pi(x) > 0$.

(d) Montrer que P **est irréductible.**

Soit $(x,y) \in E^2$, il existe $n_1, n_2 > 0$ tels que $P^{n_1}(a,x) > 0$ et $P^{n_2}(a,y) > 0$.

D'après la question précédente, on a $\pi(x) > 0$, $\pi(y) > 0$. On en déduit que :

$$\begin{aligned} P^{n_1+n_2}(x,y) &= (P^{n_1} \times P^{n_2})(x,y) \\ &= \sum_{z\in E} P^{n_1}(x,z)P^{n_2}(z,x) \\ &\geqslant P^{n_1}(x,a)P^{n_2}(a,x) \end{aligned}$$

Or, d'après la question 1.5.a, P^{n_1} est réversible par rapport àπ. Ainsi

$$P^{n_1}(x,a) = \frac{\pi(a)}{\pi(x)} P^{n_1}(a,x) > 0$$

Par conséquent, $P^{n_1+n_2}(x,y) > 0$, pour tout $(x,y) \in E^2$, et donc, par définition, P est irréductible.

1.6. Pour toute fonction $f : E \to \mathbb{R}$ bornée et tout entier $n \geqslant 1$, on pose

$$\mathcal{E}_n(f) = \frac{1}{2} \sum_{(x,y)\in E^2} [f(x) - f(y)]^2 \pi(x) P^n(x,y)$$

(a) Montrer que $\mathcal{E}_n(f) = \langle f - P^n f, f\rangle_\pi$.

On a

$$\begin{aligned} \langle f - P^n f, f\rangle_\pi &= \pi[(f - P^n f)f] \\ &= \sum_{x\in E} \pi(x)(f(x) - P^n f(x))f(x) \\ &= \sum_{x\in E} \pi(x) \left(f(x) - \sum_{y\in E} P^n(x,y) f(y) \right) f(x) \end{aligned}$$

Montrons que la famille $(\pi(x)(f(x) - f(y))f(x)P^n(x,y))_{(x,y)\in E^2}$ est sommable.

Puisque P est réversible par rapport à π, on a :

$$\begin{aligned} \sum_{(x,y)\in E^2} |\pi(x)(f(x) - f(y))f(x)P^n(x,y)| &= \sum_{(x,y)\in E^2} |\pi(y)(f(y) - f(x))f(y)P^n(y,x)| \\ &= \sum_{y\in E} \pi(y)|f(y)| \sum_{x\in E} |f(y) - f(x)|P^n(y,x) \\ &\leqslant 2\|f\|_\infty \sum_{y\in E} \pi(y)|f(y)| \sum_{x\in E} P^n(y,x) \\ &= 2\|f\|_\infty \sum_{y\in E} \pi(y)|f(y)| \end{aligned}$$

Car $\sum_{x\in E} P^n(y,x) = 1$, pour tout $y \in E$, puisque P^nest une matrice de transition.

On a alors

$$\begin{aligned}\sum_{(x,y)\in E^2} |\pi(x)(f(x)-f(y))f(x)P^n(x,y)| &\leqslant 2\|f\|_\infty^2 \sum_{y\in E}\pi(y)\\ &= 2\|f\|_\infty^2\\ &< +\infty\end{aligned}$$

Donc, la famille $(\pi(x)(f(x)-f(y))f(x)P^n(x,y))_{(x,y)\in E^2}$ est sommable, et on a

$$\begin{aligned}\langle f - P^n f, f\rangle_\pi &= \sum_{x\in E}\pi(x)\left(f(x)\sum_{y\in E}P^n(x,y) - \sum_{y\in E}P^n(x,y)f(y)\right)f(x) \qquad (*)\\ &= \sum_{(x,y)\in E^2}\pi(x)(f(x)-f(y))f(x)P^n(x,y)\end{aligned}$$

Et puisque P est réversible par rapport à π, alors

$$\begin{aligned}\sum_{(x,y)\in E^2}\pi(x)(f(x)-f(y))f(x)P^n(x,y) &= \sum_{(x,y)\in E^2}\pi(y)(f(y)-f(x))f(y)P^n(y,x)\\ &= \sum_{(x,y)\in E^2}\pi(x)(f(y)-f(x))f(y)P^n(x,y)\end{aligned}$$

Ainsi,

$$\begin{aligned}\sum_{(x,y)\in E^2}\pi(x)(f(x)-f(y))f(x)P^n(x,y) &= \frac{1}{2}\sum_{(x,y)\in E^2}\pi(x)(f(x)-f(y))f(x)P^n(x,y)\\ &\quad +\frac{1}{2}\sum_{(x,y)\in E^2}\pi(x)(f(y)-f(x))f(y)P^n(x,y)\\ &= \frac{1}{2}\sum_{(x,y)\in E^2}\pi(x)(f(x)^2 - 2f(y)f(x) + f(y)^2)P^n(x,y)\\ &= \frac{1}{2}\sum_{(x,y)\in E^2}\pi(x)(f(x)-f(y))^2P^n(x,y)\\ &= \mathcal{E}_n(f)\end{aligned}$$

(*b*) **Montrer que si $Pf = f$, la fonction est f est constante.**

Supposons que $Pf = f$, et montrons que $f$est constante.

Puisque $Pf = f$, alors par récurrence simple sur $k \in \mathbb{N}$, on a $P^k f = f$ pour tout $k \in \mathbb{N}$.

D'après la question précédente, pour tout $k \in \mathbb{N}$,

$$\begin{aligned}\mathcal{E}_k(f) &= \langle f - P^k f, f\rangle_\pi \\ &= 0\end{aligned}$$

Donc

$$\frac{1}{2}\sum_{(x,y)\in E^2} \pi(x)(f(x)-f(y))^2 P^k(x,y) = 0$$

Or, la somme est à termes positifs. En particulier, pour tout $(x,y) \in E^2$

$$\pi(x)(f(x)-f(y))^2 P^k(x,y) = 0$$

Puisqu'il existe un entier$n \geqslant 1$ pour lequel $P^n(a,x) > 0$ et $\pi(a) > 0$, alors en particulier pour $x = a$, et $k = n$, on obtient pour tout $y \in E$ que $(f(x)-f(y))^2 = 0$.

Ce qui montre que f est une fonction constante.

(c) Soit μ un élément de $\mathcal{P}(E)$ tel que $\mu P = \mu$. En posant $f(x) = \frac{\mu(x)}{\pi(x)}$, montrer que $Pf = f$, puis que $\mu = \pi$.

On a, pour tout $x \in E$

$$\begin{aligned}Pf(x) &= \sum_{y\in E} P(x,y) f(y) \\ &= \sum_{y\in E} P(x,y)\frac{\mu(y)}{\pi(y)} \\ &= \sum_{y\in E} P(y,x)\frac{\mu(y)}{\pi(x)} \\ &= \frac{1}{\pi(x)}\sum_{y\in E} P(y,x)\mu(y) \\ &= \frac{1}{\pi(x)}\mu P(x) \\ &= \frac{1}{\pi(x)}\mu(x) \\ &= f(x)\end{aligned}$$

On a donc $Pf = f$,

Supposons maintenant que $\frac{\mu}{\pi}$ est bornée. D'après la question précédente, f est donc constante. Posons pour tout $x \in E$, $f(x) = C^{\text{st}} \in \mathbb{R}$. On a alors :

$$\mu(x) = \pi(x) C^{\text{st}}$$

De plus, puisque

$$1 = \sum_{x\in E}\mu(x) = C^{\text{st}}\sum_{x\in E}\pi(x) = C^{\text{st}}$$

Ainsi, $C^{\text{st}} = 1$, d'où $f(x) = \frac{\mu(x)}{\pi(x)} = 1$, pour tout $x \in E$.
Par conséquent, $\mu(x) = \pi(x)$, pour tout $x \in E$, donc $\pi = \mu$.

À partir de maintenant, on supposera également qu'il existe un élément $b \in E$ tel que $P(b, b) > 0$.

1.7. (a) **Montrer que pour tous entiers positifs** k, l, n, **on a** $P^n(b, b) > 0$ **et**

$$P^{k+n+l}(x, y) \geq P^k(x, b)P^n(b, b)P^l(b, y) \,\text{pour tout}\, (x, y) \in E^2.$$

Montrons par récurrence sur $n \in \mathbb{N}$ que $P^n(b, b) > 0$.
Pour $n = 0$, on a $P^0(b, b) = 1 > 0$.
Soit $n \in \mathbb{N}$, supposons que $P^n(b, b) > 0$, et montrons que $P^{n+1}(b, b) > 0$.
On a, par positivité des termes :

$$\begin{aligned} P^{n+1}(b, b) &= P^n \times P(b, b) \\ &= \sum_{x\in E} P^n(b, x)P(x, b) \\ &\geqslant P^n(b, b)P(b, b) \\ &> 0 \end{aligned}$$

D'où le résultat par récurrence sur $n \in \mathbb{N}$.
Soient $k, l, n \in \mathbb{N}$, et $(x, y) \in E^2$. Montrons que $P^{k+n+l}(x, y) \geq P^k(x, b)P^n(b, b)P^l(b, y)$
On a :

$$\begin{aligned} P^{k+n+l}(x, y) &= \sum_{z\in E}\sum_{t\in E} P^k(x, t)P^n(t, z)P^l(z, y) \\ &\geqslant P^k(x, b)P^n(b, b)P^l(b, y) \end{aligned}$$

D'où le résultat.

(b) **Montrer que** P^2 **est irréductible. On rappelle (cf. la question** $5(a)$**) que** P^2 **est réversible par rapport à** π.

D'après la question 1.5.d. P est irréductible, donc il existe $n_1, n_2 > 0$ tels que $P^{n_1}(b,x) > 0$ et $P^{n_2}(b,y) > 0$.

De plus, $\pi(y), \pi(a) > 0$, donc, via la question précédente, on a

$$\begin{aligned}(P^2)^{n_1+n_2}(x,y) &= P^{n_1+(n_1+n_2)+n_2}(x,y)\\ &\geqslant P^{n_1}(x,b)P^{n_1+n_2}(b,b)P^{n_2}(b,y)\\ &= \frac{\pi(b)}{\pi(x)}P^{n_1}(b,x)P^{n_1+n_2}(b,b)P^{n_2}(b,y)\\ &> 0\end{aligned}$$

D'où le résultat.

(*c*)**Montrer que si une fonction bornée $f : E \to \mathbb{R}$ vérifie$Pf = f$, alors $f(x) = 0$ pour tout $x \in E$.**

Soit $f : E \to \mathbb{R}$ une fonction bornée telle que $Pf = -f$.

Par récurrence simple sur $n \in \mathbb{N}$, on obtient $P^n f = (-1)^n f$. En particulier, pour tout $n \in \mathbb{N}$,

$$P^{2n} f - f = 0$$

Ensuite, en utilisant le résultat de la question 1.6.a, on a pour tout $n \geqslant 1$ $\mathcal{E}_{2n}(f) = 0$.

Ainsi, pour tout $n \geqslant 1$, on a, pour tout $n \in \mathbb{N}$:

$$\frac{1}{2}\sum_{(x,y)\in E^2}[f(x)-f(y)]^2\pi(x)P^{2n}(x,y) = 0$$

Puisque, pour tout $(x,y) \in E^2$, on a

$$[f(x)-f(y)]^2\pi(x)P^{2n}(x,y) \geqslant 0$$

Cela implique que pour tout $(x,y) \in E^2$, on a $[f(x)-f(y)]^2\pi(x)P^{2n}(x,y) = 0$ (✠)

Soit $(x,y) \in E^2$, on a montré dans la question précédente que P^2 est irréductible. Donc, par définition de l'irréductibilité, il existe $n_{x,b}, n_{b,y} \geqslant 1$ tels que $P^{n_{x,b}}(x,b) > 0$ et $P^{n_{b,y}}(b,y) > 0$.

Or, il existe un entier $n \in \mathbb{N}$ tel que $n_{x,b} + n_{b,y} + n_b$ soit pair. Notons ce nombre par $2k$.

On obtient alors, en utilisant la question 1.7.a :

$$P^{2k}(x,y) \geqslant P^{n_{x,b}}(x,b)P^{n_b}(b,b)P^{n_{b,y}}(b,y)$$

Or, $P(b,b) > 0$, donc pour tout $n \in \mathbb{N}$, on a $P^n(b,b) \geqslant (P(b,b))^n > 0$. Par conséquent

$$P^{2k}(x,y) > 0$$

Ainsi, via (✠), on a $[f(x)-f(y)]^2\pi(x)P^{2k}(x,y) = 0$, avec $\pi(x), P^{2k}(x,y) > 0$.

Donc, $f(x) = f(y)$, ainsi f est constante.

Par ailleurs, pour tout $x \in E$, on a

$$\begin{aligned} f(x) &= -\sum_{x\in E} P(x,y)f(y) \\ &= -f(x)\sum_{x\in E} P(x,y) \\ &= -f(x) \end{aligned}$$

Ainsi $f(x) = 0$, et ça pour tout $x \in E$.

D'où le résultat.

1.8. Dans cette question, on prend $E = \{1, ..., d\}$, où $d$est un entier. Une fonction $f : E \to \mathbb{R}$ peut alors être vue comme un élément de $\mathbb{R}^d$.

(a) **Montrer que $\langle ., . \rangle_\pi$ définit un produit scalaire sur $\mathbb{R}^d$. On note $\|.\|_\pi$ la norme associée.**

On a pour tous $f, g, h \in \mathbb{R}^d$, et $\lambda \in \mathbb{R}$,

$$\begin{aligned} \langle f, g\rangle_\pi &= \pi[fg] \\ &= \sum_{x\in E} \pi(x)f(x)g(x) \\ &= \sum_{x\in E} \pi(x)g(x)f(x) \\ &= \langle g, f\rangle_\pi \end{aligned}$$

Donc $\langle ., . \rangle_\pi$ est symétrique.

Montrons que $\langle ., . \rangle_\pi$ est bilinéaire. On a

$$\begin{aligned} \langle f, g + \lambda h\rangle_\pi &= \pi[f(g + \lambda h)] \\ &= \sum_{x\in E} \pi(x)f(x)(g(x) + \lambda h(x)) \\ &= \sum_{x\in E} \pi(x)f(x)g(x) + \lambda\sum_{x\in E} \pi(x)f(x)h(x) \\ &= \langle f, g\rangle_\pi + \lambda\langle f, h\rangle_\pi \end{aligned}$$

Par symétrie, $\langle .,. \rangle_\pi$ est bilinéaire.

Il reste à montrer que $\langle .,. \rangle_\pi$ est défini, positif.

On a pour $f$non nul, il existe $x_0 \in E$ tel que $f(x_0) \not=0$. Donc

$$\begin{aligned}
\langle f, f \rangle_\pi &= \pi[f^2] \\
&= \sum_{x \in E} \pi(x) f^2(x) \\
&= \sum_{x \in E \setminus \{x_0\}} \pi(x) f^2(x) + \pi(x_0) f^2(x_0) \\
&> 0
\end{aligned}$$

Car $\pi(x_0) f^2(x_0) > 0$ et $\sum_{x \in E \setminus \{x_0\}} \pi(x) f^2(x) \geqslant 0$.

D'où le résultat.

(b) **Montrer que l'application $f \longmapsto Pf$ est un endomorphisme de $\mathbb{R}^d$ symétrique pour le produit scalaire $\langle .,. \rangle_\pi$.**

Soient $f, g \in \mathbb{R}^d$ et $\lambda \in \mathbb{R}$. Pour tout $x \in E$, on a :

$$\begin{aligned}
P(f + \lambda g)(x) &= \sum_{y \in E} P(x,y)(f(y) + \lambda g(y)) \\
&= \sum_{y \in E} P(x,y) f(y) + \lambda \sum_{y \in E} P(x,y) g(y) \\
&= Pf(x) + \lambda P g(x) \\
&= (Pf + \lambda P g)(x)
\end{aligned}$$

Comme cette égalité est vraie pour tout $x \in E$, on a donc

$$P(f + \lambda g) = Pf + \lambda P g$$

Ainsi, l'application $f \longmapsto Pf$ est un endomorphisme de $\mathbb{R}^d$.

Montrons maintenant qu'elle est symétrique pour le produit scalaire $\langle .,. \rangle_\pi$

Pour tous $f, g \in \mathbb{R}^d$, On a

$$\begin{aligned}
\langle Pf, g\rangle_\pi &= \pi[gPf] \\
&= \sum_{x\in E} \pi(x)g(x)Pf(x) \\
&= \sum_{x\in E} \pi(x)g(x) \sum_{y\in E} P(x,y)f(y) \\
&= \sum_{y\in E}\sum_{x\in E} \pi(x)P(x,y)g(x)f(y) \\
&= \sum_{y\in E}\sum_{x\in E} \pi(y)P(y,x)g(x)f(y) \\
&= \sum_{y\in E} f(y)\pi(y) \sum_{x\in E} P(y,x)g(x) \\
&= \sum_{y\in E} f(y)\pi(y)Pg(y) \\
&= \pi[fPg] \\
&= \langle f, Pg\rangle_\pi
\end{aligned}$$

D'où le résultat.

(*c*) **Montrer que si**$\lambda \in \mathbb{C}$ **est une valeur propre de** P**, alors** λ **est réelle et vérifie** $1 < \lambda \leqslant 1$**.**

Puisque $P \longmapsto Pf$ est symétrique pour le produit scalaire $\langle ., .\rangle_\pi$, alors P est une matrice réelle symétrique. D'après le théorème spectral, P est diagonalisable sur une base orthonormale de $\mathbb{R}^d$ pour le produit scalaire $\langle ., .\rangle_\pi$.

Ainsi, λ est réelle, il reste à vérifie que $1 < \lambda \leqslant 1$

Soit $e \in \mathbb{R}^d$ un vecteur propre de P associé à λ, alors $Pe = \lambda e$

Notons $P = (p_{i,j})_{1\leqslant i,j\leqslant d}$, et $e = (e_1, \ldots, e_d)^T$, on a alors pour tout $i \in [\![1, d]\!]$

$$\sum_{j=1}^{d} p_{i,j}e_j = \lambda e_j$$

Soit $i_0 \in [\![1, d]\!]$ qui vérifie $|e_{i_0}| = \max\limits_{1\leqslant i\leqslant d} |e_i|$. Puisque e est non nul, on a

$|e_{i_0}| > 0$. on obtient alors :

$$\begin{aligned} |\lambda| &= \frac{1}{|e_{i_0}|}\left|\sum_{j=1}^{d} p_{i,j}e_j\right| \\ &\leqslant \sum_{j=1}^{d} p_{i,j}\frac{|e_j|}{|e_{i_0}|} \\ &\leqslant \sum_{j=1}^{d} p_{i,j} \\ &= 1 \end{aligned}$$

D'après la question 1.7.c, $\lambda \neq 0$ (-1 n'est pas valeur propre de P, le seul vecteur f qui vérifie $Pf = -f$ est $f = 0$).

D'où

$$-1 < \lambda \leqslant 1$$

D'où le résultat.

(*d*) **On note b_1 le vecteur de $\mathbb{R}^d$ dont toutes les composantes valent 1. Montrer que b_1 est un vecteur propre de P associé à la valeur propre 1, qui est une valeur propre de multiplicité 1 pour P.**

On a

$$\begin{aligned} Pb_1 &= \begin{pmatrix} \sum_{y\in E} P(1,y) \\ . \\ . \\ . \\ \sum_{y\in E} P(d,y) \end{pmatrix} \\ &= b_1 \end{aligned}$$

Ainsi, $b_1$est un vecteur propre de P associée à 1. De plus, d'après la question 1.6.b, pour tout $f \in \mathbb{R}^d$ tel que $Pf = f$, $f$est constante, donc elle est proportionnelle à b_1.

D'où 1 est une valeur propre de multiplicité 1 pour P.

(e) **Montrer qu'il existe $\lambda \in [0,1[$ tel que pour tout $n \geqslant 1$ et pour toute fonction $f : E \to \mathbb{R}$, on a**

$$\|P^n f - \pi[f]b_1\|_\pi \leqslant \lambda^n \|f - \pi[f]b_1\|_\pi$$

Si f est une fonction constante, on a pour tout $n \in \mathbb{N}$,

$$P^n f - \pi[f]b_1 = 0$$

et

$$f - \pi[f]b_1 = 0$$

Donc tout $\lambda \in [0,1[$ convient.

Dans la suite, on suppose que f est non constante.

Montrons d'abord que b_1 est un vecteur normal pour la norme $\|.\|_\pi$. Pour cela, on a :

$$\begin{aligned}
\|b_1\|_\pi^2 &= \langle b_1, b_1 \rangle_\pi \\
&= \pi[b_1 b_1] \\
&= \sum_{x \in E} \pi(x) b_1(x) b_1(x) \\
&= \sum_{x \in E} \pi(x) \\
&= 1
\end{aligned}$$

Complétons b_1 en une base orthonormée de $\mathbb{R}^d$ pour le produit scalaire $\langle ., . \rangle_\pi$, notée $(b_1, \ldots, b_d)$ formée par les vecteurs propres de P.

Il existe donc des scalaires $x_1, \ldots, x_n \in \mathbb{R}$ tels que $f = \sum_{k=1}^{d} x_k b_k$.

Notons $\lambda_k \in \mathbb{R}$ la valeur propre associée à b_k ($\lambda_1 = 1$) pour tout $k \in [\![1, d]\!]$.

Soit $n \in \mathbb{N}$. On a :

$$\begin{aligned}
\|P^n f - \pi[f]b_1\|_\pi^2 &= \left\|\sum_{k=1}^d x_k P^n b_k - \pi[f]b_1\right\|_\pi^2 \\
&= \left\|\sum_{k=1}^d x_k \lambda_k^n b_k - \pi[f]b_1\right\|_\pi^2 \\
&= \left\|(x_1 - \pi[f])b_1 + \sum_{k=2}^d x_k \lambda_k^n b_k\right\|_\pi^2 \\
&= (x_1 - \pi[f])^2 + \sum_{k=2}^d x_k^2 {\lambda_k^2}^n
\end{aligned}$$

On définit la fonction

$$\gamma : \lambda \longmapsto \left((x_1 - \pi[f])^2 + \sum_{k=2}^d x_k^2\right)\lambda^{2n}$$

γ est une fonction strictement croissante sur $\mathbb{R}$ (car $(x_1-\pi[f])^2+\sum\limits_{k=2}^d x_k^2 > 0$, puisque f est non constante).

De plus, on a :

$$\gamma(1) - \|P^n f - \pi[f]b_1\|_\pi^2 = \sum_{k=2}^d x_k^2\left(1 - {\lambda_k^2}^n\right)$$

Puisque 1 est une valeur propre de multiplicité 1 de l'endomorphisme $f \longmapsto Pf$, alors, d'après la question 1.8.c, on a pour tout $2 \leqslant k \leqslant d$

$$-1 < \lambda_k < 1$$

Par conséquent,

$$\sum_{k=2}^d x_k^2\left(1 - {\lambda_k^2}^n\right) \geqslant \min_{2\leqslant k\leqslant d}\left(1 - {\lambda_k^2}^n\right)\sum_{k=2}^d x_k^2 > 0$$

car $f$est non constante.

Ainsi,

$$\gamma(1) > \|P^n f - \pi[f]b_1\|_\pi^2$$

Puisque γ est strictement croissante, et par caractérisation de la borne inférieure, il existe $\lambda \in [0, 1[$ tel que

$$\gamma(\lambda) \geqslant \|P^n f - \pi[f]b_1\|_\pi^2$$

Donc, pour ce $\lambda \in [0,1[$, on a

$$\left((x_1 - \pi[f])^2 + \sum_{k=2}^{d} x_k^2\right) \lambda^{2n} \quad \geqslant \quad \|P^n f - \pi[f] b_1\|_\pi^2$$

Avec

$$(x_1 - \pi[f])^2 + \sum_{k=2}^{d} x_k^2 \quad = \quad \|f - \pi[f] b_1\|_\pi^2$$

Ainsi

$$\lambda^{2n} \|f - \pi[f] b_1\|_\pi^2 \geqslant \|P^n f - \pi[f] b_1\|_\pi^2$$

D'où

$$\lambda^{n} \|f - \pi[f] b_1\|_\pi \geqslant \|P^n f - \pi[f] b_1\|_\pi$$

(f) **En déduire qu'il existe une constante C telle que**

$$\forall n \geqslant 1, \sup_{x \in E} |\mu_n(x) - \pi(x)| \leqslant C\lambda^n$$

Soit $n \in \mathbb{N}^\star$, et $x \in E$,
D'après la question précédente, pour

$$f_x : y \longmapsto \mathbf{1_{x=y}(y)} = \begin{cases} 1 \,\text{si}\, x = y \\ 0 \,\text{sinon} \end{cases}$$

On a

$$\lambda^{2n} \|f_x - \pi[f_x] b_1\|_\pi^2 \geqslant \|P^n f_x - \pi[f_x] b_1\|_\pi^2$$

Avec :

$$\begin{aligned} \pi[f_x] &= \sum_{y \in E} \pi(y) f_x(y) \\ &= \pi(x) \end{aligned}$$

Avec b_1 a toutes les composantes valent 1.
Ainsi

$$\lambda^{2n} \|f_x - \pi(x)\|_\pi^2 \geqslant \|P^n f_x - \pi(x)\|_\pi^2$$

De plus,

$$\begin{aligned}
\|f_x - \pi(x)\|_\pi^2 &= \langle f_x - \pi(x), f_x - \pi(x)\rangle_\pi \\
&= \pi[(f_x - \pi(x))^2] \\
&= \sum_{y\in E} \pi(y)(f_x - \pi(x))^2(y) \\
&= \sum_{y\in E} \pi(y)(f_x(y) - \pi(x))^2 \\
&= \sum_{y\in E} \pi(y)(f_x(y) - \pi(x))^2 \\
&= \sum_{\substack{y\in E \\ y\neq x}} (\pi(y))^3 + \pi(x)(1-\pi(x))^2 \\
&= \sum_{y\in E} (\pi(y))^3 + \pi(x) - 2(\pi(x))^2 \\
&\leqslant \sum_{y\in E} (\pi(y))^3 + 1
\end{aligned}$$

Posons

$$C^2 = \sum_{y\in E} (\pi(y))^3 + 1$$

Et

$$\begin{aligned}
\|P^n f_x - \pi(x)\|_\pi^2 &= \langle P^n f_x - \pi(x), P^n f_x - \pi(x)\rangle_\pi \\
&= \pi[(P^n f_x - \pi(x))^2] \\
&= \sum_{y\in E} \pi(y)(P^n f_x - \pi(x))^2(y) \\
&= \sum_{y\in E} \pi(y)(P^n f_x(y) - \pi(x))^2 \\
&= \sum_{y\in E} \pi(y) \left(\sum_{z\in E} P^n(y,z) f_x(z) - \pi(x)\right)^2 \\
&= \sum_{y\in E} \pi(y)(P^n(y,x) - \pi(x))^2 \\
&\geqslant \left(\sum_{y\in E} \mu_0(y) P^n(y,x) - \pi(x)\right)^2 \\
&= |\mu_n(x) - \pi(x)|^2
\end{aligned}$$

Ainsi,

$$|\mu_n(x) - \pi(x)|^2 \leqslant C^2\lambda^{2n}$$

Et cela pour tout $x \in E$, alors

$$\sup_{x\in E}|\mu_n(x) - \pi(x)| \leqslant C\lambda^n$$

Agrégation externe 2019

Corrigé par : SABIR ILYASS.

⋆ ⋆ ⋆

Le problème présenté ici est issu du sujet d'algèbre du concours de l'Agrégation externe 2019.

Ce problème est long : il est composé de cinq grandes parties, aboutissant finalement à une démonstration du théorème de Fermat-Wiles pour certains nombres premiers dits *réguliers*.

Le problème est un excellent sujet formateur pour les futurs candidats de l'agrégation en maths, et peut-être aussi intéressant pour les étudiants de CPGE scientifiques.

C'est un excellent sujet de formation pour les futurs candidats à l'agrégation de mathématiques et peut-être également intéressant pour les étudiants en classes préparatoires scientifiques.

La première partie consiste à démontrer quelques résultats sur la division euclidienne des polynômes à coefficients entiers et à montrer que l'anneau $\mathbb{Z}[\zeta]$ est euclidien pour $\zeta = \exp(2i\pi/3)$. Ensuite, on introduit la notion de polynôme cyclotomique, un résultat important concernant ces polynômes étant qu'ils ont des coefficients entiers et sont irréductibles sur $\mathbb{Q}[X]$. Cela nous fournit un excellent exemple pour montrer que, pour tout entier $n \in \mathbb{N}$, il existe un polynôme de $\mathbb{Q}[X]$ irréductible dans $\mathbb{Q}[X]$. Ce résultat n'est pas valable pour $\mathbb{R}[X]$ ni pour $\mathbb{C}[X]$. En particulier, $\mathbb{Q}$ n'est pas algébriquement clos.

