Direction du Concours d'Admission

Concours d'admission à l'Ecole Polytechnique 2019

Filière MP

Mathématiques

Nous présentons une sélection d'exercices de mathématiques posés aux candidats de la filière MP lors du concours d'admission 2019. Pour chaque exercice, nous donnons des éléments d'une correction possible, les examinateurs étant évidemment ouverts à toutes les propositions des candidats dans le cadre du programme.

Certains exercices sont plus délicats et peuvent nécessiter des indications, qui seront apportées par les examinateurs au fil de l'interrogation (selon les besoins et les réactions des candidats), sans que ce soit a priori pénalisant.

Exercice 1

Enoncé

Si $p \geq 3$ est un nombre premier et si $x = (a/b)p^n$, avec

$$pgcd(a,b) = 1 \ , \ pgcd(a,p) = 1 \ , \ pgcd(p,b) = 1$$

est un nombre rationnel, on note $v(x) := v_p(x) = n$ (et $v(0) = \infty$).

1) Vérifier rapidement que pour tous x, y, m entiers

$$v(xy) = v(x) + v(y), \qquad v(x+y) \geq \min(v(x), v(y)),$$
$$v(m!) \leq \frac{m}{p-1}.$$

2) Si $P(X) = \sum_{j=1}^{N} a_j X^j$ est un polynôme à coefficients entiers, on note

$$v^{(i)}(P) = \min\{v(a_j) : j \geq i\}.$$

Montrer que si $m \in \mathbb{N}$ et

$$R(X) = (X - m)P(X),$$

on a $v^{(i)}(P) \geq v^{(i+1)}(R)$.

3) Soit $(d_n)_{n\in\mathbb{N}}$ une suite d'entiers de $\mathbb{Z}$. On note

$$b_n = \sum_{k=0}^{n} \binom{n}{k} d_k p^k. \tag{1}$$

Démontrer que si $\{n : b_n = 0\}$ est infini, $(b_n)_{n\in\mathbb{N}}$ est la suite nulle.

4) On considère la suite

$$u_{n+1} = 3u_n - 5u_{n-1}, \qquad u_0,\ u_1 \in \mathbb{Z}.$$

Démontrer que pour tout $(u_0, u_1) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ la suite (u_n) ne s'annule qu'un nombre fini de fois.

[On pourra observer que si $A = \begin{pmatrix} 3 & -5 \\ 1 & 0 \end{pmatrix}$ on a

$$A^2 = I + 3B$$

où $B \in M_2(\mathbb{Z})$