D'autre part, les questions 4.a, 4.b, et 4.c servent à introduire les matrices compagnons, un outil souvent utilisé pour simplifier les démonstrations (comme celle du théorème de Cayley-Hamilton, par exemple !). Ici, la

présence des matrices compagnons permet de démontrer le résultat énoncé dans la question 4.e, qui sera utilisé à plusieurs reprises dans la suite du problème.

La deuxième partie porte sur les nombres algébriques. Un très bon résultat est présenté dans la question 1.b concernant la finitude des racines de l'unité incluses dans une extension finie de $\mathbb{Q}$, ce qui implique que le corps des nombres algébriques est de degré infini sur $\mathbb{Q}$. Vers la fin de cette partie, on montre que l'ensemble des nombres entiers algébriques est un sous-anneau de $\mathbb{C}$.

Passons ensuite à la troisième partie, qui consiste à étudier et caractériser quelques résultats sur$\mathbb{Z}[\zeta]$ (qui seront utilisés dans les parties 4 et 5), où $\zeta = \exp((2i\pi)/p)$, notamment en ce qui concerne les éléments inversibles de l'anneau $\mathbb{Z}[\zeta]$.

La partie 4 a pour but de démontrer le théorème de Fermat pour $n = 3$.

Enfin, la partie 5 traite du théorème de Fermat pour certains nombres premiers et dans des cas particuliers.

En conclusion, le théorème de Fermat (en anglais, *Fermat's Last Theorem*) a été énoncé (conjecturé) par le mathématicien français Pierre de Fermat en 1637, et il n'a été démontré qu'en 1994. Cette démonstration a été présentée pour la première fois par le mathématicien britannique Andrew Wiles. Elle repose sur plusieurs théories, comme la théorie de Galois, ainsi que sur des résultats de mathématiques modernes qui n'existaient pas au XVIIe siècle. Pour ceux qui souhaitent découvrir la démonstration de ce théorème, n'hésitez pas à cliquer sur le lien à la fin de ce document (la beauté du livre vous donnera envie de le lire en entier).

Bon courage pour la suite...

Définitions et rappels.

— Soit A un anneau commutatif unitaire intègre dont on note 1_A l'élément unité.

— On rappelle qu'un élément $u \in A$ est inversible s'il existe $u' \in A$tel que $uu' = 1_A$. On note $A^\times$ l'ensemble des inversibles de A, qui **est un groupe multiplicatif**.

— Un élément x de A est dit **irréductible** si x n'est pas inversible et si pour tous $\alpha, \beta \in A$, $x = \alpha\beta$ implique $\alpha \in A^\times$ ou $\beta \in A^\times$.

— Deux éléments $x, y \in A$ sont dits associés s'il existe $u \in A^\times$ tel que $x = uy$. On note alors $x \sim y$.

— Soit I un idéal de A ; on dit que deux éléments $\alpha, \beta \in A$ sont congrus modulo Isi $\alpha\beta \in I$. On écrit alors $\alpha = \beta (\mathrm{mod}\, I)$.

— Pour$x \in A$, on note$\langle x \rangle = xA$ l'idéal engendré par x. Un tel idéal est dit **principal**.

— Soient I, J deux idéaux de A. On dit que I divise J si $J \subseteq I$. Par ailleurs, on noteIJ l'idéal produit de I et J, qui est l'ensemble des sommes finies $\sum\limits_i x_i y_i$ avec $x_i \in I$ et $y_i \in J$.

— On rappelle qu'un nombre complexe α est dit algébrique (sur $\mathbb{Q}$) s'**il existe un polynôme non nul** P **de** $\mathbb{Q}[X]$ **tel que** $P(\alpha) = 0$.

Il existe alors un polynôme unitaire de plus petit degré annulant α, que l'on appelle **polynôme minimal de** α et que l'on note π_α. Les racines complexes de ce polynôme sont appelées les conjugués de α.

— On appelle **entier algébrique** tout nombre complexe qui est racine d'un polynôme unitaire à coefficients dans $\mathbb{Z}$.

— On rappelle une version du **lemme de Gauss**, que l'on pourra utiliser librement : soit $P \in \mathbb{Z}[X]$ tel que $P = P_1P_2$, avec P_1 et P_2 des polynômes de $\mathbb{Q}[X]$. Alors, il existe un rationnel $r \in \mathbb{Q}$, non nul, tel que $rP_1 \in \mathbb{Z}[X]$et $\frac{1}{r}P_2 \in \mathbb{Z}[X]$.

— On dit qu'un groupe abélien G est de **type fini** s'il existe une famille génératrice finie de G, c'est-à-dire un entier r et une famille $(a_1, ..., a_r)$ d'éléments de G tels que tout élément de G s'écrit comme une combinaison linéaire à coefficients entiers des $a_1, ..., a_r$.

Notations.

— Pour un anneau A commutatif et un entier naturel non nul n, on note $\mathcal{M}_n(A)$ l'algèbre des matrices carrées $n \times n$ à coefficients dans A ; la matrice unité est notée I_n.

Si M est une matrice de $\mathcal{M}_n(A)$, on note χ_M son **polynôme caractéristique**, qui est le polynôme unitaire défini par

$$\chi_M = \det(XI_nM)$$

et on note π_M son **polynôme minimal**.

— Pour un nombre premier p, on note $\mathbb{F}_p$ le corps $\mathbb{Z}/p\mathbb{Z}$.

— Pour tout entier algébrique α, on note $\mathbb{Z}[\alpha]$ l'anneau des éléments de la forme $P(\alpha)$ où P parcourt $\mathbb{Z}[X]$.

Dans le problème, les textes placés entre les symboles ✠✠...✠✠ précisent des notations et définitions qui sont utilisées dans la suite de l'énoncé.

I. Exercices préliminaires

1. Soit $B \in \mathbb{Z}[X]$ un polynôme unitaire et $A \in \mathbb{Z}[X]$. Montrer qu'il existe $Q, R \in \mathbb{Z}[X]$ tels que $A = \mathrm{BQ} + R$ avec $\deg R < \deg B$ ou $R = 0$.

Indication : On pourra faire une preuve par récurrence sur le degré de A.

2. L'anneau $\mathbb{Z}[j]$. On note $j = e^{\frac{2i\pi}{3}}$.

(a) Démontrer que j est un élément algébrique sur $\mathbb{Q}$ et préciser son polynôme minimal.

(b) Démontrer que $\mathbb{Z}[j] = \{a + bj, (a, b) \in \mathbb{Z}^2\}$.

Pour tout nombre complexe z, on pose $N(z) = z\bar{z} = |z|^2$.

(c) Démontrer que pour tout $z \in \mathbb{Z}[j]$, on a $N(z) \in \mathbb{N}$. En déduire que si $z \in \mathbb{Z}[j]$ est inversible, alors $N(z) = 1$, puis que $\mathbb{Z}[j]^\times$ possède 6 éléments que l'on précisera.

(d) Soient $x \in \mathbb{Z}[j]$ et $y \in \mathbb{Z}[j]\backslash\{0\}$. Déterminer un élément$q \in \mathbb{Z}[j]$ tel que $N\left(\frac{x}{y} - q\right) < 1$.

En déduire que l'anneau $\mathbb{Z}[j]$ est euclidien.

3. Polynômes cyclotomiques. Soit n un entier naturel non nul. On note Φ_n le $n - i$ème polynôme cyclotomique. On rappelle que si μ_n^* désigne l'ensemble des racines primitives $n - i$èmes de l'unité dans $\mathbb{C}$, ce polynôme est défini par

$$\Phi_n(X) = \prod_{\mu \in \mu_n^*} (X - \mu)$$

(a) Démontrer que

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

(b) En déduire que $\Phi_n(X) \in \mathbb{Z}[X]$.

(c) Soit p un nombre premier.

On note $\pi : \mathbb{Z} \to \mathbb{F}_p$ la surjection canonique. Le morphisme d'anneaux π s'étend, coefficient par coefficient, en un morphisme d'anneaux de $\mathbb{Z}[X]$ sur $\mathbb{F}_p[X]$, noté $\hat{}\pi$ (on ne demande pas de justifier ce point). Si Φ_p désigne le $p-i$ème polynôme cyclotomique, on rappelle que

$$\Phi_p = \sum_{k=0}^{p-1} X^k$$

i. Démontrer que $\hat{\pi}(X^p 1) = (X 1_{\mathbb{F}_p})^p$.

ii. Soient$P$ et Q deux polynômes unitaires et non constants dans $\mathbb{Z}[X]$ tels que $X^p - 1 = PQ$. Démontrer que $P(1)$ et $Q(1)$ sont des entiers multiples de p.

iii. Retrouver ainsi que Φ_p est un polynôme irréductible de $\mathbb{Q}[X]$.

✠✠ De manière générale, Φ_n est irréductible pour tout $n \in \mathbb{N}\backslash\{0\}$, résultat que l'on admet ici et que l'on pourra utiliser librement dans la suite. ✠✠

iv. Soit $\zeta = e^{\frac{2i\pi}{p}}$. Déterminer le polynôme minimal de ζ sur $\mathbb{Q}$ et en déduire le degré de l'extension de corps $\mathbb{Q}(\zeta)/\mathbb{Q}$.

4. Matrices compagnons. Soit n un entier naturel non nul. Soit $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ un polynôme unitaire de $\mathbb{C}[X]$. On lui associe sa

matrice compagnon C_P définie dans$\mathcal{M}_n(\mathbb{C})$ par

$$C_P = \begin{pmatrix} 0 & 0 & . & . & 0 & -a_0 \\ 1 & 0 & & & 0 & -a_1 \\ 0 & 1 & & & . & . \\ . & 0 & & & . & . \\ . & . & & & . & . \\ . & . & . & . & 0 & -a_{n-2} \\ 0 & 0 & 0 & 0 & 1 & -a_{n-1} \end{pmatrix}$$

On note $\mathcal{E} = (e_1, ..., e_n)$ la base canonique de $\mathbb{C}^n$.

(a) Pour $k \in \{1, ..., n1\}$, exprimer $C_P^k e_1$ dans la base $\mathcal{E}$. En déduire que pour tout polynôme $Q \in \mathbb{C}[X]$ non nul et de degré inférieur ou égal à $n1$, la matrice $Q(C_P)$ est non nulle.

En déduire le degré du polynôme minimal de C_P.

(b) Exprimer $C_p^n e_1$ dans la base $\mathcal{E}$. En déduire que P est le polynôme minimal de C_P .

(c) En déduire le polynôme χ_{C_P} .

Soit $M \in \mathcal{M}_n(\mathbb{C})$ de polynôme caractéristique χ_M . Soient $\alpha_1, ..., \alpha_n$ les racines complexes de χ_M comptées avec leur multiplicité. Soit Q un polynôme de $\mathbb{C}[X]$.

(d) Démontrer que le polynôme caractéristique de la matrice $Q(M)$ est

$$\chi_{Q(M)} = \prod_{k=1}^{n} (X - Q(\alpha_k))$$

Indication : On pourra commencer par traiter le cas où M est triangulaire.

(e) Soit A un sous-anneau de $\mathbb{C}$. On suppose que le polynôme Q est dans $A[X]$. Soit $P \in A[X]$ un polynôme unitaire dont on note $\alpha_1, ..., \alpha_n$ les racines complexes comptées avec leur multiplicité.

Démontrer que $\prod_{k=1}^{n} (X - Q(\alpha_k))$ est un polynôme de $A[X]$.

II. Nombres algébriques.

1. (a) On désigne parφ l'indicatrice d'Euler, qui à tout entier $n \in \mathbb{N}\backslash\{0\}$ associe le nombre d'entiers non nuls inférieurs à n et premiers avec$n$. Justifier que pour tout entier$d \geqslant 1$, l'ensemble des entiers n tels que $\varphi(n) \leqslant d$ est fini.

(b) En déduire que si $\boldsymbol{K}/\mathbb{Q}$ est une extension finie de $\mathbb{Q}$, où $\boldsymbol{K}$ est un sous-corps de $\mathbb{C}$, alors $\boldsymbol{K}$ contient un nombre fini de racines de l'unité.

2. Soit $\alpha \in \mathbb{C}$ un nombre algébrique dont on rappelle que l'on a noté π_α son polynôme minimal. On note $\boldsymbol{K} = \mathbb{Q}(\alpha)$ le plus petit corps contenant α et $\mathbb{Q}$, et $d = [\boldsymbol{K} : \mathbb{Q}]$, le degré de l'extension de corps $\mathbb{Q}(\alpha)/\mathbb{Q}$.

(a) Montrer que π_α est un polynôme irréductible de $\mathbb{Q}[X]$ et que son degré est égal à d.

(b) Montrer que si σ est un morphisme de $\mathbb{Q} - \text{alg è bre de } \boldsymbol{K}$ dans $\mathbb{C}$, $\sigma(\alpha)$ est une racine de π_α, c'est-à-dire un conjugué de α. En déduire qu'il y a exactement d tels morphismes de $\mathbb{Q}$-alg è bre, que l'on notera $\sigma_k : \boldsymbol{K} \to \mathbb{C}, k \in \{1, ..., d\}$.

3. Soit $\alpha \in \mathbb{C}$ un nombre algébrique et soit $\theta \in \boldsymbol{K} = \mathbb{Q}(\alpha)$. Comme dans la question précédente, les σ_k avec $k \in \{1, ..., d\}$ désignent les morphismes de $\mathbb{Q} - \text{alg è bre de } \mathbb{Q}(\alpha)$.

(a) Justifier que θ est un nombre algébrique.

On pose

$$P_\theta = \prod_{k=1}^{d} (X\sigma_k(\theta)) \in \mathbb{C}[X].$$

(b) Montrer que $P_\theta \in \mathbb{Q}[X]$.

(c) Justifier que π_θ divise P_θ, puis montrer que P_θ est une puissance de π_θ.

4. Montrer qu'un nombre algébrique α est un entier algébrique si et seulement si son polynôme minimal est à coefficients entiers.

5. Soit α un nombre complexe.

(a) Montrer que si α est un entier algébrique, alors le groupe additif G engendré par la partie $\{\alpha^n | n \in N\}$ est de type fini.

(b) Réciproquement, montrer que si G est de type fini alors α est un entier algébrique.

Indication : En notant $(g_1, ..., g_n)$ une famille génératrice finie de G, on pourra considérer le déterminant du système obtenu en écrivant les éléments αg_i, $i \in \{1, ..., n\}$ comme combinaison linéaire des g_j .

6. En déduire que l'ensemble $\mathfrak{D}_\mathbb{C}$ des entiers algébriques de $\mathbb{C}$ est un sous-anneau de $\mathbb{C}$.

Indication : On pourra utiliser sans démonstration qu'un sous-groupe d'un groupe abélien de type fini est de type fini.

7. Montrer que $\mathfrak{D}_\mathbb{C} \cap \mathbb{Q} = \mathbb{Z}$.

✠✠ Dans la suite, on considère le corps $\boldsymbol{K} = \mathbb{Q}(\zeta)$, où $\zeta = e^{\frac{2i\pi}{p}}$ avec p premier impair. On note $\mathfrak{D}_{\boldsymbol{K}}$ l'ensemble des entiers algébriques de $\boldsymbol{K}$. On pose $\lambda = 1\zeta$.

On définit la norme et la trace de tout élément $\theta \in \boldsymbol{K} = \mathbb{Q}(\zeta)$ par

$$N(\theta) = \prod_{k=1}^{p-1} \sigma_k(\theta)$$

et

$$\mathrm{Tr}(\theta) = \sum_{k=1}^{p-1} \sigma_k(\theta)$$

où les σ_k sont les morphismes de $\mathbb{Q} - \mathrm{alg\,\grave{e}\,brede}\ \mathbb{Q}(\zeta)$ définis dans la question 2 de cette partie.✠✠

III. Le corps $\mathbb{Q}(\zeta)$ et son anneau d'entiers

1. (a) Montrer que les morphismes de $\mathbb{Q} - \mathrm{alg\,\grave{e}\,bre}$ de $\mathbb{Q}(\zeta)$ sont les σ_k tels que $\sigma_k(\zeta) = \zeta^k$, avec $k \in \{1, ..., p1\}$.

(b) i. Montrer que $N(\zeta) = 1$et $\mathrm{Tr}(\zeta) = 1$.

ii. Montrer que $N(1\zeta) = p$ et $N(1 + \zeta) = 1$.

2. Montrer l'inclusion $\mathbb{Z}[\zeta] \subseteq \mathfrak{D}_{\boldsymbol{K}}$.

3. Soit $z \in \mathbb{Z}[\zeta]$.

(a) Montrer que $z \in Z[\zeta]^\times$ si et seulement si $N(z) \in \{1, +1\}$.

(b) Montrer que si $N(z)$ est un nombre premier, alors z est irréductible.

4. Le but de cette question est de montrer que l'ensemble G des racines de l'unité contenues dans$\boldsymbol{K}$ est formé exactement des éléments de la forme $\pm\zeta^k$, $k \in \{0, ..., p1\}$.

(a) Justifier que G est un groupe fini cyclique, dont on notera n le cardinal.

(b) Soit ω un générateur de G. Justifier que $2p|n$et que $\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)$.

(c) En déduire que $n = 2p$ et conclure.

5. On note $\langle\lambda\rangle = \lambda\mathbb{Z}[\zeta]$, l'idéal de $\mathbb{Z}[\zeta]$ engendré parλ.

(a) Montrer que $\langle\lambda\rangle \cap \mathbb{Z} = p\mathbb{Z}$.

(b) Montrer que pour tout $k \in \{1, ..., p1\}$, on a

$$\frac{1\zeta}{1-\zeta^k} \in Z[\zeta]^\times$$

et en déduire que

$$\lambda^{p-1}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta].$$

(c) Soit ψ le morphisme d'anneaux de $\mathbb{Z}[X]$ dans $\mathbb{Z}[\zeta]/\langle\lambda\rangle$, qui à $P \in \mathbb{Z}[X]$ associe $P(\zeta)(\mathrm{mod}\langle\lambda\rangle)$. Déterminer l'image de ψ et montrer que $\ker\psi$ est l'ensemble des polynômes $P \in \mathbb{Z}[X]$ tels que $P(1) = 0(\mathrm{mod}\, p\mathbb{Z})$.

(d) En déduire que $Z[\zeta]/\langle\lambda\rangle$ est isomorphe à $\mathbb{F}_p$.

(e) Que peut-on en déduire pour l'idéal λ ?

6. On détermine ici la structure de $\mathbb{Z}[\zeta]^\times$. Le but est de démontrer que les éléments de $\mathbb{Z}[\zeta]^\times$ sont les $\zeta^r\varepsilon$, où $r \in \mathbb{Z}$ et ε est un réel inversible de $\mathbb{Z}[\zeta]$.

Soit $u \in \mathbb{Z}[\zeta]^\times$.

(a) Soit $P = \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X]$ un polynôme unitaire de degré d, dont on note $\alpha_1, ..., \alpha_d$ les racines complexes comptées avec leur multiplicité. On suppose que, pour tout$k \in \{1, ..., d\}$, α_k est de module 1.

i. Montrer que pour tout $k \in \{0, ..., d\}$, on a $|a_k| \leqslant \begin{pmatrix} d \\ k \end{pmatrix}$.

En déduire qu'il n'existe qu'un nombre fini d'entiers algébriques de degré d dont tous les conjugués sont de module 1.

ii. En déduire également que les racines de P sont des racines de l'unité.

Indication : On pourra considérer les polynômes $P_n = \prod_{k=1}^{d} (X - \alpha_k^n)$, $n \in \mathbb{N}$, dont on montrera qu'ils sont dans $\mathbb{Z}[X]$.

(b) Soit $P \in \mathbb{Z}[X]$ tel que $u = P(\zeta)$. Montrer que, pour tout $k \in \{1, ..., p1\}$, $u_k = P(\zeta^k)$ est un conjugué de u, et que c'est un élément de $\mathbb{Z}[\zeta]^\times$.

(c) Justifier que $\frac{u_p}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.

(d) En déduire qu'il existe$m \in \mathbb{Z}$ tel que $\frac{u_1}{u_{p-1}} = \pm\zeta^m$.

(e) i. Soit $\theta \in \mathbb{Z}[\zeta]$. Justifier qu'il existe un entier $a \in \mathbb{Z}$ tel que $\theta = a(\mathrm{mod} < \lambda >)$. En déduire que deux éléments conjugués de $\mathbb{Z}[\zeta]$ sont égaux modulo $< \lambda >$.

ii. Démontrer que $\frac{u_1}{u_{p-1}} = \zeta^m$.

(f) Justifier l'existence de $r \in \mathbb{Z}$ tel que $2r = m(\mathrm{mod}\, p\mathbb{Z})$. On pose $\varepsilon = \zeta^{-r}u$. Montrer que $\varepsilon \in \mathbb{R}$ et conclure.

7. Le but de ce qui suit est de montrer que $\mathfrak{D}_{\boldsymbol{K}} = \mathbb{Z}[\zeta]$.

(a) Montrer que pour tout $\theta \in \mathfrak{D}_{\boldsymbol{K}}$, on a $N(\theta) \in \mathbb{Z}$ et $\mathrm{Tr}(\theta) \in \mathbb{Z}$.

(b) Soit $\theta \in \boldsymbol{K} = \mathbb{Q}(\zeta)$ un entier algébrique. Il existe des rationnels

$a_0, ..., a_{p-2}$ tels que

$$\theta = \sum_{k=0}^{p-2} a_k \zeta^k$$

i. Pour $k \in \{0, ..., p2\}$, calculer $b_k = \mathrm{Tr}(\theta\zeta^{-k}\theta\zeta)$ et justifier que $b_k \in \mathbb{Z}$.

ii. Montrer qu'il existe des entiers $c_0, c_1, ..., c_{p-2}$, que l'on exprimera en fonction des b_k, tels que

$$p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$$

Justifier ensuite que pour tout$k \in \{0, ..., p2\}$,

$$b_k = \sum_{l=k}^{p-2} (-1)^l \begin{pmatrix} l \\ k \end{pmatrix} c_l$$

iii. Montrer qu'il existe $\beta \in \mathbb{Z}[\zeta]$ tel que $p = \lambda^{p-1}\beta$. En déduire que$p|c_0$, puis que pour tout $k \in \{0, ..., p2\}$, on a $p|c_k$. Conclure.

IV. Le théorème de Fermat pour $p = 3$

On cherche à démontrer dans cette partie que l'équation

$$x^3 + y^3 + z^3 = 0 \tag{5}$$

n'a pas de solution entières non triviales, *i.e.*, telles que $xyz \neq 0$.

Soient x, y et z trois entiers relatifs tels que $x^3 + y^3 + z^3 = 0$.

1. On suppose que $3 \not| xyz$. Montrer que x^3 vaut $+1$ ou $1 (\mathrm{mod}\, 9)$ et conclure à une impossibilité.

✠✠ On traite à présent le cas $3|xyz$. Dans la suite de cette partie, on note $\lambda = 1j$ avec toujours $j = e^{\frac{2i\pi}{3}}$, et on suppose que les entiers x, y et z

sont premiers entre eux dans $\mathbb{Z}[j]$ (et non seulement dans $\mathbb{Z}$), cas auquel on peut se ramener en divisant par leur pgcd dans $\mathbb{Z}[j]$. ✠✠

2. Montrer que 3 et λ^2 sont associés dans $\mathbb{Z}[j]$, ce que l'on a noté $3 \sim \lambda^2$.

3. Soit $s \in \mathbb{Z}[j]$ tel que $s \neq 0(\mathrm{mod}\langle\lambda\rangle)$. Montrer qu'il existe $\varepsilon \in \{1, +1\}$ tel que $s^3 = \varepsilon(\mathrm{mod}\langle\lambda^4\rangle)$.

Indication : On pourra remarquer que tout élément $s \in \mathbb{Z}[j]$ est congru à $1, 0$ou $1(\mathrm{mod}\langle\lambda\rangle)$.

✠✠ Par symétrie des rôles de x, y et z, on peut supposer que $3|z$ (et donc 3 $\not|x$, 3 $\not|y$ puisqu'ils sont premiers entre eux). En particulier, on a $\lambda|z$, λ $\not|x$ etλ $\not|y$ dans $\mathbb{Z}[j]$.

On note n la valuation en λ de z ; il existe donc $\mu \in \mathbb{Z}[j]$ premier avec λ tel que $z = \mu\lambda^n$, et par hypothèse $n \geqslant 1$. On a donc $x^3 + y^3 + \mu^3\lambda^{3n} = 0$.

La propriété suivante (qui pourra être utilisée sans plus de justification) est donc vérifiée :

$$(P_n) : \text{il existe}\, \alpha, \beta, \delta \in \mathbb{Z}[j]\, \text{et}\, \omega \in \mathbb{Z}[j]^\times\, \text{tels que} \begin{cases} \lambda \not| \alpha\beta\delta \\ \alpha \text{ and } \beta \text{ premiers entre eux} \\ \alpha^3 + \beta^3 + \omega\lambda^{3n}\delta^3 = 0 \end{cases}$$

Nous allons montrer que si (P_n) est vérifiée, alors $n \geqslant 2$ et (P_{n-1}) est également vérifiée. ✠✠

4. Supposons (P_n) vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$. En considérant les valeurs de α^3, β^3 et $\omega\lambda^{3n}\delta^3(\mathrm{mod}\langle\lambda^4\rangle)$, montrer que $n \geqslant 2$.

5. Supposons (P_n)vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$. On montre dans cette question que (P_{n-1}) est également vérifiée.

(a) Montrer que

$$\omega\lambda^{3n}\delta^3 = (\alpha + \beta)(\alpha + j\beta)(\alpha + j^2\beta).$$

(b) En déduire que λ divise chacun des facteurs $\alpha+\beta, \alpha+j\beta$ et $\alpha+j^2\beta$.

(c) Démontrer que λ est un **pgcd** de $\alpha+\beta$et $\alpha+j\beta$. En déduire que λ^2 divise exactement l'un des éléments $\alpha+\beta, \alpha+j\beta$ ou$\alpha+j^2\beta$.

Quitte à remplacerβ par $j\beta$ ou$j^2\beta$, on peut supposer que λ^2 divise $\alpha+\beta$. Il existe donc des éléments κ_1, κ_2 et κ_3 de $\mathbb{Z}[j]$ tels que $\lambda \nmid \kappa_1\kappa_2\kappa_3$ et

$$\begin{cases} \alpha+\beta = \lambda^{3n-2}\kappa_1 \\ \alpha+j\beta = \lambda\kappa_2 \\ \alpha+j^2\beta = \lambda\kappa_3 \end{cases}$$

(d) Montrer que $\omega\delta^3 = \kappa_1\kappa_2\kappa_3$ et en déduire qu'il existe des éléments γ_1, γ_2 et γ_3 de $\mathbb{Z}[j]$ tels que pour tout $l \in \{1,2,3\}$, $\kappa_l \sim \gamma_l^3$.

(e) Démontrer qu'il existe deux inversibles τ et τ' de $\mathbb{Z}[j]^\times$ tels que

$$\gamma_2^3 + \tau\gamma_3^3 + \tau'\lambda^{3(n-1)}\gamma_1^3 = 0.$$

(f) Montrer que si $\tau = \pm 1$, alors (P_{n-1}) est vérifiée.

(g) Montrer que $\tau = \pm 1 (\mathrm{mod}\langle\lambda^3\rangle)$, puis que $\tau \notin \{j, j, j^2, j^2\}$.

6. Conclure que l'équation (1) n'a pas de solution(x,y,z) dans le cas $3|xyz$.

V. Le théorème de Fermat pour p régulier et $p \nmid xyz$

✠✠ On admet dans la suite que pour tout corps $\boldsymbol{K}$ de degré fini sur $\mathbb{Q}$, son anneau des entiers $\mathfrak{D}_{\boldsymbol{K}}$ vérifie la propriété suivante :

Tout idéal non nul de $\mathfrak{D}_{\boldsymbol{K}}$ s'écrit comme produit d'idéaux premiers, de manière unique à l'ordre près des facteurs.

Dans ce contexte, on dit que deux idéaux I et J sont premiers entre eux s'ils n'ont pas d'idéal premier en commun dans leur décomposition en produit d'idéaux premiers.

L'anneau $\mathbb{Z}[\zeta]$ qui est, d'après les résultats de la Partie 3, l'anneau des entiers de $\boldsymbol{K} = \mathbb{Q}(\zeta)$, vérifie donc cette propriété de factorisation de ses idéaux.

On suppose dans cette partie que $p > 3$ est un nombre premier régulier, ce qui signifie que si I est un idéal de $\mathbb{Z}[\zeta]$ tel que I^p est principal, alors I est lui-même principal. On rappelle que l'on a noté$\lambda = 1\zeta$ et que certaines propriétés de l'idéal $\langle\lambda\rangle$ ont été étudiées en Partie 3, question 5.

On démontre dans cette partie que l'équation

$$x^p + y^p + z^p = 0 \tag{6}$$

n'admet pas de solutions entières non triviales dans le cas où $p \not| xyz$.

Par l'absurde, on se donne trois entiers $x, y, z \in \mathbb{Z}$, deux à deux premiers entre eux dans $\mathbb{Z}$, tels que $p \not| xyz$ et qui vérifient l'équation (2). ✠✠

1. Montrer l'égalité d'idéaux

$$\prod_{k=0}^{p-1} \langle x + \zeta^k y\rangle = \langle z^p\rangle$$

2. Soient deux entiers k et l tels que $0 \leqslant k < l \leqslant p-1$. On montre dans cette question que les idéaux $\langle x+\zeta^k y\rangle$ et $\langle x+\zeta^l y\rangle$ de $\mathbb{Z}[\zeta]$ sont premiers entre eux. Par l'absurde, soit $\mathfrak{B}$ un idéal premier divisant $\langle x + \zeta^k y\rangle$ et $\langle x + \zeta^l y\rangle$.

(a) En considérant $\langle x + \zeta^l y\rangle - \langle x + \zeta^k y\rangle$, montrer que $\lambda y \in \mathfrak{B}$.

(b) Montrer que $y \notin \mathfrak{B}$, en déduire que $x + y \in \langle\lambda\rangle \cap \mathbb{Z}$ et conclure à une absurdité.

3. Justifier l'existence d'un idéal I tel que $\langle x + \zeta y\rangle = I^p$.

4. Montrer qu'il existe $r \in \mathbb{Z}$, ε réel inversible de $\mathbb{Z}[\zeta]$ et $\alpha \in \mathbb{Z}[\zeta]$ tels que $x + \zeta y = \zeta^r \varepsilon \alpha^p$.

5. Montrer qu'il existe $a \in \mathbb{Z}$ tel que $\alpha^p = a(\mathrm{mod}\langle p\rangle)$ (attention, ici $\langle p\rangle = p\mathbb{Z}[\zeta]$ et non $p\mathbb{Z}$) et en déduire que

$$x\zeta^{-r} + y\zeta^{1-r} x\zeta^r y\zeta^{r1} = 0(\mathrm{mod}\langle p\rangle).$$

6. Supposons que$r = 0(\mathrm{mod}\, p\mathbb{Z})$. Montrer alors que $p|y$ dans $\mathbb{Z}$, ce qui est contraire à l'hypothèse.

On montrerait de même que l'on ne peut avoir $r = 1(\mathrm{mod}\, p\mathbb{Z})$, ce que l'on admet.

7. D'après la question 5, il existe $\beta \in \mathbb{Z}[\zeta]$ tel que

$$x\zeta^r + y\zeta^{1r} x\zeta^r y\zeta^{r1} = \beta p.$$

Montrer que deux des entiers $\pm r, \pm(1r)$ sont égaux modulo p ; en déduire que $2r = 1(\mathrm{mod}\, p\mathbb{Z})$.

8. Montrer que $\beta p\zeta^r = (xy)\lambda$, puis que $x = y(\mathrm{mod}\, p\mathbb{Z})$.

9. Conclure à une absurdité.6. Supposons que$r = 0(\mathrm{mod}\, p\mathbb{Z})$. Montrer alors que $p|y$ dans $\mathbb{Z}$, ce qui est contraire à l'hypothèse.

On montrerait de même que l'on ne peut avoir $r = 1(\mathrm{mod}\, p\mathbb{Z})$, ce que l'on admet.

7. D'après la question 5, il existe $\beta \in \mathbb{Z}[\zeta]$ tel que

$$x\zeta^r + y\zeta^{1r} x\zeta^r y\zeta^{r1} = \beta p.$$

Montrer que deux des entiers $\pm r, \pm(1r)$ sont égaux modulo p ; en déduire que $2r = 1(\mathrm{mod}\, p\mathbb{Z})$.

8. Montrer que $\beta p\zeta^r = (xy)\lambda$, puis que $x = y(\mathrm{mod}\, p\mathbb{Z})$.

9. Conclure à une absurdité.

Solution

1. Exercices préliminaires

1. Soit $B \in \mathbb{Z}[X]$ un polynôme unitaire, et $A \in \mathbb{Z}[X]$.

Montrons par récurrence sur $n = \deg(A)$ que :

$$\exists Q, R \in \mathbb{Z}[X] \text{ tels que } \begin{cases} A = B.Q + R \\ \deg(R) < \deg(B) \text{ ou } R = 0 \end{cases}$$

Remarquons tout d'abord que si $\deg(B) = 0$, alors $B = 1$, donc le résultat est trivial puisque pour tout $A \in \mathbb{Z}[X]$, on a : $A = B \times A$.

On suppose dans la suite que $\deg(B) \geqslant 1$.

Pour $n = 0$, on a pour tout $A \in \mathbb{Z}[X]$, tel que $\deg(A) = 0$. On a

$$A = 0 \times B + A$$

Avec,

$$\deg(A) = 0 < \deg(B)$$

Donc, le résultat est vrai pour $n = 0$.

Soit $n \in \mathbb{N}$, supposons que le résultat est vrai pour $k = 0, 1, \ldots, n$, et montrons le pour $n + 1$.

Soit $A \in \mathbb{Z}[X]$, tel que $\deg(A) = n + 1$. On peut écrire A comme :

$$A = XA_1 + a_0$$

Avec,

$$\begin{cases} A_1 \in \mathbb{Z}[X] \\ a_0 = A(0) \in \mathbb{Z}[X] \end{cases}$$

On tire $\deg(A_1) = n$, donc, d'après l'hypothèse de récurrence, il existe $Q_1, R_1 \in \mathbb{Z}[X]$ tels que :

$$\begin{cases} A_1 = BQ_1 + R_1 \\ \deg(R_1) < \deg(B) \end{cases}$$

On a alors :

$$A = B(XQ_1) + XR_1 + a_0 \tag{7}$$

Or :

$$\deg(XR_1) = 1 + \deg(R_1) \leqslant \deg(B) \tag{8}$$

Si $\deg(B) \geqslant \deg(A)$ **:**

$\rightarrow$**Si** $\deg(B) > \deg(A)$ **:**

On a

$$A = 0 \times B + A$$

Donc le résultat est vrai.

$\rightarrow$ **Si** $\deg(B) = \deg(A)$ **:**

On note

$$A = \sum_{k=0}^{n+1} a_k X^k$$

et

$$B = X^{n+1} + \sum_{k=0}^{n} b_k X^k$$

avec $a_0, \ldots, a_{n+1}, b_0, \ldots, b_n \in \mathbb{Z}$

On a

$$A - a_{n+1}B = \sum_{k=0}^{n} (a_k - a_{n+1}b_k)X^k$$

Donc

$$A = a_{n+1}B + \sum_{k=0}^{n} (a_k - a_{n+1}b_k)X^k$$

avec

$$\deg\left(\sum_{k=0}^{n} (a_k - a_{n+1}b_k)X^k\right) < n+1$$

Donc par l'unicité de la division euclidienne, on a le résultat, puisque :

$$\begin{cases} a_{n+1} \in \mathbb{Z}[X] \\ \sum\limits_{k=0}^{n} (a_k - a_{n+1}b_k)X^k \in \mathbb{Z}[X] \end{cases}$$

On suppose dans le suite que $\deg(B) < \deg(A)$.

D'après (2), on a :

$$\begin{aligned} \deg(XR_1) &\leqslant \deg(B) \\ &< \deg(A) \\ &= n+1 \end{aligned}$$

Donc $\deg(XR_1) \leqslant n$.

Si $R_1 = 0$, alors d'après (1), on a :

$$A = B(XQ_1) + a_0$$

Avec $XQ_1 \in \mathbb{Z}[X]$, et $a_0 \in \mathbb{Z}[X]$. C'est fini !

Sinon ($R_1 \neq 0$), on a :

$$\deg(XR_1) \in [\![0, n]\!]$$

Par hypothèse de récurrence, on a l'existence de $Q_2, R_2 \in \mathbb{Z}[X]$, tels que :

$$\begin{cases} XR_1 = BQ_2 + R_2 \\ \deg(R_2) < \deg(B) \end{cases}$$

Donc, via (1), on a :

$$\begin{aligned} A &= B(XQ_1) + BQ_2 + R_2 + a_0 \\ &= B(XQ_1 + Q_2) + R_2 + a_0 \end{aligned}$$

Avec $XQ_1 + Q_2 \in \mathbb{Z}[X]$, $R_2 + a_0 \in \mathbb{Z}[X]$ et $\deg(R_2 + a_0) < \deg(B)$.

D'où le résultat par récurrence.

Il ne reste que le cas où $\deg(A) \notin \mathbb{N}$, donc $\deg(A) = -\infty$, c'est-à-dire $A = 0$.

On a :

$$A = 0 \times B + 0$$

Avec

$$\begin{cases} 0 \in \mathbb{Z}[X] \\ \deg(0) = -\infty < \deg(B) \end{cases}$$

D'où le résultat.

2. L'anneau $\mathbb{Z}[j]$. **2.a.** On a

$$1 + j + j^2 = \frac{1 - j^3}{1 - j} = 0$$

Donc $P(j) = 0$, où $P = X^2 + X + 1 \in \mathbb{Q}[X]$, et donc j est algébrique de $\mathbb{Q}$.

Déterminons le polynôme minimal de j :

Lemme 1.

Soient $\alpha \in \mathbb{C}$ et $P \in \mathbb{Q}[X]$ annulant α, alors $\pi_\alpha | P$.

Preuve du lemme 1.

Puisque $\pi_\alpha \neq 0$, et $\mathbb{Q}[X]$ est euclidien (car $\mathbb{Q}$ est un corps), alors il existe $(Q, R) \in \mathbb{Q}[X]^2$ tels que :

$$\begin{cases} P = Q\pi_\alpha + R \\ \deg(R) < \deg(\pi_\alpha) \end{cases}$$

On a :

$$R(\alpha) = P(\alpha) - Q(\alpha)\pi_\alpha(\alpha) = 0$$

Donc R annule α. De plus, $\deg(R) < \deg(\pi_\alpha)$, et π_α est par définition le polynôme non nul, unitaire, annulant α et de **degré minimal**. Puisque $\deg(R) < \deg(\pi_\alpha)$, alors forcément $R = 0$.

D'où

$$\pi_\alpha | P$$

Montrons maintenant que $\pi_j = X^2 + X + 1$.

Puisque $j^2 + j + 1 = 0$, alors $\pi_j | X^2 + X + 1$. Pour conclure, il suffit de montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{Q}[X]$.

On a le discriminant du trinôme $X^2 + X + 1$ est $-3 < 0$.

Donc $X^2 + X + 1$ est irréductible sur $\mathbb{R}[X]$.

Or, $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$, alors $X^2 + X + 1$ est également irréductible sur $\mathbb{Q}[X]$.

Via la relation $\pi_j | X^2 + X + 1$ et puisque $X^2 + X + 1$ est irréductible aussi sur $\mathbb{Q}[X]$, alors ou bien π_j est inversible, ou bien $\pi_j$est associé à $X^2 + X + 1$.

Avec $\deg(\pi_j) \geqslant 1$, on en déduit que $\pi_j$et X^2+X+1 sont associés. De plus, ils sont unitaires, donc ils sont égaux.

D'où

$$\pi_j = X^2 + X + 1$$

2.b. Montrons que

$$\mathbb{Z}[j] = \{a + bj | (a, b) \in \mathbb{Z}^2\}$$

Soit $(a, b) \in \mathbb{Z}^2$. On a $a + bj = P_{a,b}(j)$, avec $P_{a,b} = bX + a \in \mathbb{Z}[X]$, donc $a + bj \in \mathbb{Z}[j]$.

D'où

$$\{a + bj | (a, b) \in \mathbb{Z}^2\} \subseteq \mathbb{Z}[j]$$

Montrons maintenant que $\mathbb{Z}[j] \subseteq \{a + bj | (a, b) \in \mathbb{Z}^2\}$.

Soit $\alpha \in \mathbb{Z}[j]$. Alors par définition, il existe $P \in \mathbb{Z}[X]$tel que $\alpha = P(j)$.

En utilisant la question 1 de cette partie et puisque $X^2+X+1 \in \mathbb{Z}[X]$est unitaire, on a l'existence de $Q, R \in \mathbb{Z}[X]$ tels que :

$$\begin{cases} P = Q(X^2 + X + 1) + R \\ \deg(R) < \deg(X^2 + X + 1) = 2 \end{cases}$$

Donc

$$\alpha = P(j) = Q(j)(j^2 + j + 1) + R(j) = R(j)$$

En écrivant $R = b_1X+a_1 \in \mathbb{Z}[X]$, on a alors $\alpha = b_1j+a_1 \in \{a+bj|(a, b) \in \mathbb{Z}^2\}$

D'où

$$\mathbb{Z}[j] \subseteq \{a + bj | (a, b) \in \mathbb{Z}^2\}$$

Finalement

$$\mathbb{Z}[j] = \{a + bj | (a, b) \in \mathbb{Z}^2\}$$

Si vous êtes intéressé, je vous invite à démontrer la généralisation suivante :

Généralisation 1.

Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Notons $u_n = e^{\frac{2i\pi}{n}}$. On a

$$\mathbb{Z}[u_n] = \{a_0 + a_1u_n + \cdots + a_{n-2}u_n^{n-2} | (a_0, a_1, \ldots, a_{n-2}) \in \mathbb{Z}^{n-1}\}$$

2.c. Soit $z \in \mathbb{Z}[j]$, on a l'existence de $(a,b) \in \mathbb{Z}^2$tel que $z = a + jb$.

On a alors [2]

$$\begin{aligned} N(z) &= z\bar{z} \\ &= (a+jb)(a+\bar{j}b) \\ &= (a+jb)(a+j^2b) \\ &= a^2 + ab(j^2+j) + b^2 \\ &= a^2 - ab + b^2 \end{aligned}$$

Or, on sait que :

$$a^2 + b^2 \geqslant 2|ab|$$

Donc :

$$N(z) \geqslant 2|ab| - \text{ab} \geqslant 0$$

D'où $N(z) \in \mathbb{N}$.

Si $z \in \mathbb{Z}[j]$ est inversible dans $\mathbb{Z}[j]$, alors par définition, il existe $z' \in \mathbb{Z}[j]$ tel que $z.z'$=1.

On a alors :

$$N(z.z') = N(1) = 1.\bar{1} = 1$$

Et en développant :

$$N(z.z') = z.z'.\overline{z.z'} = z.\bar{z}.z'.\overline{z'} = N(z)N(z')$$

Donc, $N(z)N(z') = 1$ et $N(z), N(z') \in \mathbb{N}$, ce qui implique $N(z) = 1$.

Déterminons les éléments de $\mathbb{Z}[j]^\times$.

On a $z = a + bj$, où $a, b \in \mathbb{Z}$, et $N(z) = 1$, donc :

$$a^2 - ab + b^2 = 1$$

On en déduit que :

$$ab + 1 = a^2 + b^2 \geqslant 2|ab|$$

Ainsi,

$$(|ab| - ab) + |ab| \leqslant 1$$

2. car $\bar{j} = j^2$ et $j^2 + j = -1$.

Avec $|ab| - ab, |ab| \in \mathbb{N}$.
Alors,

$$\begin{cases} |ab| - ab = 0 \\ |ab| = 0 \end{cases} \text{ ou } \begin{cases} |ab| - ab = 0 \\ |ab| = 1 \end{cases} \text{ or } \begin{cases} |ab| - ab = 1 \\ |ab| = 0 \end{cases}$$

Or, $\begin{cases} |ab| - ab = 0 \\ |ab| = 0 \end{cases}$ équivaut à dire que ($a = 0$ ou $b = 0$),
Si $a = 0$, on a dans ce cas $1 = N(z) = b^2$, donc $b = 1$ ou $b = -1$.
D'où $z = j$ ou $z = -j$.
Si $b = 0$, on a de même $a = 1$ ou $a = -1$, donc $z = 1$ ou $z = -1$.

Et le système d'équations $\begin{cases} |ab| - ab = 0 \\ |ab| = 1 \end{cases}$ équivaut à $[(a = 1 \text{ and } b = 1) \text{ or } (a = -1 \,\text{et}\, b = -1)]$
Ainsi, $z = 1 + j$ ou $z = -1 - j$

Et $\begin{cases} |ab| - ab = 1 \\ |ab| = 0 \end{cases}$ n'admet pas de solutions.

En conclusion, on a :

$$\mathbb{Z}[j]^\times \subseteq \{-1, 1, -j, j, -1 - j, 1 + j\}$$

Réciproquement, vérifions que ces éléments sont bien des unités de $\mathbb{Z}[j]$:

$$\begin{aligned} (-1)^2 &= 1 \\ 1^2 &= 1 \\ -j(1 + j) &= 1 \\ j(-1 - j) &= 1 \end{aligned}$$

Par définition, on a donc :

$$\{-1, 1, -j, j, -1 - j, 1 + j\} \subseteq \mathbb{Z}[j]^\times$$

D'où :

$$\mathbb{Z}[j]^\times = \{-1, 1, -j, j, -1 - j, 1 + j\} = \{-1, 1, -j, j, -j^2, j^2\}$$

2.d. Soient $x \in \mathbb{Z}[j]$ et $y \in \mathbb{Z}[j]\backslash\{0\}$. Cherchons $q \in \mathbb{Z}[X]$ tel que $N\left(\frac{x}{y} - q\right) < 1$.

Notons

$$x = a + jb \text{ and } y = c + jd$$

On a

$$\begin{aligned} \frac{x}{y} &= \frac{a+jb}{c+jd} \\ &= \frac{(a+jd)(c+j^2d)}{c^2-cd+d^2} \\ &= \frac{ac-ad+bd}{c^2-cd+d^2} + j\frac{bc-ad}{c^2-cd+d^2} \end{aligned}$$

Notons

$$\alpha = \frac{ac-ad+bd}{c^2-cd+d^2} \in \mathbb{Q} \text{ and } \beta = \frac{bc-ad}{c^2-cd+d^2} \in \mathbb{Q}$$

Lemme 2.

Soit $a \in \mathbb{R}$, alors il existe $t_a \in \mathbb{Z}$, tel que $|a - t_a| \leqslant \frac{1}{2}$.

Preuve du lemme 2.

On a si $a - \lfloor a \rfloor > \frac{1}{2}$, alors

$$(\lfloor a \rfloor + 1) - a = (\lfloor a \rfloor - a) + 1 < \frac{1}{2}$$

D'où le résultat.

En particulier, il existe $t_\alpha, t_\beta \in \mathbb{Z}$ tels que

$$\begin{cases} |\alpha - t_\alpha| \leqslant \frac{1}{2} \\ |\beta - t_\beta| \leqslant \frac{1}{2} \end{cases}$$

Notons $q = t_\alpha + jt\beta \in \mathbb{Z}[j]$, on a alors

$$\begin{aligned} N\left(\frac{x}{y} - q\right) &= N((\alpha - t_\alpha) + j(\beta - t_\beta)) \\ &= (\alpha - t_\alpha)^2 - (\alpha - t_\alpha)(\beta - t_\beta) + (\beta - t_\beta)^2 \\ &\leqslant \frac{3}{2}[(\alpha - t_\alpha)^2 + (\beta - t_\beta)^2] \\ &\leqslant \frac{3}{4} \\ &< 1 \end{aligned}$$

Doù le résultat.

Montrons que $\mathbb{Z}[j]$ est un anneau euclidien.

Pour tout $x, y \in \mathbb{Z}[j]$tel que $y \neq 0$, on a l'existence de $q \in \mathbb{Z}[j]$ tel que $N\left(\frac{x}{y} - q\right) < 1$.

On a alors $x = yq + (x - qy)$ avec

$$\begin{aligned} N(x - qy) &= N(y)N\left(\frac{x}{y} - q\right) \\ &< N(y) \end{aligned}$$

et $x - qy \in \mathbb{Z}[j]$.

D'où l'application $N : \mathbb{Z}[j] \to \mathbb{R}$ vérifie pour tout $x, y \in \mathbb{Z}[j]$ tel que $y \neq 0$, l'existence de $(q, r) \in \mathbb{Z}[j]^2$ tel que

$$\begin{cases} x = q.y + r \\ N(r) < N(y) \end{cases}$$

D'où $\mathbb{Z}[j]$ est euclidien.

3. Polynômes cyclotomiques. **3.a.** Montrons que :

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Notons U_n l'ensemble des racines n-ième de l'unité. Montrons que :

$$U_n = \bigsqcup_{d|n} \mu_d^\star$$

Soit $d \in \mathbb{N}$, tel que $d|n$, et soit $z \in \mu_d^\star$.

On a z est une racine d-ième de l'unité donc il existe $k \in \mathbb{N}$, tel que $z = \exp\left(\frac{2i\pi k}{d}\right)$.

On a alors :

$$\begin{aligned} z^n &= \exp\left(\frac{2i\pi kn}{d}\right) \\ &= \exp\left(2i\pi k\frac{n}{d}\right) \\ &= 1 \end{aligned}$$

Donc $z \in U_n$, ensuite $\mu_d^\star \subset U_n$, et ceci pour tout $d \in \mathbb{N}$, tel que $d|n$.

Donc

$$\bigcup_{d|n} \mu_d^\star \subset U_n$$

Réciproquement, soit $z \in U_n$, alors il existe $k \in [\![0, n-1]\!]$, tel que $z = \exp\left(\frac{2ik\pi}{n}\right)$

Notons :

$$k' = \frac{k}{n \wedge k} \text{ and } n' = \frac{n}{n \wedge k}$$

On a $n' \wedge k' = 1$, et

$$z = \exp\left(\frac{2ik'\pi}{n'}\right)$$

Avec $n'|n$, et $n' \wedge k' = 1$, alors $z \in \mu_{n'}^\star \subset \bigcup_{d|n} \mu_d^\star$.

Donc :

$$U_n \subset \bigcup_{d|n} \mu_d^\star$$

Par suite :

$$U_n = \bigcup_{d|n} \mu_d^\star$$

Il ne reste qu'à montrer que $\bigcup_{d|n} \mu_d^\star$ est disjoint.

Plus généralement, soit $k, l \in \mathbb{N}^\star$, tel que $k \neq l$, montrons que $\mu_k^\star \cap \mu_l^\star = \emptyset$.

Par l'absurde, supposons que $\mu_k^\star \cap \mu_l^\star \not= \emptyset$, alors il existe $z \in \mu_k^\star \cap \mu_l^\star$

Donc,

$$\exists k_1 \in [\![0, k-1]\!] \text{ tel que } z = \exp\left(\frac{2ik_1\pi}{k}\right) \text{ and } k_1 \wedge k = 1$$

et

$$\exists l_1 \in [\![0, l-1]\!] \text{ tel que } z = \exp\left(\frac{2il_1\pi}{l}\right) \text{ and } l_1 \wedge l = 1$$

Par symétrie, on peut supposer que $k < l$. On a alors :

$$\exp\left(\frac{2ik_1 l\pi}{k}\right) = \exp\left(\frac{2il_1 l\pi}{l}\right) = \exp(2\,\mathrm{il}_1\,\pi) = 1$$

Donc $\frac{k_1 l}{k} \in \mathbb{Z}$, par suite $k|k_1 l$, avec $k_1 \wedge k = 1$.D'après le lemme de Gauss, on en déduit que $k|l$, absurde, puisque $k, l \in \mathbb{N}^\star$ et $k < l$.

D'où

$$\mu_k^\star \cap \mu_l^\star = \emptyset$$

Ainsi,

$$\bigcup_{d|n} \mu_d^\star = \bigsqcup_{d|n} \mu_d^\star$$

Donc :

$$U_n = \bigsqcup_{d|n} \mu_d^\star$$

À partir de ce résultat, on peut déduire que :

$$\begin{aligned} X^n - 1 &= \prod_{z \in U_n} (X - z) \\ &= \prod_{z \in \bigsqcup_{d|n} \mu_d^\star} (X - z) \\ &= \prod_{d|n} \left[\prod_{z \in \mu_d^\star} (X - z) \right] \\ &= \prod_{d|n} \Phi_d(X) \end{aligned}$$

3.b. En déduire que $\Phi_n(X) \in \mathbb{Z}[X]$,

Montrons le résultat par récurrence sur $n \in \mathbb{N}^*$

Pour$n = 1$, on a $\Phi_1 = X - 1 \in \mathbb{Z}[X]$.

Soit $n \in \mathbb{N}^*$, supposons que $\Phi_1, \Phi_2, \ldots, \Phi_n \in \mathbb{Z}[X]$ et montrons que $\Phi_{n+1} \in \mathbb{Z}[X]$.

D'après la question précédente, on a :

$$X^n - 1 = \Phi_{n+1} \prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d$$

Par hypothèse de récurrence, on a $\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d \in \mathbb{Z}[X]$. De plus, $\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d$ est unitaire. En utilisant la question 1 de cette partie, il vient :

$$\exists (Q, R) \in \mathbb{Z}[X]^2, \quad X^{n+1} - 1 = Q \prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d + R$$

avec

$$\deg(R) < \deg \left(\prod_{\substack{d|n+1 \\ d \leqslant n}} \Phi_d \right)$$

Pour tout $\alpha \in \mathbb{C}$ racine de $\prod_{\substack{d|n+1 \\ d\leqslant n}} \Phi_d$, on a

$$R(\alpha) = \alpha^{n+1} - 1 - Q(\alpha) \prod_{\substack{d|n+1 \\ d\leqslant n}} \Phi_d(\alpha) = 0$$

Donc α est également racine de R.

Avec $\deg(R) < \deg\left(\prod_{\substack{d|n+1 \\ d\leqslant n}} \Phi_d\right)$, donc forcément $R = 0$.

D'où

$$X^{n+1} - 1 = Q \prod_{\substack{d|n+1 \\ d\leqslant n}} \Phi_d$$

Avec

$$\Phi_{n+1} = \frac{X^{n+1}}{\prod_{\substack{d|n+1 \\ d\leqslant n}} \Phi_d} = Q \in \mathbb{Z}[X]$$

Ce qui conclut la démonstration par récurrence.

3.c. Soit p un nombre premier

3.c.i. On a

$$\begin{aligned} X^p - 1 - (X-1)^p &= -\sum_{k=1}^{p-1} \binom{p}{k} X^k (-1)^{p-k} \\ &= \sum_{k=1}^{p-1} (-1)^k \binom{p}{k} X^k \end{aligned}$$

On a, pour tout $k \in [\![1, p-1]\!]$,

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

donc

$$p! = k!(p-k)! \binom{p}{k}$$

Avec, pour tout $i \in [\![1, k]\!]$, on a $p \wedge i = 1$, donc $p \wedge k! = 1$, et pour tout $i \in [\![1, p-k]\!]$ on a également $p \wedge i = 1$, donc $p \wedge (p-k)! = 1$.

Ainsi,

$$p \wedge k!(p-k)! = 1$$

avec $p|k!(p-k)!\begin{pmatrix} p \\ k \end{pmatrix}$, donc d'après le lemme de Gauss, on a

$$p|\begin{pmatrix} p \\ k \end{pmatrix}$$

Ainsi,

$$\pi\left((-1)^k\begin{pmatrix} p \\ k \end{pmatrix}\right) = 0$$

D'où :

$$\begin{aligned}\hat{\pi}(X^p - 1 - (X-1)^p) &= \sum_{k=1}^{p-1}\pi\left((-1)^k\begin{pmatrix} p \\ k \end{pmatrix}\right)X^k \\ &= 0\end{aligned}$$

Donc :

$$\hat{\pi}(X^p - 1) - \hat{\pi}((X-1)^p) = 0$$

D'où :

$$\hat{\pi}(X^p - 1) = (X - 1_{\mathbb{F}_p})^p$$

Ce qui conclut la démonstration.

3.c.ii. Soient P et Q deux polynômes unitaires non constants dans $\mathbb{Z}[X]$ tels que

$$X^p - 1 = PQ$$

Montrons que P divise $P(1)$ et $Q(1)$.

D'après la question précédente, on a

$$\hat{\pi}(X^p - 1) = (X - 1_{\mathbb{F}_p})^p$$

Donc

$$\hat{\pi}(P)\hat{\pi}(Q) = (X - 1_{\mathbb{F}_p})^p$$

Puisque P et Q sont non constant, alors $\hat{\pi}(P)$ et $\hat{\pi}(Q)$ les sont aussi.

Par unicité de la décomposition en irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, on en déduit l'existence de $k \in [\![1, p-1]\!]$ tel que

$$\begin{cases} \hat{\pi}(P) = (X - 1_{\mathbb{F}_p})^k \\ \hat{\pi}(Q) = (X - 1_{\mathbb{F}_p})^{p-k} \end{cases}$$

Ainsi,

$$\begin{cases} \hat{\pi}(P)(1_{F_p}) = 0_{\mathbb{F}_p} \\ \hat{\pi}(Q)(1_{F_p}) = 0_{\mathbb{F}_p} \end{cases}$$

Ensuite

$$\begin{cases} \pi(P(1)) = 0 \\ \pi(Q(1)) = 0 \end{cases}$$

Cela implique que $p|P(1)$ et $p|Q(1)$.

3.c.iii. Montrons que Φ_p est irréductible de $\mathbb{Q}[X]$.

Par l'absurde, supposons que Φ_p n'est pas irréductible de $\mathbb{Q}[X]$.

Alors, il existe $P, Q \in \mathbb{Q}[X]$ tel que $\Phi_p = PQ$, et P, Q sont non-constants.

D'après le résultat admis, il existe $r \in \mathbb{Q}$, tel que :

$$\begin{cases} rP \in \mathbb{Z}[X] \\ \frac{1}{r}Q \in \mathbb{Z}[X] \end{cases}$$

Notons $P_1 = rP$ et $Q_1 = \frac{1}{r}Q$. On a alors

$$\Phi_p = P_1 Q_1$$

avec $P_1, Q_1 \in \mathbb{Z}[X]$ sont non-constants.

Notons

$$\begin{aligned} R_p(X) &= \Phi_p(X+1) \\ &= \sum_{k=0}^{p-1} (X+1)^k \\ &= \frac{(X+1)^p - 1}{X} \\ &= \sum_{k=1}^{p} \begin{pmatrix} p \\ k \end{pmatrix} X^{k-1} \\ &= \sum_{k=0}^{p-1} \begin{pmatrix} p \\ k+1 \end{pmatrix} X^k \end{aligned}$$

Écrivons également $P_1 = \sum_{k=0}^{l} a_k X^k$ et $Q_1 = \sum_{k=0}^{m} b_k X^k$, où $l, k \geqslant 1$ et $a_0, \ldots, a_l, b_0, \ldots, b_m \in \mathbb{Z}$.

Or, pour tout $k \in [\![0, p-2]\!]$, on a $p \mid \begin{pmatrix} p \\ k+1 \end{pmatrix}$, donc dans $\mathbb{Z}/p\mathbb{Z}[X]$, on obtient :

$$\hat{\pi}(R_p(X)) = X^{p-1}$$

Ainsi,

$$\hat{\pi}(P_1 Q_1) = X^{p-1}$$

Par conséquent,

$$\hat{\pi}(P_1)\hat{\pi}(Q_1) = X^{p-1}$$

Par unicité de la décomposition en irréductibles dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a

$$\hat{\pi}(P_1) = \overline{a_l} X^l$$

rt

$$\hat{\pi}(Q_1) = \overline{b_m} X^m$$

Ainsi $\overline{a_0} = 0$ et $\overline{b_0} = 0$, donc $p|a_0$ et $p|b_0$, ainsi $p^2|a_0 b_0$

Or,

$$a_0 b_0 = \begin{pmatrix} p \\ 1 \end{pmatrix} = p$$

Alors $p^2|p$, absurde.

D'où Φ_p est irréductible.

3.c.iv. Soit $\zeta = e^{\frac{2i\pi}{p}}$.

On a ζ est une racine primitive de l'unité, donc $\Phi_p(\zeta) = 0$.

Par conséquent,

$$\pi_\zeta | \Phi_p$$

Or, d'après la question précédente, on a Φ_p est irréductible ; ainsi, soit π_ζ est constant, soit $\pi_\zeta$est associé à Φ_p.

Avec π_ζ n'est pas constant, alors π_ζ et Φ_p sont associé. De plus, ils sont unitaires, donc ils sont égaux.

D'où,

$$\pi_\zeta = \Phi_p$$

On a :

$$\mathbb{Q}(\zeta) = \{P(\zeta)/P \in \mathbb{Q}[X]\}$$

est un corps (facile à vérifier).

De plus, si $P \in \mathbb{Q}[X]$, par division euclidienne de P par Φ_p, on a l'existence de $Q, R \in \mathbb{Q}[X]^2$ tels que

$$P = Q\Phi_p + R \text{ and } \deg(R) < p$$

Notons $R = \sum_{k=0}^{p-1} a_k X^k$, on a alors

$$\begin{aligned} P(\zeta) &= R(\zeta) \\ &= \sum_{k=0}^{p-1} a_k \zeta^k \\ &\in \text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1}) \end{aligned}$$

Donc

$$\mathbb{Q}(\zeta) \subset \text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1})$$

Réciproquement, pour tout $k \in [\![0, p-1]\!]$, on a $\zeta^k \in \mathbb{Q}(\zeta)$, avec $\mathbb{Q}(\zeta)$ est un $\mathbb{Q}$-espace vectoriel.

Ainsi,

$$\text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1}) \subset \mathbb{Q}(\zeta)$$

D'où

$$\mathbb{Q}(\zeta) = \text{vect}_{\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-1})$$

Ainsi, la famille $(1, \zeta, \ldots, \zeta^{p-1})$ est génératrice de $\mathbb{Q}(\zeta)$. Montrons qu'elle est $\mathbb{Q}$-libre.

Pour cela, soient $a_0, \ldots, a_{p-1} \in \mathbb{Q}$, tels que

$$\sum_{k=0}^{p-1} a_k \zeta^k = 0$$

On a donc

$$\left. \sum_{k=0}^{p-1} a_k X^k \right|_{X=\zeta} = 0$$

Avec $\deg\left(\sum_{k=0}^{p-1} a_k X^k\right) \leqslant p-1 < p$. Par minimalité du degré de $\pi_\zeta = \Phi_p$, on a forcément

$$\sum_{k=0}^{p-1} a_k X^k = 0$$

Par suite $a_0 = \cdots = a_{p-1} = 0$.

Ainsi, la famille $(1, \zeta, \ldots, \zeta^{p-1})$ est $\mathbb{Q}-$ libre .

Donc

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \dim_{\mathbb{Q}}(\mathbb{Q}(\zeta)) = p$$

On en conclut que l'extension de corps $\mathbb{Q}(\zeta)/\mathbb{Q}$ est de degré p.

4. Matrice compagnon **4.a.** Soit $k \in \{1, \ldots, n-1\}$. Par récurrence finie sur k, on peut montrer facilement que :

$$C_p^k e_1 = e_{k+1}$$

Donc, pour tout $Q \in \mathbb{C}[X]$non nul de degré inférieur ou égal à $(n-1)$, si l'on note :

$$Q = \sum_{k=0}^{n-1} a_k X^k$$

On a :

$$\begin{aligned} Q(C_p)e_1 &= \sum_{k=0}^{n-1} a_k C_p^k e_1 \\ &= \sum_{k=0}^{n-1} a_k e_{k+1} \\ &\neq 0 \end{aligned}$$

Car $(e_1, \ldots, e_n)$ est $\mathbb{C}$-libre, et $(a_0, \ldots, a_{n-1})$ne sont pas tous nuls.

Ainsi, on obtient :

$$Q(C_p) \neq 0$$

En particulier, le degré du polynôme minimal π_{C_p} est supérieur ou égal à n.

Or,

$$\deg(\pi_{C_p}) \leqslant \deg(\chi_{C_p}) = n$$

Où χ_{C_p} désigne le polynôme caractéristique de C_p.
Donc :

$$\deg(\pi_{C_p}) = n$$

4.b. D'après la question précédente, on a :

$$C_p^{n-1} e_1 = e_n$$

Donc,

$$\begin{aligned} C_p^n e_1 &= C_p e_n \\ &= \begin{pmatrix} -a_0 \\ -a_1 \\ . \\ . \\ . \\ -a_{n-1} \end{pmatrix} \\ &= -\sum_{k=0}^{n-1} a_k e_{k+1} \end{aligned}$$

Ainsi,

$$P(C_p) = C_p^n + \sum_{k=0}^{n-1} a_k C_p^k$$

Pour tout $j \in [\![2, n]\!]$, on a :

$$\begin{aligned} P(C_p)e_j &= C_p^n e_j + \sum_{k=0}^{n-1} a_k C_p^k e_j \\ &= C_p^n (C_p^{j-1} e_1) + \sum_{k=0}^{n-1} a_k C_p^k (C_p^{j-1} e_1) \end{aligned}$$

L'égalité reste vrai aussi pour $j = 1$, donc pour tout $j \in [\![1, n]\!]$, on a :

$$\begin{aligned} P(C_p)e_j &= C_p^{n+j-1} e_1 + \sum_{k=0}^{n-1} a_k C_p^{k+j-1} e_1 \\ &= C_p^{j-1} \left(C_p^n e_1 + \sum_{k=0}^{n-1} a_k C_p^k e_1 \right) \\ &= C_p^{j-1} \left(-\sum_{k=0}^{n-1} a_k e_k + \sum_{k=0}^{n-1} a_k e_k \right) \\ &= 0 \end{aligned}$$

Ainsi, $e_j \in \mathrm{Ker}(P(C_p))$ pour tout $j \in [\![1, n]\!]$, donc $\mathrm{Ker}(P(C_p)) = \mathbb{C}^n$.

Alors,

$$P(C_p) = 0$$

Ensuite,

$$\pi_{C_p} | P$$

Avec $\deg(\pi_{C_p}) = \deg(P)$, et π_{C_p} et P sont unitaires, donc π_{C_p} et P sont égaux.

4.c. D'après le théorème de Cayley-Hamilton, $\pi_{C_p} | \chi_{C_p}$, avec $\deg(\pi_{C_p}) = \deg(\chi_{C_p}) = n$

Ainsi, π_{C_p} et χ_{C_p} sont associés. De plus, étant unitaires, on obtient :

$$\chi_{C_p} = \pi_{C_p} = P$$

4.d. Montrons que

$$\chi_{Q(M)} = \prod_{k=1}^{n} (X - Q(\alpha_k))$$

Puisque $\mathbb{C}$ est algébriquement clos, alors M est trigonalisable. Donc, il existe $P \in \mathrm{GL}_n(\mathbb{C})$ et $T \in T_{n,s}(\mathbb{C})$ tels que :

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

On a $\alpha_1, \ldots, \alpha_n$ sont les racines de χ_M, donc il existe une permutation $\sigma : \mathcal{S}_n \to \mathcal{S}_n$ telle que

$$T = \begin{pmatrix} \alpha_{\sigma(1)} & * & . & . & * \\ 0 & \alpha_{\sigma(2)} & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & \alpha_{\sigma(n)} \end{pmatrix}$$

Pour tout $k \in \mathbb{N}$, on a :

$$M^k = P \begin{pmatrix} \alpha_{\sigma(1)}^k & * & . & . & * \\ 0 & \alpha_{\sigma(2)}^k & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & \alpha_{\sigma(n)}^k \end{pmatrix} P^{-1}$$

Notons $Q(X) = \sum_{k=0}^{l} a_k X^k$. Alors,

$$\begin{aligned} Q(M) &= \sum_{k=0}^{l} a_k P \begin{pmatrix} \alpha_{\sigma(1)}^k & * & . & . & * \\ 0 & \alpha_{\sigma(2)}^k & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & \alpha_{\sigma(n)}^k \end{pmatrix} P^{-1} \\ &= P \begin{pmatrix} \sum_{k=0}^{l} a_k \alpha_{\sigma(1)}^k & * & . & . & * \\ 0 & \sum_{k=0}^{l} a_k \alpha_{\sigma(2)}^k & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & 0 & * \\ 0 & 0 & 0 & 0 & \sum_{k=0}^{l} a_k \alpha_{\sigma(n)}^k \end{pmatrix} p^{-1} \\ &= P \begin{pmatrix} Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & Q(\alpha_{\sigma(n)}) \end{pmatrix} P^{-1} \end{aligned}$$

Ainsi,

$$\begin{aligned}
\chi_{Q(M)} &= \det(XI_n - M) \\
&= \det\left(P\begin{pmatrix} X-Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & X-Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & X-Q(\alpha_{\sigma(n)}) \end{pmatrix}P^{-1}\right) \\
&= \det\left(P\times P^{-1}\times\begin{pmatrix} X-Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & X-Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & X-Q(\alpha_{\sigma(n)}) \end{pmatrix}\right) \\
&= \det\begin{pmatrix} X-Q(\alpha_{\sigma(1)}) & * & . & . & * \\ 0 & X-Q(\alpha_{\sigma(2)}) & & & \star \\ . & 0 & & & . \\ . & . & & & . \\ . & . & . & . & * \\ 0 & 0 & 0 & 0 & X-Q(\alpha_{\sigma(n)}) \end{pmatrix} \\
&= \prod_{k=1}^{n}(X - Q(\alpha_{\sigma(k)})) \\
&= \prod_{k=1}^{n}(X - Q(\alpha_k))
\end{aligned}$$

4.e. A est un sous-anneau de $\mathbb{C}$, et $Q \in A[X]$.

Soit $P \in A[X]$ un polynôme unitaire dont les racines complexes, comptées avec leur multiplicité, sont $\alpha_1, \ldots, \alpha_n$.

Puisque $P \in A[X]$, alors $C_p \in \mathcal{M}_n(A)$. Étant donné que $\mathcal{M}_n(A)$ est un anneau, alors

$$\forall k \in \mathbb{N}, \quad C_p^k \in \mathcal{M}_n(A)$$

Ensuite,

$$\forall R \in A[X], \quad R(C_p) \in \mathcal{M}_n(A)$$

En particulier,

$$Q(C_p) \in \mathcal{M}_n(A)$$

Ainsi,

$$XI_n - Q(C_p) \in \mathcal{M}_n(A)$$

Par définition du déterminant, et puisque A est un anneau, on en déduit que

$$\chi_{Q(C_p)} = \det(XI_n - Q(C_p)) \in A[X]$$

Or, le polynôme caractéristique de C_p est P, dont les racines sont $\alpha_1, \ldots, \alpha_n$. D'après la question précédente, on a donc

$$\chi_{Q(C_p)} = \prod_{k=1}^{n} (X - Q(\alpha_k))$$

Enfin,

$$\prod_{k=1}^{n} (X - Q(\alpha_k)) \in A[X]$$

II Nombres algébriques

1.a. On considère la $\varphi : \mathbb{N}^\star \to \mathbb{N}$ définie pour tout $n \in \mathbb{N}^*$ par :

$$\varphi(n) = \text{card}\{k \in [\![1, n]\!] | k \wedge n = 1\}$$

Soit $d \geqslant 1$ un entier. Montrons que $\{n \in \mathbb{N}^\star, \varphi(n) \leqslant d\}$ est fini.

Pour tout $n \geqslant 2$, écrivons n sous la forme :

$$n = \prod_{j=1}^{r} p_{i_j}^{\alpha_{i_j}}$$

où $i_1 < \ldots < i_r \in \mathbb{N}^*$, $(p_i)_{i \in \mathbb{N}^*}$est la suite des nombres premiers, et $\alpha_{i_1}, \ldots, \alpha_{i_r} \in \mathbb{N}^*$.

On a alors :

$$\varphi(n) = n \prod_{j=1}^{r} \left(1 - \frac{1}{p_{i_j}}\right)$$

Or, pour tout $i \in \mathbb{N}^*$, on a $p_i \geqslant (i+1)$ (Car la suite $(p_i)_{i \in \mathbb{N}^*}$ est une suite d'entiers strictement croissante avec $p_1 = 2$).

Donc :

$$\begin{aligned}\varphi(n) &\geqslant n\prod_{j=1}^{r}\left(1-\frac{1}{i_j+1}\right)\\ &\geqslant n\prod_{j=1}^{i_r}\left(1-\frac{1}{j+1}\right)\\ &= \frac{n}{i_r+1}\end{aligned}$$

Avec :

$$\begin{aligned}n &= \prod_{j=1}^{r}p_{i_j}^{\alpha_{i_j}}\\ &\geqslant 2^{\alpha_{i_1}+\cdots+\alpha_{i_r}}\\ &\geqslant 2^{i_r}\end{aligned}$$

On en déduit que :

$$i_r \leqslant \frac{\log(n)}{\log(2)}$$

Ainsi :

$$\begin{aligned}\varphi(n) &\geqslant \frac{n}{\frac{\log(n)}{\log(2)}+1}\\ &\underset{n\to+\infty}{\sim} \log(2)\frac{n}{\log(n)}\\ &\underset{n\to+\infty}{\to} +\infty\end{aligned}$$

Par conséquent, il existe un entier $N_0 \in \mathbb{N}$ tel que, pour tout $n \geqslant N_0$, on a $\varphi(n) > d$.

D'où :

$$\{n \in \mathbb{N}^* | \varphi(n) \leqslant d\} \subseteq [\![1, N_0 - 1]\!]$$

On en conclut que l'ensemble $\{n \in \mathbb{N}^\star, \varphi(n) \leqslant d\}$ est fini.

1.b. Soit K un sous-corps de $\mathbb{C}$, tel que $K/\mathbb{Q}$ soit une extension finie.

Montrons que K contient un nombre fini de racines de l'unité.

Soit u une racine de l'unité, donc par définition, il existe $n \in \mathbb{N}^*$, tel que $u^n = 1$.

Soit n_0 le plus petit entier non nul tel que $u^{n_0} = 1$.

Alors, u est une racine n_0-ième primitive de l'unité.

On a alors :

$$\Phi_{n_0}(u) = 0$$

où Φ_{n_0} est irréductible sur $\mathbb{Q}[X]$, donc $\pi_\alpha = \Phi_{n_0}$.

Ainsi, $\mathbb{Q}(u)/\mathbb{Q}$ est une extension finie de degré $\deg(\Phi_{n_0}) = \varphi(n_0)$.

On obtient donc :

$$\varphi(n_0) \leqslant [K : \mathbb{Q}]$$

Ainsi,

$$u \in \bigcup_{\substack{n_0 \in \mathbb{N}^\star \\ \varphi(n_0) \leqslant [K:\mathbb{Q}]}} \{\alpha \in \mathbb{C} | \alpha^{n_0} = 1\}$$

Or, pour tout $n_0 \in \mathbb{N}$, $\{\alpha \in \mathbb{C} | \alpha^{n_0} = 1\}$ est fini, et d'après la question précédente, on a l'ensemble

$$\{n_0 \in \mathbb{N}^* | \varphi(n_0) \leqslant [K : \mathbb{Q}]\}$$

est fini.

D'où le résultat.

2.a. Montrons que π_α est irréductible de $\mathbb{Q}[X]$.

Soient $P, Q \in \mathbb{Q}[X]$ tels que $\pi_\alpha = \mathrm{PQ}$.

On a

$$P(\alpha)Q(\alpha) = \pi_\alpha(\alpha) = 0$$

Donc $P(\alpha) = 0$ ou $Q(\alpha) = 0$.

Par symétrie, on suppose que $P(\alpha) = 0$. Alors $\pi_\alpha | P$, car P est non nul (si c'est le cas, on aurait $\pi_\alpha = 0$, ce qui contredit le fait que $\deg(\pi_\alpha) \geqslant 1$).

Comme $\deg(P) \leqslant \deg(\pi_\alpha)$, on a nécessairement $\deg(P) = \deg(\pi_\alpha)$.

Ce qui implique que Pet π_α sont associés.

D'où, π_α est irréductible de $\mathbb{Q}[X]$.

Notons $n = \deg(\pi_\alpha)$. Et soit $P \in \mathbb{Q}[X]$. Par division euclidienne de P par π_α, on a l'existence de $Q, R \in \mathbb{Q}[X]$tels que

$$P = Q\pi_\alpha + R$$

Donc

$$\begin{aligned} P(\alpha) &= Q(\alpha)\pi_\alpha(\alpha) + R(\alpha) \\ &= R(\alpha) \\ &\in \text{vect}_{\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) \end{aligned}$$

Cela signifie que

$$\mathbb{Q}(\alpha) = \{P(\alpha) | P \in \mathbb{Q}[X]\} \subset \text{vect}_{\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1})$$

En particulier, la famille $(1, \alpha, \ldots, \alpha^{n-1})$ est génératrice de $\mathbb{Q}(\alpha)$.

Si $a_0, \ldots, a_{n-1} \in \mathbb{Q}$, tels que

$$\sum_{k=0}^{n-1} a_k \alpha^k = 0$$

Alors $\pi_\alpha \left| \sum_{k=0}^{n-1} a_k X^k \right.$. Étant donné que $\deg(\pi_\alpha) = n$, on a nécessairement $\sum_{k=0}^{n-1} a_k X^k = 0$, d'où $a_0 = \cdots = a_{n-1} = 0$.

Cela montre que la famille $(1, \alpha, \ldots, \alpha^{n-1})$ est $\mathbb{Q}$-libre.

En conclusion, la famille $(1, \alpha, \ldots, \alpha^{n-1})$ est une base de $\mathbb{Q}$-espace vectoriel $K = \mathbb{Q}(\alpha)$

Donc

$$d = [K : \mathbb{Q}] = \dim_{\mathbb{Q}}(K) = n$$

Ainsi,

$$\deg(\pi_\alpha) = d$$

2.b. Soit σ un morphisme de $\mathbb{Q}$-algèbre de K dans $\mathbb{C}$.

Montrons que $\sigma(\alpha)$ est une racine de π_α.

Notons $\pi_\alpha = \sum_{k=0}^{d} a_k X^k$. On a $\pi_\alpha(\alpha) = 0$, donc

$$\sum_{k=0}^{d} a_k \alpha^k = 0$$

Ainsi,

$$\sigma\left(\sum_{k=0}^{d} a_k \alpha^k\right) = 0$$

Par suite,

$$\sum_{k=0}^{d} a_k \sigma(\alpha)^k = 0$$

D'où

$$\pi_\alpha(\sigma(\alpha)) = 0$$

Cela prouve le résultat. Montrons maintenant qu'il y a exactement d morphismes de $\mathbb{Q}$-algébre.

Lemme 3.

Soit $P \in \mathbb{Q}[X]$ irréductible ; alors les racines complexes de P sont deux à deux distinctes.

Preuve du lemme 3.

Si P admet une racine double $\alpha \in \mathbb{C}$, alors α est aussi racine de P'.

Donc on a $P \wedge P'$ est non constant dans $\mathbb{C}[X]$.

Or, la division euclidienne est invariante par extension de corps ; donc, d'après l'algorithme d'Euclide, $P \wedge P'$ reste non constant dans $\mathbb{Q}[X]$.

Or, comme P est irréductible, donc $P \wedge P' = P$, en particulier $P' | P$.

Et puisque $\deg(P') = \deg(P) - 1 < \deg(P)$, cela implique $P' = 0$, ce qui est absurde, car P serait alors constant !

D'où le résultat du lemme.

On en déduit que π_α admet exactement d recines complexes, notées $\alpha_1, \ldots, \alpha_d$ avec $\alpha_1 = \alpha$.

Soient $\sigma, \tau : K \to \mathbb{C}$ deux morphismes d'algèbre tels que $\sigma(\alpha) = \tau(\alpha)$. Montrons que $\sigma = \tau$.

Soit $x \in K = \mathbb{Q}(\alpha)$. Alors il existe $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$ tel que $x = P(\alpha)$

On a alors

$$\begin{aligned}\sigma(x) &= \sigma\left(\sum_{k=0}^{n} a_k \alpha^k\right)\\ &= \sum_{k=0}^{n} a_k \sigma(\alpha)^k\\ &= \sum_{k=0}^{n} a_k \tau(\alpha)^k\\ &= \tau\left(\sum_{k=0}^{n} a_k \alpha^k\right)\\ &= \tau(x)\end{aligned}$$

Cela est vrai pour tout $x \in K$, donc $\sigma = \tau$. On en conclut qu'un morphisme d'algèbre $K \to \mathbb{C}$ est déterminé par l'image de α, et cette image est une racine de π_α.

On en déduit qu'il existe exactement d morphismes de $\mathbb{Q}$-algèbre, notés $\sigma_k : K \to \mathbb{C}$, où $k \in \{1, 2, \ldots, d\}$.

3. Soit $\alpha \in \mathbb{C}$ un nombre algébrique, et $\theta \in K = \mathbb{Q}(\alpha)$.

3.a. Justifiant que θ est un nombre algébrique.

On a $\mathbb{Q}(\theta)$ est une sous-algèbre de $\mathbb{Q}(\alpha)$.

Or, α est algébrique, donc l'extension de corps $\mathbb{Q}(\alpha)/\mathbb{Q}$ est finie. Par conséquent, $\mathbb{Q}(\theta)/\mathbb{Q}$ est aussi finie (car $\mathbb{Q}(\theta)$ est une sous-algèbre de $\mathbb{Q}(\alpha)$).

D'où θ est un nombre algébrique.

3.b. Montrons que $P_\theta = \prod_{k=1}^{d} (X - \sigma_k(\theta)) \in \mathbb{Q}[X]$

Comme $\theta \in \mathbb{Q}(\alpha)$, alors il existe $R = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$ tel que $\theta = R(\alpha)$.

On a pour tout $k \in [\![1, d]\!]$:

$$\begin{aligned}\sigma_k(\theta) &= \sigma_k\left(\sum_{j=0}^{n} a_j \alpha^j\right)\\ &= \sum_{j=0}^{n} a_j \sigma_k(\alpha)^j\\ &= R(\sigma_k(\alpha))\end{aligned}$$

Donc :

$$P_\theta = \prod_{k=1}^{d} (X - R(\sigma_k(\alpha)))$$

Or, $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ sont les racines de $\pi_\alpha \in \mathbb{Q}[X]$, et $R \in \mathbb{Q}[X]$.

D'après la question **4.e** de la partie **I**, on a donc :

$$P_\theta = \prod_{k=1}^{d} (X - R(\sigma_k(\alpha))) \in \mathbb{Q}[X]$$

3.c. Justifions que π_θ divise P_θ, en utilisant la même notation que dans la question précédente :

$$\theta = \sum_{j=0}^{n} a_j \alpha^j$$

où $a_0, \ldots, a_n \in \mathbb{Q}$.

On a :

$$\begin{aligned} P_\theta(\theta) &= \prod_{k=1}^{d} (\theta - \sigma_k(\theta)) \\ &= \prod_{k=1}^{d} \left(\sum_{j=0}^{n} a_j \alpha^j - \sigma_k \left(\sum_{j=0}^{n} a_j \alpha^j \right) \right) \\ &= \prod_{k=1}^{d} \left(\sum_{j=0}^{n} a_j (\alpha^j - \sigma_k(\alpha)^j) \right) \end{aligned}$$

Or, les $\sigma_1(\alpha), \ldots, \sigma_d(\alpha)$ sont exactement les racines de π_α.

Donc, il existe $k_0 \in [\![1, d]\!]$ tel que

$$\sigma_{k_0}(\alpha) = \alpha$$

On a alors :

$$\begin{aligned} P_\theta(\theta) &= \left(\sum_{j=0}^{n} a_j (\alpha^j - \alpha^j) \right) \prod_{\substack{k=1 \\ k \neq k_0}}^{d} \left(\sum_{j=0}^{n} a_j (\alpha^j - \sigma_k(\alpha)^j) \right) \\ &= 0 \end{aligned}$$

Comme $P_\theta \in \mathbb{Q}[X]$ (d'après la question précédente), on en déduit, via le lemme 1, que $\pi_\theta | P_\theta$.

Montrons maintenant que P_θ est une puissance de π_θ.

Notons :

$$\mathcal{A}_\theta = \{k \in \mathbb{N} | \pi_\theta | P_\theta\}$$

D'après la première partie de cette question $1 \in \mathcal{A}_\theta$, donc $\mathcal{A}_\theta \neq \varnothing$. Ainsi, cette partie de $\mathbb{N}$ admet un plus grand élément, noté $k_0 = \max(\mathcal{A}_\theta)$.

On a alors $\pi_\theta^{k_0} | P_\theta$ et $\pi_\theta^{k_0+1} \not| P_\theta$.

Donc, il existe $Q \in \mathbb{Q}[X]$ tel que $P_\theta = Q\pi_\theta^{k_0}$.

Comme $\pi_\theta \not| Q$ et π_θ est irréductible, alors $Q \wedge \pi_\theta = 1$.

Par suite, via le théorème de Bézout [3], on a l'existence de $R, S \in \mathbb{Q}[X]$ tels que :

$$R\pi_\theta + SQ = 1$$

Par l'absurde, supposons que Q est non constant.

Alors, d'après le théorème fondamental de l'algèbre, Q est scindé sur $\mathbb{C}$. De plus, toutes ses racines sont des racines de P_θ.

Notons

$$\pi_\theta = \sum_{j=0}^{l} \beta_j X^j$$

On a les racines de P_θ sont $\sigma_1(\theta), \ldots, \sigma_d(\theta)$. Et pour tout $k \in [\![1, d]\!]$, on a :

$$\begin{aligned}
\pi_\theta(\sigma_k(\theta)) &= \pi_\theta(\sigma_k(\theta)) \\
&= \sum_{j=0}^{l} \beta_j \sigma_k(\theta)^j \\
&= \sigma_k\left(\sum_{j=0}^{l} \beta_j \theta^j\right) \\
&= \sigma_k(\pi_\theta(\theta)) \\
&= \sigma_k(0) \\
&= 0
\end{aligned}$$

Soit γ un racine de Q. Puisque les racines de Q sont des racines de P_θ, alors il existe $k_0 \in [\![1, d]\!]$ tel que :

$$\gamma = \sigma_{k_0}(\theta)$$

3. Le théorème de Bézout est valable sur $\mathbb{Q}[X]$, car l'anneau $\mathbb{Q}[X]$ est euclidien (puisque $\mathbb{Q}$ est un corps), donc $\mathbb{Q}[X]$ est un anneau de Bézout.

via la relation (5), on a :

$$1 = R(\sigma_{k_0}(\theta))\pi_\theta(\sigma_{k_0}(\theta)) + S(\sigma_{k_0}(\theta))Q(\sigma_{k_0}(\theta)) = 0$$

ce qui est absurde !

D'où Q est constant. Comme P_θ et π_θ sont unitaires, alors $Q = 1$.

Par suite,

$$P_\theta = \pi_\theta^{k_0}$$

D'où le résultat.

4. Soit $\alpha \in \mathbb{C}$

$\Rightarrow$) Si α est un entier algébrique, alors par définition, il existe un polynôme unitaire à coefficients entiers tel que $P(\alpha) = 0$.

On a alors $\pi_\alpha | P$, donc il existe $Q \in \mathbb{Q}[X]$ tel que $P = \pi_\alpha Q$.

D'après le résultat admis, on a l'existence de $r \in \mathbb{Q}$ tel que :

$$\begin{cases} r\pi_\alpha \in \mathbb{Z}[X] \\ \frac{1}{r}Q \in \mathbb{Z}[X] \end{cases}$$

Le coefficient dominant de $r\pi_\alpha$ est r, donc $r \in \mathbb{Z}$.

De même, le coefficient dominant de $\frac{1}{r}Q$ est $\frac{1}{r}$, alors $\frac{1}{r} \in \mathbb{Z}$.

Ainsi, $r \in \{-1, 1\}$, d'où $\pm\pi_\alpha \in \mathbb{Z}[X]$, donc $\pi_\alpha \in \mathbb{Z}[X]$.

$\Leftarrow$) Si $\pi_\alpha \in \mathbb{Z}[X]$,

puisque $\pi_\alpha(\alpha) = 0$, par définition, α est un entier algébrique.

5.a. Si α est un entier algébrique, notons $d = \deg(\pi_\alpha)$.

Soit $x \in \mathrm{gr}\{\alpha^n | n \in \mathbb{N}\}$, donc il existe $n_1, \ldots, n_r \in \mathbb{N}$ et $a_1, \ldots, a_r \in \mathbb{Z}$ tels que

$$x = a_1\alpha^{n_1} + \cdots + a_r\alpha^{n_r}$$

Notons

$$P = \sum_{k=1}^{r} a_k X^{n_k} \in \mathbb{Z}[X]$$

D'après **la question 1 de la partie** I, on a l'existence de $Q, R \in \mathbb{Z}[X]$ tels que

$$P = \pi_\alpha Q + R$$

avec $\deg(R) \leqslant d-1$.

On a donc

$$x = P(\alpha) = \pi_\alpha(\alpha)Q(\alpha) + R(\alpha)$$

Ainsi, x s'écrit comme une combinaison linéaire à coefficients entiers de $1, \alpha, \ldots, \alpha^{d-1}$.

D'où le groupe engendré par $\{\alpha^n | n \in \mathbb{N}\}$ est de type fini.

5.b. Réciproquement, si G est de type fini, montrons que α est un entier algébrique.

Soit $(g_1, \ldots, g_n)$ une famille génératrice finie de G.

Notons, pour tout $i \in [\![1, n]\!]$,

$$\alpha g_i = \sum_{k=1}^{n} a_{i,k} g_k$$

Où $a_{i,k} \in \mathbb{Z}$, pour tous $i, k \in [\![1, n]\!]$

Notons $A = (a_{i,k})_{1 \leqslant i,k \leqslant n}$ et $X = \begin{pmatrix} g_1 \\ g_2 \\ . \\ . \\ . \\ g_n \end{pmatrix}$

On a alors

$$\alpha X = AX$$

Donc,

$$(A - \alpha I_n)X = 0$$

En particulier,

$$A - \alpha I_n \notin \mathrm{GL}_n(\mathbb{C})$$

D'où,

$$\det(A - \alpha I_n) = 0$$

Ainsi,

$$\sum_{\sigma \in \mathcal{S}_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^{n} (a_{\sigma(i),i} - \alpha \delta_{\sigma(i),i}) = 0$$

Où $\varepsilon(\sigma) \in \{-1, 1\}$ est la signature de σ, pour tout $\sigma \in \mathcal{S}_n$.

D'où,

$$P(\alpha) = 0$$

Avec,

$$P = \sum_{\sigma \in \mathcal{S}_n} (-1)^{\varepsilon(\sigma)} \prod_{i=1}^{n} (a_{\sigma(i),i} - X\delta_{\sigma(i),i}) \in \mathbb{Z}[X]$$

D'où α est un entier algébrique.

6. Montrons que $\mathcal{D}_{\mathbb{C}}$, l'ensemble des entiers algébriques de $\mathbb{C}$, est un sous-anneau de $\mathbb{C}$.

On a $0 \in \mathcal{D}_{\mathbb{C}}$ (car $\pi_0 = X \in \mathbb{Z}[X]$), donc $\mathcal{D}_{\mathbb{C}} \neq \varnothing$.

Soient $\alpha, \beta \in \mathcal{D}_{\mathbb{C}}$.

Les deuc groupes $G_\alpha := \mathrm{gr}\{\alpha^n | n \in \mathbb{N}\}$ et $G_\beta := \mathrm{gr}\{\beta^n | n \in \mathbb{N}\}$ sont de type fini.

Donc, il existe une famille $(g_1, \ldots, g_n)$ (respectivement $(l_1, \ldots, l_m)$) génératrice de G_α (respectivement de G_β).

On a, pour tout $i \in \mathbb{N}$, il existe $a_{i,1}, \ldots, a_{i,n} \in \mathbb{Z}$, tel que

$$\alpha^i = \sum_{k=1}^{n} a_{i,k} g_k$$

Et pour tout $i \in \mathbb{N}$, il existe $b_{i,1}, \ldots, b_{i,m} \in \mathbb{Z}$, tel que

$$\beta^i = \sum_{k=1}^{m} b_{i,k} l_k$$

Pour tout $x \in G_{\alpha\beta} := \mathrm{gr}\{(\alpha\beta)^n | n \in \mathbb{N}\}$, on a l'existence de $c_0, \ldots, c_r \in \mathbb{Z}$ tel que

$$x = \sum_{j=0}^{r} c_j (\alpha\beta)^j$$

On a alors

$$\begin{aligned} x &= \sum_{j=0}^{r} c_j \alpha^j \beta^j \\ &= \sum_{j=0}^{r} c_j \left(\sum_{k=1}^{n} a_{j,k} g_k \right) \left(\sum_{i=1}^{m} b_{j,i} l_i \right) \\ &= \sum_{j=0}^{r} \sum_{k=1}^{n} \sum_{i=1}^{m} c_j a_{j,k} b_{j,i} g_k l_i \\ &= \sum_{k=1}^{n} \sum_{i=1}^{m} \left(\sum_{j=0}^{r} c_j a_{j,k} b_{j,i} \right) g_k l_i \end{aligned}$$

Avec, pour tout $k \in [\![1,n]\!]$ et $i \in [\![1,m]\!]$, $\sum_{j=0}^{r} c_j a_{j,k} b_{j,i} \in \mathbb{Z}$.

Donc la famille finie $(g_k l_i)_{\substack{1\leqslant k\leqslant n\\ 1\leqslant i\leqslant m}}$ est une famille génératrice de $G_{\alpha\beta}$.

D'après **les questions** $5.a$ **et** $5.b$ **de cette partie**, on déduit que $\alpha\beta \in \mathcal{D}_{\mathbb{C}}$.

Et pour tout $y \in G_{\alpha-\beta} := \mathrm{gr}\{(\alpha-\beta)^n | n \in \mathbb{N}\}$, on a l'existence de $c_0; \ldots; c_r \in \mathbb{Z}$ tel que

$$y = \sum_{j=0}^{r} c_j (\alpha-\beta)^j$$

On a alors

$$\begin{aligned}
y &= \sum_{j=0}^{r} c_j (\alpha-\beta)^j \\
&= \sum_{j=0}^{r}\sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j \alpha^{j-k}\beta^k \\
&= \sum_{j=0}^{r}\sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j \left(\sum_{i=1}^{n} a_{j-k,i} g_i\right)\left(\sum_{s=1}^{m} b_{k,s} l_s\right) \\
&= \sum_{j=0}^{r}\sum_{k=0}^{j}\sum_{i=1}^{n}\sum_{s=1}^{m} \binom{j}{k} c_j (-1)^j a_{j-k,i} b_{k,s} g_i l_s \\
&= \sum_{i=1}^{n}\sum_{s=1}^{m}\left(\sum_{j=0}^{r}\sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j a_{j-k,i} b_{k,s}\right) g_i l_s
\end{aligned}$$

Avec, pour tout $(i,s) \in [\![1,n]\!]\times[\![1,m]\!]$, on a $\sum_{j=0}^{r}\sum_{k=0}^{j} \binom{j}{k} c_j (-1)^j a_{j-k,i} b_{k,s} \in \mathbb{Z}$.

Alors, la famille finie $(g_i l_s)_{\substack{1\leqslant i\leqslant n\\ 1\leqslant s\leqslant m}}$ est génératrice de $G_{\alpha-\beta}$.

D'où, d'après ce qui précède, $\alpha-\beta \in \mathcal{D}_{\mathbb{C}}$.

Par suite, $\mathcal{D}_{\mathbb{C}}$ est un sous anneau de $\mathbb{C}$.

7. Montrons que $\mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$.

Tout d'abord pour tout $z \in \mathbb{Z}$, on a $X - z \in \mathbb{Z}[X]$ annule z, donc $z \in \mathcal{D}_{\mathbb{C}}$, et de plus $z \in \mathbb{Q}$.

Ainsi, $z \in \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q}$. Par suite, $\mathbb{Z} \subseteq \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q}$.

Réciproquement, pour tout $z \in \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q}$.

On a $X - z \in \mathbb{Q}[X]$ annule z. Donc $\pi_z | X - z$, avec $\deg(\pi_z) \geqslant 1$. Alors, $\pi_z = X - z$.

Or, z est un entier algébrique, donc

$$\pi_z = X - z \in \mathbb{Z}[X]$$

On en déduit que $z \in \mathbb{Z}$.

D'où $\mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} \subseteq \mathbb{Z}$.

Enfin, $\mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$.

III Le corps $\mathbb{Q}(\zeta)$ et son anneau d'entiers

1.a. Montrons que les morphismes de $\mathbb{Q}$-algébre de $\mathbb{Q}(\zeta)$ sont les σ_k, tels que $\sigma_k(\zeta) = \zeta^k$, pour tout $k \in \{1, \ldots, p-1\}$.

Puisque p est premier, donc $\pi_\zeta = \Phi_p$, dont les racines sont $\zeta, \zeta^2, \ldots, \zeta^{p-1}$.

D'après les questions **2.*a*** et 2.*b* **de la partie** $\mathbb{I}$, il existe exactement $(p-1)$ morphismes de $\mathbb{Q}$-algébre $\sigma_k : K = \mathbb{Q}(\zeta) \to \mathbb{C}$ tels que pour tout $k \in \{1, \ldots, p-1\}$, $\sigma_k(\zeta)$ soit racine de Φ_p et $\sigma_1(\zeta), \ldots, \sigma_{p-1}(\zeta)$ soient deux à deux distinctes.

Quitte à réordonner les $\sigma_1, \ldots, \sigma_{p-1}$. On conclut que les les morphismes de $\mathbb{Q}$-algèbre de $\mathbb{Q}(\zeta)$ sont les σ_k tels que $\sigma_k(\zeta) = \zeta^k$ pour tout $k \in \{1, 2, \ldots, p-1\}$.

1.b.i. On a

$$\begin{aligned} N(\zeta) &= \prod_{k=1}^{p-1} \sigma_k(\zeta) \\ &= \prod_{k=1}^{p-1} \zeta^k \\ &= \zeta^{p\frac{p-1}{2}} \\ &= \exp\left(2i\pi \frac{p-1}{2}\right) \end{aligned}$$

Avec p est impair, alors $\frac{p-1}{2} \in \mathbb{N}$, donc $N(\zeta) = 1$.

Et

$$\begin{aligned}\mathrm{Tr}(\zeta) &= \sum_{k=1}^{p-1}\sigma_k(\zeta)\\ &= \sum_{k=1}^{p-1}\zeta^k\\ &= \zeta\frac{1-\zeta^{p-1}}{1-\zeta}\\ &= \frac{\zeta-1}{1-\zeta}\\ &= -1\end{aligned}$$

1.b.ii. Montrons que $N(1-\zeta)=p$ et $N(1+\zeta)=1$

Notons

$$\begin{aligned}P &= \Phi_p(X+1)\\ &= \sum_{k=0}^{p-1}(X+1)^k\\ &= \frac{(X+1)^p-1}{(X+1)-1}\\ &= \sum_{k=1}^{p}\begin{pmatrix}p\\k\end{pmatrix}X^{k-1}\\ &= \sum_{k=0}^{p-1}\begin{pmatrix}p\\k+1\end{pmatrix}X^{k}\end{aligned}$$

Avec

$$P=\prod_{k=1}^{p-1}(X-(\zeta^k-1))$$

D'après les identités de Newton des polynômes symétriques, on a

$$(-1)^{p-1}\prod_{k=1}^{p-1}(\zeta^k-1)=\begin{pmatrix}p\\1\end{pmatrix}=p$$

Donc,

$$\prod_{k=1}^{p-1}(1-\zeta^k)=p$$

Ainsi,

$$\begin{aligned} N(1-\zeta) &= \prod_{k=1}^{p-1}(1-\sigma_k(\zeta)) \\ &= \prod_{k=1}^{p-1}(1-\zeta^k) \\ &= p \end{aligned}$$

Notons

$$Q = \Phi_p(X-1)$$

D'autre part, on a

$$\begin{aligned} Q &= \sum_{k=0}^{p-1}(X-1)^k \\ &= \sum_{k=0}^{p-1}\sum_{i=0}^{k}\begin{pmatrix} k \\ i \end{pmatrix}(-1)^{k-i}X^i \\ &= \sum_{i=0}^{p-1}\left[\sum_{k=i}^{p-1}\begin{pmatrix} k \\ i \end{pmatrix}(-1)^{k-i}\right]X^i \end{aligned}$$

Avec

$$Q = \prod_{k=1}^{p-1}(X-(\zeta^k+1))$$

Donc, d'après les identités de Newton, on a

$$\begin{aligned} (-1)^{p-1}\prod_{k=1}^{p-1}(\zeta^k+1) &= \sum_{k=0}^{p-1}\begin{pmatrix} k \\ 0 \end{pmatrix}(-1)^k \\ &= \sum_{k=0}^{p-1}(-1)^k \\ &= 1 \end{aligned}$$

Ainsi,

$$\begin{aligned} N(1+\zeta) &= \prod_{k=1}^{p-1}(\zeta^k+1) \\ &= 1 \end{aligned}$$

2. Montrons que $\mathbb{Z}[\zeta] \subseteq \mathcal{D}_K$

Soit $x \in \mathbb{Z}[\zeta]$,

Alors il existe $(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$, tel que $x = \sum_{k=0}^{n} a_k \zeta^k$.

Tout d'abord, remarquons que $x \in \mathbb{Q}(\zeta) = K$.

D'autre part, en utilisant la division euclidienne de $P = \sum_{k=0}^{n} a_k X^k$ par π_ζ, et la question 1 de la partie I, on a l'existence de $Q, R \in \mathbb{Z}[X]$ tels que

$$\begin{cases} P = Q\pi_\zeta + R \\ \deg(R) < \deg(\pi_\zeta) = \deg(\Phi_p) = p - 1 \end{cases}$$

En écrivant $R = \sum_{k=0}^{p-2} r_k X^k$ où $r_0, \dots, r_{p-2} \in \mathbb{Z}$

On a alors

$$\begin{aligned} x &= P(\zeta) \\ &= Q(\zeta)\pi_\zeta(\zeta) + R(\zeta) \\ &= \sum_{k=0}^{p-2} r_k \zeta^k \end{aligned}$$

Or, $\zeta \in \mathcal{D}_{\mathbb{C}}$ (car $\Phi_p \in \mathbb{Z}[X]$ annule ζ), et $\mathcal{D}_{\mathbb{C}}$ est un sous-anneau de $\mathbb{C}$.

Ainsi,

$$x = \sum_{k=0}^{p-2} r_k \zeta^k \in \mathcal{D}_{\mathbb{C}}$$

D'où

$$\mathbb{Z}[\zeta] \subseteq \mathcal{D}_{\mathbb{C}}$$

Ainsi,

$$\mathbb{Z}[\zeta] \subseteq \mathcal{D}_{\mathbb{C}} \cap K = \mathcal{D}_K$$

D'où le résultat.

3. Soit $z \in \mathbb{Z}[\zeta]$

3.a. Montrons que

$$z \in \mathbb{Z}[\zeta]^\times \text{ si and seulement si } N(z) \in \{-1, 1\}$$

$\Rightarrow$)Si $z \in \mathbb{Z}[\zeta]^\times$.

Alors, il existe $z' \in \mathbb{Z}[\zeta]$ tel que $z.z' = 1$.

Lemme 4.

Soit $\theta \in \mathbb{Z}[\zeta]$, si θ est un entier algébrique, alors $N(\theta) \in \mathbb{Z}$.

Preuve du lemme 4.

On a θ est un entier algébrique ; en particulier, il est algébrique sur $\mathbb{Q}$.

D'après **la question 3.b de la partie** $\mathbb{I}$, on a

$$P_\theta = \prod_{k=1}^{p-1}(X - \sigma_k(\theta)) \in \mathbb{Q}[X]$$

En particulier :

$$N(\theta) = \prod_{k=1}^{p-1}\sigma_k(\theta) \in \mathbb{Q}$$

En écrivant $\theta = P(\zeta)$, avec $P \in \mathbb{Z}[X]$, on obtient alors :

$$\begin{aligned} N(\theta) &= \prod_{k=1}^{p-1}\sigma_k(\theta) \\ &= \prod_{k=1}^{p-1}P(\zeta^k) \end{aligned}$$

Comme ζ est un entier algébrique, donc pour tout $k \in [\![1, p-1]\!]$, on a $P(\zeta^k)$ est un entier algébrique. D'où :

$$\prod_{k=1}^{p-1}P(\zeta^k) \in \mathcal{D}_{\mathbb{C}}$$

Ainsi :

$$\prod_{k=1}^{p-1}P(\zeta^k) \in \mathcal{D}_{\mathbb{C}} \cap \mathbb{Q} = \mathbb{Z}$$

D'où :

$$N(\theta) = \prod_{k=1}^{p-1}P(\zeta^k) \in \mathbb{Z}$$

Puisque $z.z' = 1$, alors :

$$N(z.z') = N(1) = \prod_{k=1}^{p-1}\sigma_k(1) = 1$$

Or,

$$\begin{aligned} N(z.z') &= \prod_{k=1}^{p-1} \sigma_k(z.z') \\ &= \prod_{k=1}^{p-1} \sigma_k(z)\sigma_k(z') \\ &= \left(\prod_{k=1}^{p-1} \sigma_k(z)\right)\left(\prod_{k=1}^{p-1} \sigma_k(z')\right) \\ &= N(z)N(z') \end{aligned}$$

Donc :

$$N(z)N(z') = 1$$

Avec $N(z), N(z') \in \mathbb{Z}$ (d'après le lemme 4), donc $N(z) \in \{-1, 1\}$.

$\Leftarrow$)Réciproquement, si $N(z) \in \{-1, 1\}$, alors

$$\begin{aligned} N(z) &= \prod_{k=1}^{p-1} \sigma_k\left(\sum_{j=0}^{n} a_j \zeta^j\right) \\ &= \prod_{k=1}^{p-1} \left(\sum_{j=0}^{n} a_j \sigma_k(\zeta)^j\right) \\ &= \prod_{k=1}^{p-1} \left(\sum_{j=0}^{n} a_j \zeta^{jk}\right) \\ &= \prod_{k=1}^{p-1} P(\zeta^k) \end{aligned}$$

D'où,

$$\prod_{k=1}^{p-1} P(\zeta^k) \in \{-1, 1\}$$

Ainsi,

$$z \times \prod_{k=2}^{p-1} P(\zeta^k) \in \{-1, 1\}$$

Avec $\prod_{k=2}^{p-1} P(\zeta^k) \in \mathbb{Z}[\zeta]$.
Donc $z \in \mathbb{Z}[\zeta]^\times$.
D'où l'équivalence.

3.b. Si $N(z)$ est un nombre premier.

Montrons que z est irréductible.

Soient $a, b \in \mathbb{Z}[\zeta]$ tels que $z = a.b$

On a alors :

$$\begin{aligned} N(z) &= N(ab) \\ &= N(a)N(b) \end{aligned}$$

D'après le lemme 4, on a

$$N(a), N(b) \in \mathbb{Z}$$

Or, $N(z)$ est un nombre premier.

Ainsi, $N(a) \in \{-1, 1\}$ ou $N(b) \in \{-1, 1\}$.

Via la question précédente, on en déduit que $a \in \mathbb{Z}[\zeta]^\times$ ou $b \in \mathbb{Z}[\zeta]^\times$.

Ainsi, z est irréductible de $\mathbb{Z}[\zeta]$.

4.a. Justifions que G est un groupe fini cyclique.

Par définition, G est l'ensemble des racines de l'unité contenues dans K, où Kest un corps. Alors $1 \in G$.

Soient z, z' deux racines de l'unité dans K, Puisque K est un corps, alors $z \times \frac{1}{z'}$ est également une racine de l'unité contenue dans K.

Ainsi

$$z \times \frac{1}{z'} \in G$$

Cela prouve que G est un groupe.

De plus, $K/\mathbb{Q}$ est une extension finie. D'après la question **1.b de la partie 2**, on a K contient un nombre fini de racines de l'unité.

Donc, G est un groupe fini ; notons $n = \#G$.

On a alors, pour tout $z \in G$, $z^n = 1$.

Ainsi, G est un sous-groupe de $(\mathbb{U}_n, \times)$, qui est monogène. Par conséquent, G est également monogène.

On en déduit que G est cyclique.

D'où le résultat.

4.b. Soit ω un générateur de G. Justifions que $2p|n$et que$\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)$.

On a $\omega \in G$, donc $|w| = 1$, et il existe $a_0, \ldots, a_{p-1} \in \mathbb{Q}$ tels que

$$\omega = \sum_{k=0}^{p-1} a_k \zeta^k$$

On a alors

$$\begin{aligned}
\omega^p &= \left(\sum_{k=0}^{p-1} a_k \zeta^k\right)^p \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \prod_{k=0}^{p-1} a_{i_k} \zeta^{i_k} \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \prod_{k=0}^{p-1} a_{i_k} \zeta^{i_k} \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \left(\prod_{k=0}^{p-1} a_{i_k}\right) \zeta^{i_0+\cdots+i_{p-1}} \\
&= \sum_{i_0+\cdots+i_{p-1}=p} \left(\prod_{k=0}^{p-1} a_{i_k}\right) \\
&\in \mathbb{R}
\end{aligned}$$

Ainsi, $\omega^p \in \mathbb{R}$ et $|\omega^p| = 1$, donc $\omega^p = \pm 1$, ce qui entraîne que $\omega^{2p} = 1$.

Par conséquent, $2p|n$.

Montrons maintenant que $\mathbb{Q}(\omega) = \mathbb{Q}(\zeta)$.

On a $\omega \in \mathbb{Q}(\zeta)$, donc $\mathbb{Q}(\omega) \subset \mathbb{Q}(\zeta)$.

Or, $\zeta \in G =< \omega >$, donc il existe $k \in \mathbb{N}$, tel que $\zeta = \omega^k \in \mathbb{Q}(\omega)$.

Ainsi, $\mathbb{Q}(\zeta) \subset \mathbb{Q}(\omega)$

On en déduit donc que

$$\mathbb{Q}(\zeta) = \mathbb{Q}(\omega)$$

4.c. Montrons que $2p = n$.

On a forcément $G = \mathbb{U}_n$, ce qu'on va justifier dans un premier temps.

On a $\text{ord}(G) = n$, donc pour tout $g \in G$, on a $g^n = 1$, ce qui implique $G \subset \mathbb{U}_n$.

Or,

$$\text{card}(G) = \text{card}(\mathbb{U}_n) = n < +\infty$$

D'où,

$$G = \mathbb{U}_n$$

Avant de continuer, montrons un lemme :

Lemme 5.

Soit $z \in \mathbb{C}$, on a alors

$$[\mathbb{Q}(z) : \mathbb{Q}] = \deg(\pi_z)$$

Preuve du lemme 5.

Soit $z \in \mathbb{C}$, rappelons que π_z est irréductible de $\mathbb{Q}[X]$.

Soit $x \in \mathbb{Q}(z)$, alors il existe $a_0, \ldots, a_r \in \mathbb{Q}$ tels que

$$x = \sum_{j=0}^{n} a_j z^j$$

Par division euclidienne de $P = \sum\limits_{j=0}^{n} a_j X^j$ par Φ_z, on a l'existence de $(Q, R) \in \mathbb{Q}[X]^2$ tel que

$$P = Q\pi_z + R$$

Alors

$$\begin{aligned} x &= P(z) \\ &= Q(z)\pi_z(z) + R(z) \\ &= R(z) \\ &\in \operatorname{vect}_{\mathbb{Q}}(1, z, \ldots, z^{\deg(\pi_z)-1}) \end{aligned}$$

Ainsi, $(1, z, \ldots, z^{\deg(\pi_z)-1})$ est génératrice de $\mathbb{Q} -$ espace vectoriel $\mathbb{Q}(z)$.

Montrons que cette famille est $\mathbb{Q}-$libre.

Pour cela, considérons $b_0, \ldots, b_{\deg(\pi_z)-1} \in \mathbb{Q}$, tels que

$$\sum_{k=0}^{\deg(\pi_z)-1} b_k z^k = 0$$

Alors, π_z divise $\sum\limits_{k=0}^{\deg(\pi_z)-1} b_k z^k$, donc

$$\begin{aligned} \deg(\pi_z) &\leqslant \deg\left(\sum_{k=0}^{\deg(\pi_z)-1} b_k z^k\right) \\ &= \deg(\pi_z) - 1 \end{aligned}$$

absurde !

D'où, $(1, z, \dots, z^{\deg(\pi_z)-1})$ est $\mathbb{Q}$-libre.

Ensuite, $(1, z, \dots, z^{\deg(\pi_z)-1})$ est une base de $\mathbb{Q}(z)$ en tant que $\mathbb{Q}$-espace vectoriel.

Ainsi,

$$\begin{aligned}[\mathbb{Q}(z) : \mathbb{Q}] &= \#\{1, z, \dots, z^{\deg(\pi_z)-1}\} \\ &= \deg(\pi_z)\end{aligned}$$

D'où le résultat.

On a ω est un générateur de G, donc ω est une racine primitive de n.

En utilisant le lemme précédent, on a

$$\begin{aligned}[\mathbb{Q}(\omega) : \mathbb{Q}] &= \deg(\pi_\omega) \\ &= \deg(\Phi_n) \\ &= \varphi(n)\end{aligned}$$

Or, d'après la question précédente, on a $2p|n$, donc il existe $k \in \mathbb{N}^*$ tel que $n = 2kp$.

Si k s'écrit sous la forme $k = 2^a p^b$, où $a, b \in \mathbb{N}$ non tous nuls. On a alors

$$\begin{aligned}\varphi(n) &= \varphi(2^{a+1}p^{b+1}) \\ &= 2^{a+1}p^{b+1}\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p}\right) \\ &= 2^a p^b (p-1) \\ &\geqslant \min(2(p-1), p(p-1)) \\ &> p\end{aligned}$$

Donc

$$\begin{aligned}p &= [\mathbb{Q}(\zeta) : Q] \\ &= [\mathbb{Q}(\omega) : \mathbb{Q}] \\ &= \varphi(n) \\ &> p\end{aligned}$$

ce qui est absurde !

Sinon, si k est de la forme

$$k = 2^a p^b \prod_{i=1}^{l} p_i^{y_i}$$

où $a, b \in \mathbb{N}$ et $y_1, \ldots, y_l > 1$, et $p_1, \ldots, p_l \geqslant 3$. On a alors

$$\begin{aligned}
p &= [\mathbb{Q}(\zeta) : \mathbb{Q}] \\
&= [\mathbb{Q}(\omega) : \mathbb{Q}] \\
&= \varphi(n) \\
&= \varphi\left(2^{a+1} p^{b+1} \prod_{i=1}^{l} p_i^{y_i}\right) \\
&= 2^{a+1} p^{b+1} \prod_{i=1}^{l} p_i^{y_i} \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{p}\right) \prod_{i=1}^{l} \left(1 - \frac{1}{p_i}\right) \\
&= 2^a p^b \prod_{i=1}^{l} p_i^{y_i - 1}(p_i - 1)(p - 1) \\
&\geqslant 2(p-1) \\
&> p
\end{aligned}$$

absurde !

D'où $k = 1$, par suite $n = 2p$.

Ainsi,

$$\begin{aligned}
G &= \mathbb{U}_{2p} \\
&= \left\{ \exp\left(\frac{2ik\pi}{2p}\right) / k \in [\![0, 2p-1]\!] \right\} \\
&= \{\pm \zeta^k / k \in [\![0, p-1]\!]\}
\end{aligned}$$

D'où le résultat.

5.a. Montrons que

$$< \lambda > \cap \mathbb{Z} = p\mathbb{Z}$$

On a

$$< \lambda >= \lambda \mathbb{Z}[\zeta]$$

Avec $0 = \lambda \times 0 \in \lambda\mathbb{Z}[\zeta] =< \lambda >$. Donc $< \lambda > \neq \emptyset$.

De plus, pour tout $x, y \in < \lambda >$, on a l'existence de $P, Q \in \mathbb{Z}[X]$ tels que $x = \lambda P(\zeta)$ et $y = \lambda Q(\zeta)$.

Donc

$$\begin{aligned} x - y &= \lambda(P - Q)(\zeta) \\ &\in \lambda\mathbb{Z}[\zeta] \\ &= < \lambda > \end{aligned}$$

Ainsi, $< \lambda >$ est un sous-groupe de $\mathbb{C}$.

Comme $\mathbb{Z}$ est un sous-groupe de $\mathbb{C}$, donc l'intersection $< \lambda > \cap \mathbb{Z}$ est un sous-groupe de $\mathbb{C}$.

Étant donné que $< \lambda > \cap \mathbb{Z} \subseteq \mathbb{Z}$, alors $< \lambda > \cap \mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Il existe donc $n \in \mathbb{N}$ tel que

$$< \lambda > \cap \mathbb{Z} = n\mathbb{Z}$$

Or, d'après la question $b.\,\mathrm{ii}\,.$ de cette partie, on a

$$\begin{aligned} p &= N(\lambda) \\ &= N(1 - \zeta) \\ &= \prod_{k=1}^{p-1} \sigma_k(1 - \zeta) \\ &= \prod_{k=1}^{p-1} (1 - \zeta^k) \\ &= \lambda \prod_{k=2}^{p-1} (1 - \zeta^k) \end{aligned}$$

Avec $\prod_{k=2}^{p-1} (1 - \zeta^k) \in \mathbb{Z}[\zeta]$

Donc

$$p \in < \lambda > \cap \mathbb{Z} = n\mathbb{Z}$$

En particulier, $n \neq 0$.

De plus $p \in n\mathbb{Z}$, il existe donc $r \in \mathbb{N}$ tel que $p = nr$.

Puisque p est premier, alors $n = 1$ ou $n = p$.

Si $n = 1$, donc $< \lambda > \cap \mathbb{Z} = \mathbb{Z}$.

En particulier $1 \in < \lambda >$.

Donc, il existe $x \in \mathbb{Z}[\zeta]$ tel que

$$1 = \lambda x$$

Cela impliquerait que $\lambda \in \mathbb{Z}[\zeta]^\times$, ce qui est absurde car $N(\lambda) = p \notin \{-1, 1\}$.

Donc $n = p$.

En conclusion,

$$< \lambda > \cap \mathbb{Z} = p\mathbb{Z}$$

5.b. Soit $K \in \{1, 2, \ldots, p-1\}$. Montrons que

$$\frac{1-\zeta}{1-\zeta^k} \in \mathbb{Z}[\zeta]^\times$$

Méthode 1.

On a

$$\frac{1-\zeta^k}{1-\zeta} = \sum_{j=0}^{k-1} \zeta^j \in \mathbb{Z}[\zeta]$$

Et

$$\begin{aligned} N\left(\frac{1-\zeta^k}{1-\zeta}\right) &= N\left(\sum_{j=0}^{k-1} \zeta^j\right) \\ &= \prod_{l=1}^{p-1} \sigma_l \left(\sum_{j=0}^{k-1} \zeta^j\right) \\ &= \prod_{l=1}^{p-1} \left(\sum_{j=0}^{k-1} \sigma_l(\zeta)^j\right) \\ &= \prod_{l=1}^{p-1} \left(\sum_{j=0}^{k-1} \zeta^{jl}\right) \\ &= \prod_{l=1}^{p-1} \left(\frac{1-\zeta^{kl}}{1-\zeta^l}\right) \end{aligned}$$

Pour tous $k, l \in [\![1, p-1]\!]$, notons $r_{k,l}$ l'unique entier dans $[\![0, p-1]\!]$ qui représente le reste de la division euclidienne de kl par p.

On a pour tout $k, l \in [\![1, p-1]\!]$:

$$k \wedge p = 1 \text{ and } l \wedge p = 1$$

Donc $kl \wedge p = 1$, ainsi $r_{kl} \in [\![1, p-1]\!]$

Donc l'application

$$l \in [\![1, p-1]\!] \quad \longmapsto \quad r_{k,l} \in [\![1, p-1]\!]$$

est bien définie. De plus, pour tous $l, l' \in [\![1, p-1]\!]$, si $r_{k,l} = r_{k,l'}$, alors

$$k(l - l') \text{ est divisible par } p$$

Avec $p \wedge k = 1$, on en déduit via le lemme de Gauss que

$$P | l - l'$$

Donc, il existe $s \in \mathbb{Z}$ tel que $l - l' = s.p$.

Or,

$$-(p-1) \leqslant l - l' \leqslant p - 1$$

Donc,

$$-\frac{p-1}{p} \leqslant s \leqslant \frac{p-1}{p}$$

Ainsi, $s = 0$, par suite $l = l'$. D'où l'application $l \in [\![1, p-1]\!] \quad \longmapsto \quad r_{k,l} \in [\![1, p-1]\!]$ est injective, donc elle est bijective.

D'où,

$$\begin{aligned} \prod_{l=1}^{p-1} (1 - \zeta^{kl}) &= \prod_{l=1}^{p-1} (1 - \zeta^{r_{k,l}}) \\ &= \prod_{l=1}^{p-1} (1 - \zeta^{l}) \end{aligned}$$

D'où,

$$\begin{aligned} N\left(\frac{1-\zeta^k}{1-\zeta}\right) &= \frac{\prod_{l=1}^{p-1} (1 - \zeta^{l})}{\prod_{l=1}^{p-1} (1 - \zeta^{l})} \\ &= 1 \end{aligned}$$

Finalement,

$$\frac{1-\zeta^k}{1-\zeta} \in \mathbb{Z}[\zeta]^\times$$

D'où

$$\frac{1-\zeta}{1-\zeta^k} = \frac{1}{\frac{1-\zeta^k}{1-\zeta}} \in \mathbb{Z}[\zeta]^\times$$

Méthode 2.

On a $p \wedge k = 1$, donc d'après le théorème de Bézout, il existe $n_0, m_0 \in \mathbb{Z}$ tel que

$$pn_0 + km_0 = 1$$

Donc, pour tout $\alpha \in \mathbb{Z}$

$$p(n_0 - \alpha k) + k(m_0 + \alpha p) = 1$$

Avec $\lim\limits_{\alpha \to +\infty} m_0 + \alpha p = +\infty$, alors il existe $\alpha_0 \in \mathbb{N}$ tel que

$$m_0 + \alpha_0 p > 0$$

Pour ce $\alpha_0 \in \mathbb{N}$, on a

$$\begin{aligned}
\frac{1-\zeta}{1-\zeta^k} &= \frac{1-\zeta^{1-p(n_0-\alpha_0 k)}}{1-\zeta^k} \\
&= \frac{1-\left(\zeta^k\right)^{m_0+\alpha_0 p}}{1-\zeta^k} \\
&= \sum_{j=0}^{m_0+\alpha_0 p-1} \zeta^{kj} \\
&\in \mathbb{Z}[\zeta]
\end{aligned}$$

D'autre part,

$$\begin{aligned}
\frac{1}{\frac{1-\zeta}{1-\zeta^k}} &= \frac{1-\zeta^k}{1-\zeta} \\
&= \sum_{j=0}^{k-1} \zeta^j \\
&\in \mathbb{Z}[\zeta]
\end{aligned}$$

Donc, par définition,

$$\frac{1-\zeta}{1-\zeta^k} \in \mathbb{Z}[\zeta]^\times$$

Montrons que

$$\lambda^{p-1}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta]$$

Soit $x \in p\mathbb{Z}[\zeta]$, donc il existe $P \in \mathbb{Z}[X]$ tel que $x = pP(\zeta)$.
Donc

$$\begin{aligned} x &= N(1-\zeta)P(\zeta) \\ &= \prod_{k=1}^{p-1} \sigma_k(1-\zeta)P(\zeta) \\ &= \prod_{k=1}^{p-1} (1-\zeta^k)P(\zeta) \\ &= \prod_{k=1}^{p-1} \left[(1-\zeta)\left(\sum_{j=0}^{k-1}\zeta^j\right)\right] P(\zeta) \\ &= (1-\zeta)^{p-1}\left[\prod_{k=1}^{p-1}\left(\sum_{j=0}^{k-1}\zeta^j\right)\right] P(\zeta) \\ &\in \lambda^{p-1}\mathbb{Z}[\zeta] \end{aligned}$$

D'où

$$p\mathbb{Z}[\zeta] \subset \lambda^{p-1}\mathbb{Z}[\zeta]$$

Réciproquement, on a

$$\begin{aligned} \lambda^{p-1} &= (1-\zeta)^{p-1} \\ &= \prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right)\prod_{k=1}^{p-1}(1-\zeta^k) \\ &= N(1-\zeta)\prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right) \\ &= p\prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right) \end{aligned}$$

Avec $\frac{1-\zeta}{1-\zeta^k} \in \mathbb{Z}[\zeta]^\times$ pour tout $k \in [\![1, p-1]\!]$.
Donc,

$$\prod_{k=1}^{p-1}\left(\frac{1-\zeta}{1-\zeta^k}\right) \in \mathbb{Z}[\zeta]^\times$$

D'où,

$$\lambda^{p-1} \in p\mathbb{Z}[\zeta]$$

Ainsi,

$$\lambda^{p-1}\mathbb{Z}[\zeta] \subset p\mathbb{Z}[\zeta]$$

Enfin,

$$\lambda^{p-1}\mathbb{Z}[\zeta] = p\mathbb{Z}[\zeta]$$

5.c. Soit Ψ : le morphisme d'anneaux de $\mathbb{Z}[X] \to \mathbb{Z}[\zeta]/ < \lambda >$.
Soit $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$.
On a, pour tout $k \in [\![0, n]\!]$:

$$\begin{aligned}
\zeta^k &= (\zeta - 1 + 1)^k \\
&= (1-\lambda)^k \\
&= \sum_{j=0}^{k} (-1)^j \binom{k}{j} \lambda^j \\
&= 1 + \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^j
\end{aligned}$$

Donc,

$$\begin{aligned}
P(\zeta) &= \sum_{k=0}^{n} a_k \zeta^k \\
&= \sum_{k=0}^{n} a_k \left(1 + \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^j\right) \\
&= \sum_{k=0}^{n} a_k + \lambda \sum_{k=0}^{n} a_k \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^{j-1}
\end{aligned}$$

Avec, $\sum_{k=0}^{n} a_k \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^{j-1} \in \mathbb{Z}[\zeta]$.
Donc,

$$\sum_{k=0}^{n} a_k \sum_{j=1}^{k} (-1)^j \binom{k}{j} \lambda^{j-1} \in < \lambda >$$

Et donc,

$$\begin{aligned}
P(\zeta) &= \sum_{k=0}^{n} a_k (\text{mod} < \lambda >) \\
&= P(1) (\text{mod} < \lambda >)
\end{aligned}$$

Par division euclidienne de $P(1)$ par p, on a l'existence de $q, r \in \mathbb{N}$ tels que

$$\begin{cases} P(1) = pq + r \\ r \in [\![0, p-1]\!] \end{cases}$$

Or, $p \in p\mathbb{Z}[\zeta]$, donc $p \in \lambda^{p-1}\mathbb{Z}[\zeta]$.

Donc, il existe $Q \in \mathbb{Z}[X]$ tel que $p = \lambda^{p-1}Q(\zeta)$.

Ainsi,

$$\begin{aligned} p &= \lambda(1-\zeta)^{p-2}Q(\zeta) \\ &= \lambda[(1-X)^{p-2}Q]|_{X=\zeta} \\ &= 0(\text{mod} < \lambda >) \end{aligned}$$

Donc,

$$P(1) = r(\text{mod} < \lambda >)$$

Ainsi,

$$\Psi(P) = r(\text{mod} < \lambda >)$$

D'où,

$$\Psi(P) = P(1)(\text{mod}\, p\mathbb{Z})$$

Donc l'image de P par Ψ est le reste de la division euclidienne de $P(1)$par p.

Soit $P \in \text{Ker}(\Psi)$, alors d'après ce qui précède, le reste de la division euclidienne de $P(1)$par p est nul.

Donc,

$$P(1) = 0(\text{mod}\, p\mathbb{Z})$$

Réciproquement, si $P \in \mathbb{Z}[X]$ tel que $P(1) = 0(\text{mod}\, p\mathbb{Z})$.

Alors, d'après ce qui précède, on a

$$\begin{aligned} \Psi(P) &= 0(\text{mod}\, p\mathbb{Z}) \\ &= 0(\text{mod} < \lambda >) \end{aligned}$$

D'où $P \in \text{Ker}(\Psi)$

D'où le résultat.

5.d. D'après ce qui précède, $\text{Im}(\Psi)$ est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Donc $\mathbb{Z}[\zeta]/ < \lambda >$ est isomorphe à $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

5.e. Puisque $\mathbb{Z}[\zeta]/ < \lambda >$ est isomorphe à $\mathbb{F}_p$, et que p est un nombre premier.

Alors l'idéal $< \lambda >$ est premier, comme étant un idéal de l'anneau $\mathbb{Z}[\zeta]$.

6.a. Soit $P = \sum_{k=0}^{d} a_k X^k$ un polynôme unitaire de degré d, dont on note $\alpha_1, ..., \alpha_d$ les racines complexes comptées avec leur multiplicité. On suppose que pour tout $k \in \{1, ..., d\}$, α_k est de module 1.

6.a.i. Soit $k \in [\![0, d]\!]$, montrons que

$$|a_k| \leqslant \begin{pmatrix} d \\ k \end{pmatrix}$$

On a, d'après les identités de Newton

$$a_k = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \prod_{j=1}^{k} \alpha_{i_j}$$

Donc

$$\begin{aligned} |a_k| &\leqslant \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} \left| \prod_{j=1}^{k} \alpha_{i_j} \right| \\ &= \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant d} 1 \\ &= \begin{pmatrix} d \\ k \end{pmatrix} \end{aligned}$$

Notons

$$\mathcal{E}_d = \{z \in \mathcal{D}_{\mathbb{C}} | \deg(\pi_z) = d, \text{ and les conjugés de } z \text{ sont tous de module } 1\}$$

et

$$\mathcal{O}_d = \{P \in \mathbb{Z}[X] | P \text{ de degré } d \text{ dont toutes les racines sont de module } 1\}$$

On a

$$\mathcal{E}_d \subset \bigcup_{P \in \mathcal{O}_d} P^{-1}(\{0\})$$

Or, un polynôme de degré d admet au plus d racines distincts dans $\mathbb{C}$.

Donc, pour tout $P \in \mathcal{O}_d$, on a

$$\#P^{-1}(\{0\}) \leqslant d$$

De plus

$$\mathcal{O}_d \subset \left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] | \forall k \in [\![0,d]\!], a_k \leqslant \left(\begin{array}{c} d \\ k \end{array} \right) \right\}$$

Et la famille

$$\left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] | \forall k \in [\![0,d]\!], a_k \leqslant \left(\begin{array}{c} d \\ k \end{array} \right) \right\}$$

est en bijection avec $\left\{ (a_0, \ldots, a_d) \in \mathbb{Z}^d | \forall k \in [\![0,d]\!], a_k \leqslant \left(\begin{array}{c} d \\ k \end{array} \right) \right\}$

Comme cet ensemble est fini, cela implique que

$$\left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] | \forall k \in [\![0,d]\!], a_k \leqslant \left(\begin{array}{c} d \\ k \end{array} \right) \right\}$$

est fini aussi. Ainsi $\mathcal{O}_d$ est fini.

Par suite,

$$\begin{array}{rcl} \#\mathcal{E}_d & \leqslant & \# \bigcup_{P \in \mathcal{O}_d} P^{-1}(\{0\}) \\ & \leqslant & d \times \#\mathcal{O}_d \\ & \leqslant & d \times \# \left\{ \sum_{k=0}^{d} a_k X^k \in \mathbb{Z}[X] | \forall k \in [\![0,d]\!], a_k \leqslant \left(\begin{array}{c} d \\ k \end{array} \right) \right\} \\ & = & d \prod_{k=0}^{d} \left(2 \left(\begin{array}{c} d \\ k \end{array} \right) + 1 \right) \\ & < & +\infty \end{array}$$

D'où le résultat.

6.a.ii. On a $X^n \in \mathbb{Z}[X]$, et $P \in \mathbb{Z}[X]$ est un polynôme unitaire de degré d, dont on note $\alpha_1, ..., \alpha_d$ les racines complexes comptées avec leur multiplicité. Avec, $\mathbb{Z}$ est un sous-anneau de $\mathbb{C}$.

D'après **la question 4.e de la partie** I, on a pour tout $n \in \mathbb{N}$

$$P_n = \prod_{k=1}^{d} (X - \alpha_k^n) \in \mathbb{Z}[X]$$

Avec pour tout $(n, d) \in \mathbb{N} \times [\![1, d]\!]$, on a $|\alpha_k^n| = 1$, En utilisant les mêmes notations que précédemment, on a, pour tout $k \in [\![1, d]\!]$, et pour tout $n \in \mathbb{N}$

$$\alpha_k^n \in \mathcal{E}_d$$

où $\mathcal{E}_d$ est fini. Donc il existe $n_0, n_1 \in \mathbb{N}$, tels que $n_0 < n_1$ et $\alpha_k^{n_0} = \alpha_k^{n_1}$.

Avec $\alpha_k \neq 0$, donc

$$\alpha_k^{n_1 - n_0} = 1$$

On en déduit que α_k est un racine de l'unité

D'où le résultat.

6.b. Soit $P \in \mathbb{Z}[X]$ tel que $u = P(\zeta)$. Montrons que, pour tout $k \in \{1, ..., p1\}$, $u_k = P(\zeta^k)$ est un conjugué de u et que c'est un élément de $\mathbb{Z}[\zeta]^\times$.

On a, en utilisant les mêmes notations de la partie $\mathbb{I}$.

$$\begin{aligned}
\prod_{k=1}^{p-1} (X - P(\zeta^k)) &= \prod_{k=1}^{p-1} (X - P(\sigma_k(\zeta))) \\
&= \prod_{k=1}^{p-1} (X - \sigma_k(P(\zeta))) \\
&= \prod_{k=1}^{p-1} (X - \sigma_k(u)) \\
&= P_u
\end{aligned}$$

D'après la **question 3.c de la partie** $\mathbb{I}$, on a P_u est une puissance de π_u.

Donc, pour tout $k \in \{1, ..., p1\}$, $u_k = P(\zeta^k)$ est un conjugué de u.

De plus $u = P(\zeta) \in \mathbb{Z}[\zeta]^\times$.

Ainsi, d'après la **question 3.a de cette partie**, on a :

$$N(u) \in \{-1, 1\}$$

Donc, pour tout $k \in \{1, 2, \ldots, p-1\}$, on a :

$$\begin{aligned} u_k \prod_{\substack{j=1 \\ j\neq k}}^{p-1} P(\zeta^j) &= \prod_{j=1}^{p-1} P(\zeta^j) \\ &= \prod_{j=1}^{p-1} \sigma_j(P(\zeta)) \\ &= \prod_{j=1}^{p-1} \sigma_j(u) \\ &= N(u) \\ &\in \{-1, 1\} \end{aligned}$$

Avec $\prod_{\substack{j=1 \\ j\neq k}}^{p-1} P(\zeta^j) \in Z[\zeta]$, donc par définition

$$u_k \in \mathbb{Z}[\zeta]^\times$$

6.c. Justifions que $\frac{u_p}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.

Soit $k \in [\![1, p-1]\!]$,

On a :

$$\begin{aligned} u_{p-k} &= P(\zeta^{p-k}) \\ &= P(\zeta^{-k}) \\ &= \overline{P(\zeta)} \\ &= \overline{u_k} \end{aligned}$$

Donc $\left|\frac{u_k}{u_{p-k}}\right| = 1$.

Or, $\frac{u_1}{u_{p-1}} \in \mathbb{Z}[\zeta]^\times \subset \mathfrak{D}_K$, et ses conjugués sont donnés par :

$$\begin{aligned} \sigma_k\left(\frac{u_1}{u_{p-1}}\right) &= \frac{\sigma_k(u_{k1})}{\sigma_k(u_{p-1})} \\ &= \frac{u_k}{P(\sigma_k(\zeta^{-1}))} \\ &= \frac{u_k}{u_{p-k}} \end{aligned}$$

D'où le résultat.

6.d. En déduire qu'il existe$m \in \mathbb{Z}$ tel que $\frac{u_1}{u_{p-1}} = \pm\zeta^m$.

En utilisant la question 6.a.ii, on a $\frac{u}{u_{p-1}}$ est une racine de l'unité de K.

Ainsi, il existe $m \in \mathbb{Z}$ tel que $\frac{u}{u_{p-1}} = \pm\zeta^m$ (cf. question 4 de la partie 3).

6.e.i. Soit $\theta \in \mathbb{Z}[\zeta]$. Justifions qu'il existe un entier $a \in \mathbb{Z}$ tel que $\theta = a(\mathrm{mod} < \lambda >)$.

On a $\theta \in \mathbb{Z}[\zeta]$, donc il existe des entiers $a_0, \ldots, a_{p-2}$ tels que

$$\theta = \sum_{k=0}^{p-2} a_k \zeta^k$$

Ainsi,

$$\begin{aligned} \theta &= \sum_{k=0}^{p-2} a_k(\zeta^k - 1) + \sum_{k=0}^{p-2} a_k \\ &= \lambda \sum_{k=0}^{p-2} a_k \sum_{j=0}^{k-1} \zeta^j + \sum_{k=0}^{p-2} a_k \\ &= \sum_{k=0}^{p-2} a_k (\mathrm{mod} < \lambda >) \end{aligned}$$

On a donc $\theta = a(\mathrm{mod} < \lambda >)$, où $a = \sum_{k=0}^{p-2} a_k \in \mathbb{Z}$.

En déduire que deux éléments conjugués de $\mathbb{Z}[\zeta]$ sont égaux modulo $< \lambda >$.

Soit $\theta = \sum_{k=0}^{p-2} a_k \zeta^k \in \mathbb{Z}[\zeta]$, et $\sigma_j(\theta) = \sum_{k=0}^{p-2} a_k \zeta^{jk}$ un des conjugués de θ, où $k \in [\![0, p-1]\!]$.

On a

$$\begin{aligned} \theta - \sigma_j(\theta) &= \sum_{k=0}^{p-2} a_k(\zeta^k - \zeta^{jk}) \\ &= \lambda \sum_{k=0}^{p-2} a_k \zeta^k \sum_{l=0}^{jk-k-1} \zeta l \\ &= 0(\mathrm{mod} < \lambda >) \end{aligned}$$

D'où le résultat.

6.e.ii. Montrons que $\frac{u_1}{u_{p-1}} = \zeta^m$.

On a $\frac{u_1}{u_{p-1}} = \pm\zeta^m$. Par l'absurde, supposons que $\frac{u_1}{u_{p-1}} = -\zeta^m$.

Alors

$$\begin{aligned} u &= -\zeta^m u_{p-1} \\ &= -u_{p-1}(\text{mod} < \lambda >) \end{aligned}$$

De plus, u et u_{p-1}sont conjugués, donc d'après la question précédente, on a

$$u = u_{p-1}(\text{mod} < \lambda >)$$

Donc

$$2u = 0(\text{mod} < \lambda >)$$

Ainsi, $2u \in < \lambda >$, avec $< \lambda >$ est premier.

Donc, $2 \in < \lambda >$ ou $u \in < \lambda >$.

Si $2 \in < \lambda >$, alors

$$N(\lambda)|N(2) = 2^{p-1}$$

Ainsi, $p|2^{p-1}$, absurde !

Donc $u \in < \lambda >$

Ainsi,

$$p = N(\lambda)|N(u) = 1$$

Absurde !

D'où le résultat.

Remarque.

On peut répondre directement à la question **6.e.ii** sans faire les questions **6.c, 6.d** et **6.e.i**.

En justifiant que $\frac{u_1}{u_{p-1}}$ est un entier algébrique dont tous les conjugués sont de module 1.

D'après la question précécente, on a

$$u_1, u_{p-1} \in \mathbb{Z}[\zeta]^\times$$

Donc

$$u_1, \frac{1}{u_{p-1}} \in \mathbb{Z}[\zeta]$$

D'après la question 2, on sait que $\mathbb{Z}[\zeta] \subseteq \mathcal{D}_K \subseteq D_{\mathbb{C}}$, où $\mathcal{D}_{\mathbb{C}}$ est un anneau (d'après la **question 6 de la partie** $\mathbb{I}$).

Ainsi,

$$\frac{u_1}{u_{p-1}} = u_1 \times \frac{1}{u_{p-1}} \in \mathcal{D}_{\mathbb{C}}$$

Autrement dit, $\frac{u_1}{u_{p-1}}$ est un entier algébrique.

Il ne reste qu'à montrer que tous les conjugués de $\frac{u_1}{u_{p-1}}$sont de module 1. En s'inspirant des questions **6.a.i** et **6.a.ii** de cette partie, il est préférable (étant donné que $\frac{u_1}{u_{p-1}}$ est un entier algébrique) de montrer que $\frac{u_1}{u_{p-1}}$ est une racine de l'unité.(Ce faisant, on répond également à la deuxième partie de cette question).

Notons,

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

D'après la formule multinôme, on a :

$$\begin{aligned}
u_{p-1}^p &= P(\zeta^{p-1})^p \\
&= P\left(\frac{1}{\zeta}\right)^p \\
&= \left(\sum_{k=0}^{n} a_k \zeta^{-k}\right)^p \\
&= \sum_{i_1+\cdots+i_n=p} \prod_{k=0}^{n} a_{i_k} \zeta^{-i_k} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{-(i_1+\cdots+i_n)} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{-p} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{p} \\
&= \sum_{i_1+\cdots+i_n=p} \left(\prod_{k=0}^{n} a_{i_k}\right) \zeta^{i_1+\cdots+i_n} \\
&= \sum_{i_1+\cdots+i_n=p} \prod_{k=0}^{n} a_{i_k} \zeta^{i_k} \\
&= \left(\sum_{k=0}^{n} a_k \zeta^{k}\right)^p \\
&= P(\zeta)^p \\
&= u_1^p
\end{aligned}$$

Donc :

$$\left(\frac{u_1}{u_{p-1}}\right)^p = 1$$

Ainsi, il existe $m \in \mathbb{Z}$ tel que :

$$\frac{u_1}{u_{p-1}} = \zeta^m$$

D'où le résultat.

6.f. Justifions l'existence de $r \in \mathbb{Z}$ tel que $2r = m (\mathrm{mod}\, p\mathbb{Z})$.

D'après le théorème de Fermat :

$$2^{p-1} = 1(\mathrm{mod}\, p\mathbb{Z})$$

Ainsi, pour $r = m2^{p-1}$, on a $r = m(\mathrm{mod}\, p\mathbb{Z})$.

On pose $\varepsilon = \zeta^{-r}u$. Montrons que $\varepsilon \in \mathbb{R}$.

On a [4]

$$\begin{aligned}
\bar{\varepsilon} &= \zeta^r \bar{u} \\
&= \zeta^r u_{p-1} \\
&= \zeta^r(\zeta^{-m}u) \\
&= \zeta^r(\zeta^{-2r}u) \\
&= \zeta^{-r}u \\
&= \varepsilon
\end{aligned}$$

D'où $\varepsilon \in \mathbb{R}$.

Puisque $u, \zeta^{-r} \in \mathbb{Z}[\zeta]^\times$, alors $\varepsilon \in \mathbb{Z}[\zeta]^\times$.

Ainsi, $u = \zeta^r\varepsilon$, où ε est un réel dans $\mathbb{Z}[\zeta]^\times$.

Conculsion.

Pour tout $u \in \mathbb{Z}[\zeta]^\times$, on a l'existence de $r \in \mathbb{Z}$ et ε un réel inversible de $\mathbb{Z}[\zeta]$, tels que :

$$u = \zeta^r\varepsilon$$

7. Le but de ce qui suit est de montrer que $\mathcal{D}_K = \mathbb{Z}[\zeta]$.

7.a. Soit $\theta \in \mathcal{D}_K$. Montrons que

$$N(\theta) \in \mathbb{Z} \text{ and } \mathrm{Tr}(\theta) \in \mathbb{Z}$$

Puisque $\theta \in K = \mathbb{Q}(\zeta)$, alors il existe $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Q}[X]$, tel que $\theta = P(\zeta)$.

On a alors

$$P_\theta = \prod_{k=1}^{p-1}(X - \sigma_k(\theta)) \in \mathbb{Q}[X]$$

En particulier :

$$N(\theta) = \prod_{k=1}^{p-1}\sigma_k(\theta) \in \mathbb{Q}$$

4. Il est facile à vérifier que $\overline{u_{p-1}} = u$.

De plus,

$$N(\theta) = \prod_{k=1}^{p-1} P(\zeta^k)$$

Et $\zeta \in \mathcal{D}_K$, $P \in \mathbb{Q}[X]$, et $\mathcal{D}_K$ est un sous-anneau de $\mathbb{C}$, alors

$$N(\theta) = \prod_{k=1}^{p-1} P(\zeta^k) \in \mathcal{D}_K$$

Par suite :

$$N(\theta) \in \mathcal{D}_K \cap \mathbb{Q} = \mathbb{Z}$$

Ensuite, pour la trace, on a :

$$\begin{aligned}
\mathrm{Tr}(\theta) &= \sum_{k=1}^{p-1} \sigma_k(\theta) \\
&= \sum_{k=1}^{p-1} \sigma_k(P(\zeta)) \\
&= \sum_{k=1}^{p-1} P(\sigma_k(\zeta)) \\
&= \sum_{k=1}^{p-1} P(\zeta^k) \\
&= \sum_{k=1}^{p-1} \sum_{j=0}^{n} a_j \zeta^{jk} \\
&= \sum_{j=0}^{n} a_j \left(\sum_{k=1}^{p-1} \zeta^{jk} \right) \\
&= \sum_{j=0}^{n} a_j \zeta^j \frac{1-\zeta^{j(p-1)}}{1-\zeta^j} \\
&= \sum_{j=0}^{n} a_j \frac{\zeta^j - 1}{1-\zeta^j} \\
&= -\sum_{j=0}^{n} a_j \\
&\in \mathbb{Q}
\end{aligned}$$

Comme $\zeta \in \mathcal{D}_K$, $P \in \mathbb{Q}[X]$, et $\mathcal{D}_K$ est un sous-anneau de $\mathbb{C}$, alors

$$\mathrm{Tr}(\theta) = \sum_{k=1}^{p-1} P(\zeta^k) \in \mathcal{D}_K$$

Par suite :

$$\mathrm{Tr}(\theta) \in \mathcal{D}_K \cap \mathbb{Q} = \mathbb{Z}$$

D'où le résultat.

7.b.i. Soit $k \in [\![0, p-2]\!]$, on a

$$\begin{aligned}
b_k &= \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta) \\
&= \sum_{j=1}^{p-1} \sigma_j(\theta\zeta^{-k} - \theta\zeta) \\
&= \sum_{j=1}^{p-1} (\sigma_j(\theta)\sigma_j(\zeta)^{-k} - \sigma_j(\theta)\sigma_j(\zeta)) \\
&= \sum_{j=1}^{p-1} \left(\sigma_j\left(\sum_{l=0}^{p-2} a_l\zeta^l\right)\zeta^{-jk} - \sigma_j\left(\sum_{l=0}^{p-2} a_l\zeta^l\right)\zeta^j \right) \\
&= \sum_{j=1}^{p-1}\sum_{l=0}^{p-2} a_l(\zeta^{jl-jk} - \zeta^{jl-j}) \\
&= \sum_{l=0}^{p-2} a_l \left(\sum_{j=1}^{p-1}(\zeta^{l-k})^j\right) - \sum_{l=0}^{p-2} a_l \left(\sum_{j=1}^{p-1}(\zeta^{l-1})^j\right) \\
&= \sum_{\substack{l=0 \\ l\neq k}}^{p-2} a_l \left(\sum_{j=1}^{p-1}(\zeta^{l-k})^j - \sum_{j=1}^{p-1}(\zeta^{l-1})^j\right) + a_k\left(p-1-\sum_{j=1}^{p-1}(\zeta^{l-1})^j\right) \\
&= \sum_{\substack{l=0 \\ l\neq k}}^{p-2} a_l \left(\sum_{j=1}^{p-1}(\zeta^{l-k})^j - \sum_{j=1}^{p-1}(\zeta^{l-1})^j\right) + a_k\left(p-1-\zeta^{l-1}\frac{1-\zeta^{(l-1)(p-1)}}{1-\zeta^{l-1}}\right) \\
&= \sum_{\substack{l=0 \\ l\neq k}}^{p-2} a_l \left[\zeta^{l-k}\frac{1-\zeta^{(l-k)(p-1)}}{1-\zeta^{l-k}} - \zeta^{l-1}\frac{1-\zeta^{(l-1)(p-1)}}{1-\zeta^{l-1}}\right] + pa_k \\
&= \sum_{\substack{l=0 \\ l\neq k}}^{p-2} a_l[-1-(-1)] + pa_k \\
&= pa_k
\end{aligned}$$

De plus,

$$\theta\zeta^{-k} - \theta\zeta \in \mathcal{D}_K$$

Donc d'après la question précédente :

$$b_k = \mathrm{Tr}(\theta\zeta^{-k} - \theta\zeta) \in \mathbb{Z}$$

7.b.ii. Montrons qu'il existe des entiers $c_0, \ldots, c_{p-2}$. que l'on exprimera en fonction des b_k tels que :

$$p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$$

On a :

$$\begin{aligned} p\theta &= \sum_{k=0}^{p-2} p a_k (1-\lambda)^k \\ &= \sum_{k=0}^{p-2} \sum_{j=0}^{k} b_k (-1)^j \left(\begin{array}{c} k \\ j \end{array} \right) \lambda^j \\ &= \sum_{j=0}^{p-2} \sum_{k=j}^{p-2} b_k (-1)^j \left(\begin{array}{c} k \\ j \end{array} \right) \lambda^j \end{aligned}$$

On pose pour tout $k \in [\![0, p-2]\!]$,

$$c_k = \sum_{j=k}^{p-2} b_j (-1)^k \left(\begin{array}{c} j \\ k \end{array} \right) \in \mathbb{Z}$$

On a alors

$$p\theta = \sum_{k=0}^{p-2} c_k \lambda^k$$

CQFD.

Montrons que, pour tout $k \in [\![0, p-2]\!]$,

$$b_k = \sum_{l=k}^{p-2} (-1)^l \left(\begin{array}{c} l \\ k \end{array} \right) c_l$$

On a :

$$\begin{aligned}
\sum_{k=0}^{p-2} b_k \zeta^k &= p\sum_{k=0}^{p-2} a_k \zeta^k \\
&= p\theta \\
&= \sum_{k=0}^{p-2} c_k \lambda^k \\
&= \sum_{k=0}^{p-2} c_k (1-\zeta)^k \\
&= \sum_{k=0}^{p-2}\sum_{j=0}^{k} c_k (-1)^j \binom{k}{j} \zeta^j \\
&= \sum_{k=0}^{p-2}\sum_{l=k}^{p-2} c_l (-1)^l \binom{l}{k} \zeta^k
\end{aligned}$$

Avec $(1, \zeta, \ldots, \zeta^{p-2})$ est $\mathbb{Q}$-libre, alors pour tout $k \in [\![0, p-2]\!]$,

$$b_k = \sum_{l=k}^{p-2} c_l (-1)^l \binom{l}{k}$$

D'où le résultat.

7.b.iii. D'après la question 1.b.ii de cette partie, on a :

$$\begin{aligned}
p &= N(1-\zeta) \\
&= \prod_{k=1}^{p-1} \sigma_k (1-\zeta) \\
&= \prod_{k=1}^{p-1} (1-\zeta^k) \\
&= \prod_{k=1}^{p-1} \left[(1-\zeta) \sum_{j=0}^{k-1} \zeta^j \right] \\
&= (1-\zeta)^{p-1} \prod_{k=1}^{p-1} \left(\sum_{j=0}^{k-1} \zeta^j \right) \\
&= \lambda^{p-1} \prod_{k=1}^{p-1} \left(\sum_{j=0}^{k-1} \zeta^j \right)
\end{aligned}$$

Avec

$$\beta = \prod_{k=1}^{p-1} \left(\sum_{j=0}^{k-1} \zeta^j \right) \in \mathbb{Z}[\zeta]$$

Montrons maintenant que $p|c_0$. On a :

$$\begin{aligned} c_0 &= p\theta - \sum_{k=1}^{p-2} c_k \lambda^k \\ &= \beta\lambda^{p-1} - \lambda \sum_{k=1}^{p-2} c_k \lambda^{k-1} \end{aligned}$$

Donc,

$$\begin{aligned} c_0^{p-1} &= N(c_0) \\ &= N\left(\lambda\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k\lambda^{k-1}\right)\right) \\ &= N(\lambda)N\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k\lambda^{k-1}\right) \\ &= pN\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k\lambda^{k-1}\right) \end{aligned}$$

Avec $N\left(\beta\lambda^{p-2} - \sum_{k=1}^{p-2} c_k\lambda^{k-1}\right) \in \mathbb{Z}$, donc $p|c_0^{p-1}$, et comme p est premier, alors $p|c_0$.

Passons maintenant à montrer que $p|c_k$pour tout $k \in [\![0, p-2]\!]$.

Montrons ce résultat par récurrence fini sur $k \in [\![0, p-2]\!]$.

Pour $k = 0$**,** c'est déjà fait !

Soit $\boldsymbol{k \in [\![0, p-3]\!]}$, supposons que le résultat est vrai pour $1, 2, \ldots, k$ et montrons-le pour $k+1$.

On a :

$$c_{k+1}\lambda^{k+1} = p\left(\theta - \sum_{l=0}^{k} \frac{c_l}{p}\lambda^l\right) - \lambda^{k+2} \sum_{l=k+2}^{p-2} c_l \lambda^{l-k-2}$$

Avec pour tout $l \in [\![1, p-2]\!]$,

$$\begin{aligned}
c_{k+1}p^{k+1} &= c_{k+1}N(\lambda^{k+1}) \\
&= N(c_{k+1}\lambda^{k+1}) \\
&= N\left(\beta\lambda^{p+1}\left(\theta - \sum_{l=0}^{k}\frac{c_l}{p}\lambda^l\right) - \lambda^{k+2}\sum_{l=k+2}^{p-2}c_l\lambda^{l-k-2}\right) \\
&= N\left(\lambda^{k+2}\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k}\frac{c_l}{p}\lambda^l\right) - \sum_{l=k+2}^{p-2}c_l\lambda^{l-k-2}\right]\right) \\
&= N(\lambda^{k+2})N\left(\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k}\frac{c_l}{p}\lambda^l\right) - \sum_{l=k+2}^{p-2}c_l\lambda^{l-k-2}\right]\right) \\
&= p^{k+2}N\left(\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k}\frac{c_l}{p}\lambda^l\right) - \sum_{l=k+2}^{p-2}c_l\lambda^{l-k-2}\right]\right)
\end{aligned}$$

Donc,

$$c_{k+1} = pN\left(\left[\beta\lambda^{p-k-1}\left(\theta - \sum_{l=0}^{k}\frac{c_l}{p}\lambda^l\right) - \sum_{l=k+2}^{p-2}c_l\lambda^{l-k-2}\right]\right)$$

Ainsi, $p|c_{k+1}$.

D'où le résultat.

IV Le théorème de Fermat pour$p = 3$

1. On a $3 \not| xyz$, en particulier $3 \not| x$, donc $x \equiv 1[3]$ ou $x \equiv -1[3]$.

Si $x \equiv 1[3]$, on a :

$$(x-1)^3 = x^3 + 3(x - x^2) - 1$$

Avec $9|(x-1)^3$ et $9|3(x-x^2)$, donc

$$x^3 \equiv 1[9]$$

De même, si $x \equiv -1[3]$, on a :

$$(x+1)^3 = x^3 + 3(x^2 + x) + 1$$

Avec $9|(x-1)^3$ et $9|3(x^2+x)$, donc

$$x^3 \equiv -1[9]$$

De même, on obtient :

$$y^3 \equiv 1[9] \text{ or } y^3 \equiv -1[9]$$

et

$$z^3 \equiv 1[9] \text{ or } z^3 \equiv -1[9]$$

Avec

$$x^3 = -(y^3+z^3)$$

Donc, modulo 9, on a les possibilités suivantes :

$$1 \equiv -2[9] \text{ or } 1 \equiv 0[9] \text{ or } 1 \equiv 2[9] \text{ or } -1 \equiv -2[9] \text{ or } -1 \equiv 0[9] \text{ or } 1 \equiv 2[9]$$

Ce qui est absurde !

2. On a :

$$\begin{aligned} \lambda^2 &= (1-j)^2 \\ &= 1-2j+j^2 \\ &= (1+j+j^2)-3j \\ &= -3j \end{aligned}$$

D'après **la question 2.c de la partie** I, on sait que $-j \in \mathbb{Z}[j]^\times$.

Ainsi,

$$3 \sim \lambda^2$$

3. Soit $s \in \mathbb{Z}[j]$ tel que $s \neq 0(\text{mod} < \lambda >)$. Montrons qu'il existe $\varepsilon \in \{1,+1\}$ tel que $s^3 = \varepsilon(\text{mod} < \lambda >)$.

Suivant l'indication, montrons qu'il existe $\varepsilon \in \{-1,1\}$ tel que $s = \varepsilon(\text{mod} < \lambda >)$.

D'après la question précédente, on a $\lambda^2 \sim 3$ dans $\mathbb{Z}[j]$.

Il existe $a, b \in \mathbb{Z}$ tels que $s = a + jb$.

Donc :

$$\begin{aligned} s &= a - 2b + 3jb \\ &= a - 2b(\text{mod} < \lambda >) \\ &= \varepsilon(\text{mod} < \lambda >) \end{aligned}$$

Où $\varepsilon \in \{-1, 0, 1\}$ est obtenu à partir de la division euclidienne de $a - 2b$ par 3.

Puisque $s \neq 0(\text{mod} < \lambda >)$, on a alors $\varepsilon \in \{-1, 1\}$.

Il existe donc $\chi \in \mathbb{Z}[j]$ tel que : $s - \varepsilon = \chi\lambda$.

Ainsi,

$$\begin{aligned} s^3 - \varepsilon &= s^3 - \varepsilon^3 \\ &= (s-\varepsilon)^3 + 3\varepsilon s^2 - 3s \\ &= \chi^3\lambda^3 + 3\varepsilon s(s - \chi) \\ &= \chi^3\lambda^3 - j^2\lambda^2\varepsilon(\chi\lambda + \varepsilon)\chi\lambda \\ &= \chi^3\lambda^3 - j^2\lambda^3\varepsilon(\chi\lambda + \varepsilon)\chi \\ &= \chi\lambda^3(\chi^2 - j^2\varepsilon(\chi\lambda + \varepsilon)) \\ &= \chi\lambda^3(\chi^2 - j^2\varepsilon\chi\lambda - j^2) \end{aligned}$$

D'après ce qui précède, on a l'existence de $\varepsilon' \in \{-1, 1\}$ tel que $\chi = \varepsilon'(\text{mod} < \lambda >)$.

Ainsi, on a, modulo $< \lambda >$

$$\begin{aligned} \chi^2 - j^2\varepsilon\chi\lambda - j^2 &= \varepsilon'^2 - j^2\varepsilon\chi\lambda - j^2(\text{mod} < \lambda >) \\ &= \lambda[(1+j) - j^2\varepsilon\chi](\text{mod} < \lambda >) \\ &= 0(\text{mod} < \lambda >) \end{aligned}$$

Ainsi, il existe $\mu \in \mathbb{Z}[j]$ tel que

$$\chi^2 - j^2\varepsilon\chi\lambda - j^2 = \mu\lambda$$

Par suite,

$$\begin{aligned} s^3 - \varepsilon &= \chi\mu\lambda^4 \\ &= 0(\text{mod} < \lambda^4 >) \end{aligned}$$

D'où le résultat.

4. Supposons que (P_n) est vérifiée pour un quadruplet $(\alpha, \beta, \delta, \omega)$.

Montrons que $n \geqslant 2$.

On a

$$z = \mu\lambda^n$$

Donc

$$\alpha^3 + \beta^3 + \omega\delta^3\lambda^{3n} = 0$$

Et on a

$$\lambda \not| \alpha\beta\delta$$

Donc $\lambda \not| \alpha$, $\lambda \not| \beta$ et $\lambda \not| \delta$.

Ainsi, $\alpha \neq 0(\text{mod} < \lambda >)$, $\beta \neq 0(\text{mod} < \lambda >)$ et $\delta \neq 0(\text{mod} < \lambda >)$.

En utilisant la question 3 de cette partie, on a l'existence de $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{-1, 1\}$ tels que :

$$\begin{cases} \alpha^3 = \varepsilon_1(\text{mod} < \lambda^4 >) \\ \beta^3 = \varepsilon_1(\text{mod} < \lambda^4 >) \\ \delta^3 = \varepsilon_1(\text{mod} < \lambda^4 >) \end{cases}$$

Donc

$$\begin{aligned} \omega\delta^3\lambda^{3n} &= -(\alpha^3 + \beta^3) \\ &= -(\varepsilon_1 + \varepsilon_2) \quad (\text{mod} < \lambda^4 >) \end{aligned}$$

Avec $\alpha \wedge \beta = 1$, alors $\varepsilon_1 \neq \varepsilon_2$, avec $\varepsilon_1, \varepsilon_2 \in \{-1, 1\}$, on a alors $\varepsilon_1 + \varepsilon_2 = 0$.

Par suite,

$$\omega\delta^3\lambda^{3n} = 0 \quad (\text{mod} < \lambda^4 >)$$

Autrement dit

$$\lambda^4 | \omega\delta^3\lambda^{3n}$$

Avec $\omega \in \mathbb{Z}[j]^\times$, donc il existe $u = a + jb \in \mathbb{Z}[j]^\times$ tel que $\omega(a + jb) = 1$.

Ainsi,

$$(a + b).\omega - (b\omega)\lambda = 1$$

D'après le théorème de Bézout, on a $\lambda \wedge \omega = 1$, donc $\lambda^4 \wedge \omega = 1$.

Par conséquent, via le lemme de Gauss, on a :

$$\lambda^4 | \delta^3 \lambda^{3n}$$

D'autre part, on a

$$\delta^3 = \varepsilon_1 (\text{mod} < \lambda^4 >)$$

Donc, il existe $t \in \mathbb{Z}[j]$ tel que $\delta^3 = \varepsilon_1 + t\lambda^4$.

Ainsi,

$$\varepsilon_1 \delta^3 - (\varepsilon_1 t)\lambda^4 = 1$$

D'après le théorème de Bézout, on a $\delta^3 \wedge \lambda^4 = 1$. Le lemme da Gauss assure que :

$$\lambda^4 | \lambda^{3n}$$

Étant donné que λ est non inversible, on en déduit $3n \geqslant 4$. Comme $n \in \mathbb{N}$, alors $n \geqslant 2$.

D'où le résulltat.

5. On a

$$-\omega\delta^3\lambda^{3n} = \alpha^3 + \beta^3$$

Avec $\lambda \not| \alpha\beta\delta$, en particulier $\beta \neq 0$.

On a alors

$$\begin{aligned} -\omega\delta^3\lambda^{3n} &= \alpha^3 + \beta^3 \\ &= (-\beta)^3 \left[\left(\frac{\alpha}{-\beta} \right)^3 - 1^3 \right] \end{aligned}$$

En utilisant la factorisation :

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

(Car les racines cubiques de l'unité sont exactement $1, j$ et j^2).

Alors,

$$\begin{aligned} -\omega\delta^3\lambda^{3n} &= \alpha^3 + \beta^3 \\ &= (-\beta)^3 \left[\left(\frac{\alpha}{-\beta} \right)^3 - 1^3 \right] \\ &= (-\beta)^3 \left(\frac{\alpha}{-\beta} - 1 \right) \left(\frac{\alpha}{-\beta} - j \right) \left(\frac{\alpha}{-\beta} - j^2 \right) \\ &= (\alpha+\beta)(\alpha+j\beta) \left(\alpha + j^2\beta \right) \end{aligned}$$

D'où le résultat.

Remarque.

On peut commencer par développer le terme à droite, et on obtient :

$$\begin{aligned}(\alpha+\beta)(\alpha+j\beta)\left(\alpha+j^2\beta\right) &= \alpha^3+j^2\alpha^2\beta-j^2\alpha^2\beta-j\alpha\beta^2+j\alpha\beta^2+\beta^3\\ &= \alpha^3+\beta^3\\ &= -\omega\delta^3\lambda^{3n}\end{aligned}$$

5.b. D'après la question précédente, on a $\lambda|(\alpha+\beta)(\alpha+j\beta)\left(\alpha+j^2\beta\right)$.

Comme $N(\lambda)=3$ qui est un nombre premier, alors, d'après la question 3.b de la partie 3, on a λ est irréductible.

Donc $\lambda|\alpha+\beta$ ou $\lambda|\alpha+j\beta$ ou $\lambda|\alpha+j^2\beta$.

Il existe donc $i_0\in\{0,1,2\}$ tel que $\lambda|\alpha+j^{i_0}\beta$.

Soit $k\in\{0,1,2\}$, on a :

$$\begin{aligned}\alpha+j^k\beta &= \alpha+j^{i_0}\beta+\left(j^k-j^{i_0}\right)\beta\\ &= \alpha+j^{i_0}\beta+\varepsilon_{k,i_0}j^{\min(k,i_0)}(j^{\max(k,i_0)}-1)\beta\end{aligned}$$

avec

$$\varepsilon_{k,i_0}=\operatorname{sgn}(k-i_0)\in\{-1,0,1\}$$

Ainsi,

$$\begin{aligned}\alpha+j^k\beta &= \alpha+j^{i_0}\beta+\varepsilon_{k,i_0}j^{\min(k,i_0)}(j-1)\beta\left(\sum_{l=0}^{\max(k,i_0)-1}j^l\right)\\ &= \alpha+j^{i_0}\beta-\lambda\varepsilon_{k,i_0}j^{\min(k,i_0)}\beta\left(\sum_{l=0}^{\max(k,i_0)-1}j^l\right)\end{aligned}$$

Puisque

$$\lambda\left|\alpha+j^{i_0}\beta\right.\text{ and }\lambda|\lambda\varepsilon_{k,i_0}j^{\min(k,i_0)}\beta\left(\sum_{l=0}^{\max(k,i_0)-1}j^l\right)$$

alors

$$\lambda|\alpha+j^{i_0}\beta-\lambda\varepsilon_{k,i_0}j^{\min(k,i_0)}\beta\left(\sum_{l=0}^{\max(k,i_0)-1}j^l\right)=\alpha+j^k\beta$$

Cela est vrai pour $k = 0, 1, 2$.

D'où

$$\lambda|\alpha+\beta \text{ and } \lambda|\alpha+j\beta \text{ and } \lambda|\alpha+j^2\beta$$

5.c. Montrons que λ est un **pgcd** de $\alpha+\beta$ et $\alpha+j\beta$.

Notons d un pgcd de $\alpha+\beta$ et $\alpha+j\beta$.

D'après la question précédente, $\lambda|\alpha+\beta$ and $\lambda|\alpha+j\beta$.

En particulier,

$$\lambda|d$$

Et

$$d|\lambda\beta = (\alpha+\beta)-(\alpha+j\beta)$$

Alors

$$d|\lambda$$

Ainsi, d et λ sont associés, d'où λ est un pgcd de $\alpha+\beta$ et $\alpha+j\beta$.

De la même manière, on peut montrer facilemet que λ est aussi un pgcd de $\alpha+\beta$ et $\alpha+j^2\beta$ (respectivement de $\alpha+j\beta$ et $\alpha+j^2\beta$).

Notons

$$\begin{cases} \alpha+\beta = \lambda^{m_1} r_1 \\ \alpha+j\beta = \lambda^{m_2} r_2 \\ \alpha+j^2\beta = \lambda^{m_3} r_3 \end{cases}$$

Avec $\lambda \nmid r_1$, $\lambda \nmid r_2$ et $\lambda \nmid r_3$. et $m_1, m_2, m_3 \geqslant 1$ des entiers qui représentent respectivement la valuation λ-adique de $\alpha+\beta$, $\alpha+j\beta$ et $\alpha+j^2\beta$.

D'après ce qui précède, on a

$$\begin{cases} \min(m_1, m_2) = 1 \\ \min(m_2, m_3) = 1 \\ \min(m_3, m_1) = 1 \end{cases}$$

Donc, forcément, deux des entiers m_1, m_2, m_3 sont inférieurs ou égaux à 1.

Par symétrie (il suffit de remplacer β par $j\beta$ ou $j^2\beta$), on peut supposer que $m_1, m_2 \leqslant 1$.

Or, comme $m_1, m_2 \geqslant 1$, alors $m_1 = m_2 = 1$.

Avec

$$\lambda^4| - \omega\delta^3\lambda^{3n} = (\alpha+\beta)(\alpha+j\beta)\left(\alpha+j^2\beta\right) = \lambda^{m_1+m_2+m_3} r_1 r_2 r_3$$

Comme $\lambda \not| r_1$et $\lambda \not| r_2$ et $\lambda \not| r_3$ et λ est irréductible, alors $\lambda \wedge r_1 r_2 r_3 = 1$.

Par suite,

$$m_1 + m_2 + m_3 \geqslant 4$$

Donc $m_3 \geqslant 2$.

D'où λ^2 divise $\alpha + j^2\beta$.

D'où le résultat.

5.d. On a

$$\begin{aligned} -\omega\delta^3\lambda^{3n} &= (\alpha+\beta)(\alpha+j\beta)\left(\alpha+j^2\beta\right) \\ &= \lambda^{3n}\kappa_1\kappa_2\kappa_3 \end{aligned}$$

Avec $\lambda \neq 0$, alors

$$-\omega\delta^3 = \kappa_1\kappa_2\kappa_3$$

Montrons l'existence de $\gamma_l \in \mathbb{Z}[j]$ tel que $\kappa_l \sim \gamma_l^3$ pour tout $l \in \{1,2,3\}$.

Soit $l \in \{1,2,3\}$. Comme $\mathbb{Z}[j]$ est un anneau principal, alors il existe $p_{1,l}, \ldots, p_{m_l,l} \in \mathbb{Z}[j]$ des irréductibles deux à deux distincts, et $\eta_{1,l}, \ldots, \eta_{lm_l,l} \in \mathbb{N}^*$ et $\omega_l \in \mathbb{Z}[j]^\times$ tels que :

$$\kappa_l = \omega_l \prod_{s=1}^{m_l} p_{s,l}^{\eta_{s,l}}, \quad \text{pour tout } l \in \{1,2,3\}$$

Via la question précédente, on a λ est un pgcd de $\alpha+\beta$ et $\alpha+j\beta$ (respectivement de $\alpha+j\beta$, $\alpha+j^2\beta$, $\alpha+j^2\beta$ et $\alpha+\beta$).

Donc κ_1 and κ_2 (respectivement κ_2 and κ_3, et κ_1) sont premiers entre eux.

Ainsi, $p_{1,1}, \ldots, p_{m_1,1}, p_{1,2}, \ldots, p_{m_2,2}, p_{1,3}, \ldots, p_{m_3,3}$ sont deux à deux distincts.

Et on a :

$$\begin{aligned} -\omega\delta^3 &= \kappa_1\kappa_2\kappa_3 \\ &= \prod_{l=1}^{3}\left(\omega_l \prod_{s=1}^{m_l} p_{s,l}^{\eta_{s,l}}\right) \\ &= \omega_1\omega_2\omega_3 \prod_{l=1}^{3}\prod_{s=1}^{m_l} p_{s,l}^{\eta_{s,l}} \end{aligned}$$

Notons $\delta = \vartheta \prod_{s=1}^{m} p_s^{\tau_s}$ la décomposition en produit d'irréductibles de δ.

Avec $\vartheta \in \mathbb{Z}[j]^\times$, et $p_1, \dots, p_m$ des irréductibles deux à deux distincts et $\tau_1, \dots, \tau_m \in \mathbb{N}^*$.

On a alors :

$$-\omega\vartheta^3 \prod_{s=1}^{m} p_s^{3\tau_s} = \omega_1\omega_2\omega_3 \prod_{l=1}^{3}\prod_{s=1}^{m_l} p_{s,l}^{\eta_{s,l}}$$

Par l'unicité de la décomposition en facteurs irréductibles, on a forcément 3 divise $\eta_{s,l}$ pour tout $l \in \{1,2,3\}$ et $s \in [\![1, m_l]\!]$.

Notons pour tout $l \in \{1,2,3\}$ and $s \in [\![1, m_l]\!]$:

$$\varsigma_{s,l} = \frac{\eta_{s,l}}{3} \in \mathbb{N}^*$$

On a alors, pour tout $l \in \{1,2,3\}$,

$$\kappa_{l=}\omega_l \left(\prod_{s=1}^{m_l} p_{s,l}^{\varsigma_{s,l}} \right)^3$$

Donc, pour tout $l \in \{1,2,3\}$, on a

$$\kappa_l \sim \gamma_l^3$$

Avec

$$\gamma_l^3 = \prod_{s=1}^{m_l} p_{s,l}^{\varsigma_{s,l}}$$

D'où le résultat.

5.e. Montrons qu'il existe deux inversibles τ et τ' de $\mathbb{Z}[j]^\times$ tels que

$$\gamma_2^3 + \tau\gamma_3^3 + \tau'\lambda^{3(n-1)}\gamma_1^3 = 0$$

Essayons de détailler la question tout en profitant des résultats obtenus précédemment.

Puisque pour tout $l \in \{1,2,3\}$, on a $\kappa_l \sim \gamma_l^3$, donc il existe $a_l \in \mathbb{Z}[j]^\times$ tel que : $\kappa_l = a_l\gamma_l^3$.

Ainsi,

$$\begin{cases} \alpha + \beta = \lambda^{3n-2} a_1 \gamma_1^3 \\ \alpha + j\beta = \lambda a_2 \gamma_2^3 \\ \alpha + j^2\beta = \lambda a_3 \gamma_3^3 \end{cases}$$

Il s'agit de trouver un triplet $(a,b,c) \in \mathbb{Z}[j]^\times \times \mathbb{Z}[j]^\times \times \mathbb{Z}[j]^\times$, tel que :

$$a\gamma_2^3 + b\gamma_3^3 + c\lambda^{3(n-1)}\gamma_1^3 = 0.$$

Cela équivaut à trouver $(a,b,c) \in \mathbb{Z}[j]^\times \times \mathbb{Z}[j]^\times \times \mathbb{Z}[j]^\times$, tel que :

$$a(\alpha+\beta) + b(\alpha+j\beta) + c(\alpha+j^2\beta) = 0$$

Il suffit alors de trouver $(a,b,c) \in \mathbb{Z}[j]^\times \times \mathbb{Z}[j]^\times \times \mathbb{Z}[j]^\times$, tel que :

$$\begin{cases} a+b+c=0 \\ a+jb+j^2c=0 \end{cases}$$

Le triplet $(a,b,c) = (j^2,1,j)$ convient.
Ainsi,

$$\lambda a_2\gamma_2^3 + \lambda j a_3\gamma_3^3 + j^2 a_1\lambda^{3n-2}\gamma_1^3 = 0$$

Par suite,

$$\gamma_2^3 + j a_2^{-1}a_3\gamma_3^3 + j^2 a_2^{-1}a_1\lambda^{3(n-1)}\gamma_1^3 = 0$$

D'où le résultat pour $\tau = j a_2^{-1}a_3$, et $\tau' = j^2 a_2^{-1}a_1$.

5.f. Si $\tau = \pm 1$, montrons que (P_{n-1}) est vérifiée.
On a :

$$\gamma_2^3 + (\tau\gamma_3)^3 + \lambda^{3(n-1)}\gamma_1^3 = 0$$

Avec $\lambda \nmid \omega\delta^3 = \kappa_1\kappa_2\kappa_3$ et $\kappa_l \sim \gamma_l^3$ pour $l \in \{1,2,3\}$, donc $\lambda \nmid (\gamma_1\gamma_2\gamma_3)^3$.
Or, λ est irréductible dans $\mathbb{Z}[j]$, car $N(\lambda) = 3$ est premier.
Donc $\lambda \nmid \gamma_1\gamma_2\gamma_3$.
De plus, on a :

$$\begin{cases} \alpha + j\beta = \lambda\kappa_2 \\ \alpha + j^2\beta = \lambda\kappa_3 \end{cases}$$

Donc :

$$\begin{aligned} \lambda\alpha &= (\alpha + j^2\beta) - j(\alpha + j\beta) \\ &= \lambda\kappa_3 - j\lambda\kappa_2 \end{aligned}$$

Ainsi :

$$\alpha = \kappa_3 - j\kappa_2$$

De même, on trouve :

$$\beta = j^2(\kappa_2 - \kappa_3)$$

Soit d un PGCD de κ_2 et κ_3, alors d divise à la fois $\kappa_3 - j\kappa_2 = \alpha$ et $j^2(\kappa_2 - \kappa_3) = \beta$.

Donc d est un PGCD de α et β.

Or, α et β sont premier entre eux, alors d est inversible.

Par suite, κ_2 et κ_3 sont premiers entre eux.

D'après ce qui précéde, $(\kappa_1, \kappa_2, \kappa_3)$ vérifie (P_{n-1}).

D'où le résultat.

5.g. Montrons que $\tau = \pm 1 (\mathrm{mod} \langle \lambda^3 \rangle)$.

D'après la question 5.e de cette partie, on a :

$$\gamma_2^3 + \tau\gamma_3^3 + \lambda^{3(n-1)}\gamma_1^3 = 0$$

Avec $n \geqslant 2$, alors modulo $\langle \lambda^3 \rangle$, on a :

$$\gamma_2^3 + \tau\gamma_3^3 = 0 (\mathrm{mod} \langle \lambda^3 \rangle)$$

Avec $\lambda \not| \gamma_2, \gamma_3$, d'après la qustion 3 de cette partie, on a l'existence de $\varepsilon_2, \varepsilon_3 \in \{-1, 1\}$ tels que :

$$\begin{cases} \gamma_2^3 = \varepsilon_2 (\mathrm{mod} \langle \lambda^4 \rangle) \\ \gamma_3^3 = \varepsilon_3 (\mathrm{mod} \langle \lambda^4 \rangle) \end{cases}$$

En particulier,

$$\begin{cases} \gamma_2^3 = \varepsilon_2 (\mathrm{mod} \langle \lambda^4 \rangle) \\ \gamma_3^3 = \varepsilon_3 (\mathrm{mod} \langle \lambda^4 \rangle) \end{cases}$$

Ainsi,

$$\varepsilon_2 + \varepsilon_3\tau = 0 (\mathrm{mod} \langle \lambda^3 \rangle)$$

D'où

$$\tau = \pm 1 (\mathrm{mod} \langle \lambda^3 \rangle)$$

On peut facilement montrer que $-j, j, -j^2, j^2$ ne sont pas congrus à ± 1 $(\mathrm{mod} \langle \lambda^3 \rangle)$.

Ainsi, $\tau \not\in \{j, -j, j^2, -j^2\}$.

6. D'après tout ce qu'on vu dans cette partie, on a

$$j \in \mathbb{Z}[j]^\times = \{1, -1, j, -j, j^2, -j^2\}$$

Or, d'après la question précédente, on a montré que $\tau \not\in \{j, -j, j^2, -j^2\}$.

D'où $\tau = \pm 1$.

Et, via la question 5.f, on en déduit que (P_{n-1}) est vérifiée.

Ainsi, si (P_n) est vérifiée, alors $n \geqslant 2$ et (P_{n-1}) est également vérifiée.

Par principe de récurrence, on a (P_1) est vérifiée et $1 \geqslant 2$, ce qui est absurde !

D'où l'équation $x^3 + y^3 + z^3 = 0$ n'a pas de solution $(x, y, z) \in \mathbb{Z}_*^3$ dans le cas où $3|xyz$.

V. Le théorème de Fermat pour p régulier et $p \not| xyz$

1. Montrons que

$$\prod_{k=0}^{p-1} \langle x + \zeta^k y \rangle = \langle z^p \rangle$$

Par définition, on a :

$$\prod_{k=0}^{p-1} \langle x + \zeta^k y \rangle$$

$$= \left\{ \sum_{i \in J} \prod_{k=0}^{p-1} x_{k,i} | J \text{ est un ensemble fini, and pour tout} (i,k) \in J \times [\![0, p-1]\!] x_{k,i} \in \langle x + \zeta^k y \rangle \right\}$$

Soit $t \in \prod_{k=0}^{p-1} \langle x + \zeta^k y \rangle$, on a alors l'existence d'un ensemble fini J, et une famille $(x_{i,k})_{(i,k) \in J \times [\![0,p-1]\!]}$ tels que :

$$t = \sum_{i \in J} \prod_{k=0}^{p-1} x_{k,i}$$

Et pour tout $(i,k) \in J \times [\![0, p-1]\!]$, on a $x_{k,i} \in \langle x + \zeta^k y \rangle$.

Donc, pour tout $(i,k) \in J \times [\![0, p-1]\!]$, il existe $a_{k,i} \in \mathbb{Z}[\zeta]$ tel que $x_{k,i} = (x + \zeta^k y) a_{k,i}$.

On a alors :

$$\begin{aligned} t &= \sum_{i\in J}\prod_{k=0}^{p-1}[(x+\zeta^k y)a_{k,i}] \\ &= \sum_{i\in J}\prod_{k=0}^{p-1}(x+\zeta^k y)\prod_{k=0}^{p-1}a_{k,i} \\ &= \prod_{k=0}^{p-1}(x+\zeta^k y)\sum_{i\in J}\prod_{k=0}^{p-1}a_{k,i} \end{aligned}$$

Avec $x, y \neq 0$, on a alors :

$$\begin{aligned} \prod_{k=0}^{p-1}(x+\zeta^k y) &= (-y)^p\prod_{k=0}^{p-1}\left(\frac{x}{-y}-\zeta^k\right) \\ &= (-y)^p\left(\left(\frac{x}{-y}\right)^p-1\right) \\ &= x^p+y^p \\ &= -z^p \end{aligned}$$

Donc :

$$\begin{aligned} t &= -z^p\sum_{i\in J}\prod_{k=0}^{p-1}a_{k,i} \\ &\in \langle z^p\rangle \end{aligned}$$

D'où :

$$\prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle \subset \langle z^p\rangle$$

Réciproquement, soit $u \in \langle z^p\rangle$. Alors, il existe $u' \in \mathbb{Z}[\zeta]$ tel que $u = z^p u'$. On a alors

$$\begin{aligned} u &= u'z^p \\ &= -u'(x^p+y^p) \\ &= -u'\prod_{k=0}^{p-1}(x+\zeta^k y) \\ &\in \prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle \end{aligned}$$

D'où

$$\langle z^p\rangle \subset \prod_{k=0}^{p-1}\langle x+\zeta^k y\rangle$$

Par suite,

$$\prod_{k=0}^{p-1} \langle x + \zeta^k y \rangle = \langle z^p \rangle$$

2.a. Montrons que $\lambda y \in \mathfrak{B}$.

On a

$$\begin{aligned}(x + \zeta^l y) - (x + \zeta^k y) &= \zeta^k(\zeta^{l-k} - 1)y \\ &= \zeta^k(\zeta - 1)\frac{1 - \zeta^{l-k}}{1 - \zeta} y \\ &= -\lambda y \zeta^k \frac{1 - \zeta^{l-k}}{1 - \zeta}\end{aligned}$$

Donc,

$$\lambda y = -\frac{1}{\zeta^k} \times \frac{1 - \zeta}{1 - \zeta^{l-k}}[(x + \zeta^l y) - (x + \zeta^k y)]$$

Avec $l - k \in [\![1, p-1]\!]$, et en utilisant **la question 5.b de la partie 3**, on a :

$$\frac{1 - \zeta}{1 - \zeta^{l-k}} \in \mathbb{Z}[\zeta]^\times$$

De plus, on a $N(\zeta^k) = 1$. Donc, via **la question 3.b de la partie 3**, on a $\zeta^k \in \mathbb{Z}[\zeta]^\times$, donc $\frac{1}{\zeta^k} \in \mathbb{Z}[\zeta]^\times$. Par suite,

$$\frac{1}{\zeta^k} \times \frac{1 - \zeta}{1 - \zeta^{l-k}} \in \mathbb{Z}[\zeta]^\times$$

Donc,

$$\lambda y \in \langle x + \zeta^l y \rangle \cap \langle x + \zeta^k y \rangle$$

2.b. Montrons que $y \notin \mathfrak{B}$.

On sait que $\mathfrak{B}$ est premier, donc on a $\lambda \in \mathfrak{B}$ ou $y \in \mathfrak{B}$.

Par l'absurde, supposons que $y \in \mathfrak{B}$. D'après la question 1 de cette partie, on a $\mathfrak{B}$ divise $< z^p >$. En particulier, $z \in \mathfrak{B}$.

Or, y et z sont premiers entre eux, donc d'après le théorème de Bézout, on a l'existence de $(u, v) \in \mathbb{Z}^2$ tel que

$$uy + vz = 1$$

Ainsi, $1 \in \mathfrak{B}$, ce qui est absurde !

Montrons que $x + y \in \langle \lambda \rangle \cap \mathbb{Z}$.

On a $y \notin \mathfrak{B}$, et $\mathfrak{B}$ est premier, donc $\lambda \in \mathfrak{B}$, ce qui implique que $< \lambda > \subset \mathfrak{B}$.

Or, $< \lambda >$ est premier (d'après **la question 5 de la partie 3**).

Or, pour tout $k \in [\![0, p-1]\!]$, on a

$$\begin{aligned} \zeta^k - 1 &= \lambda \sum_{j=0}^{k-1} \zeta^j \\ &= 0 (\text{mod} < \lambda >) \end{aligned}$$

Ainsi,

$$\zeta^k = 1 (\text{mod} < \lambda >)$$

Par suite,

$$x + y = x + \zeta^k y (\text{mod} < \lambda >)$$

Par définition de $\mathfrak{B}$,

$$x + \zeta^k y = 0 (\text{mod} < \lambda >)$$

Donc,

$$x + y = 0 (\text{mod} < \lambda >)$$

Ainsi, $x + y \in \mathbb{Z} \cap < \lambda >= p\mathbb{Z}$.

Par suite ,

$$p | z^p = -(x^p + y^p) = -(x + y) \sum_{k=0}^{p-1} x^k y^{p-1-k}$$

Comme p est premier, alors $p|z$, ce qui est absurde avec $p|xyz$.

D'où le résultat souhaité.

3. Justifions qu'il existe un idéal I tel que $< x + \zeta y >= I^p$.

D'après la question 1, on a :

$$\prod_{k=0}^{p-1} \langle x + \zeta^k y \rangle = \langle z^p \rangle$$

Comme les idéaux $< x + \zeta^k y >$ sont deux à deux premiers entre eux (d'après la question 2.a), et en vertu du théorème de décomposition unique des idéaux en produits d'idéaux premiers dans $\mathbb{Z}[\zeta]$, on peut conclure que cette décomposition est unique.

Or, pour tout $k \in [\![0, p-1]\!]$ l'idéal $\langle x + \zeta^k y \rangle$ est une puissance p-ième d'un idéal. En particulier, cela est vrai pour $< x + \zeta y >$.

4. Montrons qu'il existe $r \in \mathbb{Z}$, un réel ε inversible de $\mathbb{Z}[\zeta]$ et $\alpha \in \mathbb{Z}[\zeta]$ tels que

$$x + \zeta y = \zeta^r \varepsilon \alpha^p$$

Puisque $I^p =< x + \zeta y >$ est principal, et p est régulier. alors I est principal.

Ainsi, il existe $\alpha \in \mathbb{Z}[\zeta]$ tel que

$$< x + \zeta y >=< \alpha^p >$$

En particulier, il existe $\omega \in \mathbb{Z}[\zeta]^\times$ tel que

$$x + \zeta y = u\alpha^p$$

Or, d'après **la question 6 de la partie 3**, on peut écrire u sous la forme $u = \zeta^r \varepsilon$, avec $r \in \mathbb{Z}$ et $\varepsilon \in \mathbb{Z}[\zeta]^\times \cap \mathbb{R}$.

D'où le résultat.

5. Montrons l'existence de $a \in \mathbb{Z}$ tel que $\alpha^p = a (\mathrm{mod} \langle p \rangle)$.

Écrivons $\alpha = c + \zeta b$, où $c, b \in \mathbb{Z}$.

On a

$$\begin{aligned} \alpha^p &= (c + \zeta b)^p \\ &= \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} \zeta^k b^k c^{p-k} \end{aligned}$$

Avec $p \left| \begin{pmatrix} p \\ k \end{pmatrix} \right.$, pour tout $k \in [\![1, p-1]\!]$, alors

$$\alpha^p = c^p + b^p (\mathrm{mod} \langle p \rangle)$$

D'où le résultat. (on pose $a = c^p + b^p \in \mathbb{Z}$)

Montrons maintenant que

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0 (\mathrm{mod} \langle p \rangle)$$

On a

$$\begin{aligned} x\zeta^{-r} + y\zeta^{1-r} - x\zeta^{r} - y\zeta^{r-1} &= (\zeta^{-r} - \zeta^{r})(x + \zeta y) \\ &= (\zeta^{-r} - \zeta^{r})\zeta^{r}\varepsilon\alpha^{p} \\ &= (1 - \zeta^{2r})\varepsilon\alpha^{p} \\ &= (1 - \zeta^{2r})\varepsilon a (\mathrm{mod}\langle p\rangle) \end{aligned}$$

Notons r_0 le reste de la division euclidienne de $2r$ par p.
On a alors $r_0 \in [\![0, p-1]\!]$, et

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^{r} - y\zeta^{r-1} = (1 - \zeta^{2r_0})\varepsilon a (\mathrm{mod}\langle p\rangle)$$

Or,

$$\begin{aligned} (1 - \zeta^{2r_0}) \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} (1 - \zeta^{k}) &= \prod_{k=1}^{p-1} (1 - \zeta^{k}) \\ &= N(1 - \zeta) \\ &= N(\lambda) \\ &= p \end{aligned}$$

Donc,

$$(1 - \zeta^{2r_0})(1 - \zeta)^{p-1} = p \prod_{\substack{k=1 \\ k\neq r_0}}^{p-1} \frac{(1 - \zeta)}{(1 - \zeta^{k})}$$

Ainsi,

$$\begin{aligned}
1-\zeta^{2r_0} &= p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})[(1-\zeta)^{p-1}-1] \\
&= p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})\sum_{j=1}^{p-1}\begin{pmatrix} p-1 \\ j \end{pmatrix}\zeta^j \\
&= p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\left[\begin{pmatrix} p-1 \\ 2j-1 \end{pmatrix} + \begin{pmatrix} p-1 \\ 2j \end{pmatrix}\zeta\right]\zeta^{2j-1} \\
&= p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\left[\begin{pmatrix} p \\ 2j \end{pmatrix} - \lambda\begin{pmatrix} p-1 \\ 2j \end{pmatrix}\right]\zeta^j \\
&= p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\begin{pmatrix} p \\ 2j \end{pmatrix} + \lambda(1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\begin{pmatrix} p-1 \\ 2j \end{pmatrix}\zeta^j
\end{aligned}$$

Avec $p\left|\begin{pmatrix} p \\ 2j \end{pmatrix}\right.$, pour tout $j \in \left[\!\left[1, \frac{p-1}{2}\right]\!\right]$, donc

$$p\prod_{\substack{k=1\\k\neq r_0}}^{p-1}\frac{(1-\zeta)}{(1-\zeta^k)} - (1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\begin{pmatrix} p \\ 2j \end{pmatrix} \in p\mathbb{Z}[\zeta]$$

De plus,

$$\begin{aligned}
\lambda^p &= (1-\zeta)^p \\
&= \sum_{k=0}^{p}\begin{pmatrix} p \\ k \end{pmatrix}\zeta^k \\
&= \sum_{k=1}^{p-1}\begin{pmatrix} p \\ k \end{pmatrix}\zeta^k
\end{aligned}$$

Or, $p\left|\begin{pmatrix} p \\ k \end{pmatrix}\right.$, pour tout $k \in [\![1, p-1]\!]$, alors $p|\lambda^p$.

Avec, p est irréductible dans $\mathbb{Z} \subset \mathbb{Z}[\zeta]$, donc p est irréductible dans $\mathbb{Z}[\zeta]$, ainsi $p|\lambda$.

Par suite,

$$\lambda(1-\zeta^{2r_0})\sum_{j=1}^{\frac{p-1}{2}}\begin{pmatrix} p-1 \\ 2j \end{pmatrix}\zeta^j \in p\mathbb{Z}[\zeta]$$

D'où,

$$(1-\zeta^{2r_0}) \in p\mathbb{Z}[\zeta]$$

Finalement,

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0(\text{mod} < p >)$$

6. Supposons que $r = 0(\text{mod}\, p\mathbb{Z})$, Montrons que $p|y$dans $\mathbb{Z}$.
D'après la question précédente, on a :

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = 0(\text{mod}\langle p\rangle)$$

Puisque $r = 0(\text{mod}\, p\mathbb{Z})$, donc $\zeta^r = 1$. Ainsi,

$$y(\zeta^1 - \zeta^{-1}) = 0(\text{mod}\langle p\rangle)$$

Cela signifie qu'il existe un $t \in \mathbb{Z}[\zeta]$, tel que

$$y(\zeta^1 - \zeta^{p-1}) = pt$$

On a alors [5]

$$\begin{aligned} N(y(\zeta^1 - \zeta^{p-1})) &= N(y\zeta^{p-1}(\zeta+1)(\zeta-1)) \\ &= N(y)N(\zeta^{p-1})N(\zeta-1)N(\zeta+1) \\ &= -py^{p-1} \end{aligned}$$

Dautre part,

$$\begin{aligned} N(y(\zeta^1 - \zeta^{p-1})) &= N(pt) \\ &= p^{p-1}N(t) \end{aligned}$$

Ainsi,

$$p^{p-2}N(t) = -y^{p-1}$$

5. Car $\zeta^{p-1} \in \mathbb{Z}[\zeta]^\times$, alors $N(\zeta^{p-1}) = 1$ et d'après la partie 3 on a $N(1-\zeta) = p$ et $N(1+\zeta) = 1$.

Puisque $N(t) \in \mathbb{Z}$ (voir le lemme 4), cela implique $p|y^p$.

Étant donné que p est premier, alors $p|y$.

« On montrerait de même que l'on ne peut avoir $r = 1(\mathrm{mod}\, p\mathbb{Z})$, ce que l'on admet. »

7. D'après la question 5, il existe $\beta \in \mathbb{Z}[\zeta]$ tel que

$$x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1} = \beta p$$

Montrons que deux des entiers parmi $\pm r$ et $\pm(1-r)$ sont égaux modulo p.

Par l'absurde, supposons qu'aucun des entiers $\pm r$, $\pm(1-r)$ ne soit égal modulo p.

On a alors,

$$\beta = \frac{x}{p}\zeta^{-r} + \frac{y}{p}\zeta^{1-r} - \frac{x}{p}\zeta^r - \frac{y}{p}\zeta^{r-1}$$

Or, $(1, \zeta, \ldots, \zeta^{p-2})$ est une $\mathbb{Q}$-base de $\mathbb{Q}(\zeta)$, et $\beta \in \mathbb{Z}[\zeta]$.

Ainsi, $\frac{x}{p} \in \mathbb{Z}$, ce qui implique que $p|x$, ce qui est absurde.

D'où le résultat

Donc $\pm r = \pm(1-r)(\mathrm{mod}\, p\mathbb{Z})$, et cela n'est possible que pour $r = (1-r)(\mathrm{mod}\, p\mathbb{Z})$

Ainsi,

$$2r = 1(\mathrm{mod}\, p\mathbb{Z})$$

8. Montrons que

$$\beta p\zeta^r = (x-y)\lambda$$

D'après la question précédente, on a $2r = 1(\mathrm{mod}\, p\mathbb{Z})$, alors :

$$\begin{aligned}
\beta p\zeta^r &= (x\zeta^{-r} + y\zeta^{1-r} - x\zeta^r - y\zeta^{r-1})\zeta^r \\
&= x + \zeta y - x\zeta^{2r} - y\zeta^{2r-1} \\
&= x + \zeta y - x\zeta - y \\
&= (x-y)(1-\zeta) \\
&= (x-y)\lambda
\end{aligned}$$

Ainsi,

$$\begin{aligned} N(\beta p\zeta^r) &= N((x-y)\lambda) \\ &= N(\lambda)N(x-y) \\ &= p(x-y)^{p-1} \end{aligned}$$

Avec

$$\begin{aligned} N(\beta p\zeta^r) &= N(\beta)N(p)N(\zeta^r) \\ &= p^{p-1}N(\beta) \end{aligned}$$

Donc

$$(x-y)^{p-1} = p^{p-2}N(\beta)$$

Comme $N(\beta) \in \mathbb{Z}$, alors $p|(x-y)^{p-2}$. Puisque p est premier, cela implique que p divise $x-y$.

D'où

$$x = y(\mathrm{mod}\, p\mathbb{Z})$$

9. D'après la question précédente, on a :

$$x = y(\mathrm{mod}\, p\mathbb{Z})$$

Par symétrie, on trouve également $z = y(\mathrm{mod}\, p\mathbb{Z})$

Alors,

$$\begin{cases} x^p = y^p(\mathrm{mod}\, p\mathbb{Z}) \\ z^p = y^p(\mathrm{mod}\, p\mathbb{Z}) \end{cases}$$

Ainsi

$$\begin{aligned} 3x^p &= x^p + y^p + z^p(\mathrm{mod}\, p\mathbb{Z}) \\ &= 0(\mathrm{mod}\, p\mathbb{Z}) \end{aligned}$$

Alors $p|3x^p$, avec $p > 3$, donc $p|x^p$, d'où $p|x$, ce qui est absurde avec $p \not| xyz$.

Pour aller plus loin...

Pour ceux qui sont intéressés par la démonstration du théorème de Wiles-Fermat (également connu sous le nom de dernier théorème de Fermat), je vous conseille de lire l'excellent livre *The Proof of Fermat's Last Theorem* de Nigel Boston, en cliquant sur le lien suivant :

https ://people.math.wisc.edu/˜boston/869.pdf

Ce document constitue une première étape d'un projet plus vaste. Son objectif est de rendre les informations accessibles à tous et d'offrir des chances équitables à celles et ceux qui se présentent aux concours post-prépa, en particulier aux étudiants rencontrant des difficultés financières.
Si vous souhaitez participer à notre projet (nous comptons produire d'autres documents, des vidéos, et organiser des séances de travail dès que possible), sachez que nous ne sommes que trois passionnés de mathématiques. Nous cherchons encore des collaborateurs !
Pour en savoir plus ou pour vous engager à nos côtés, n'hésitez pas à nous écrire à l'adresse suivante :

ilyass@steerai.autos

Les auteurs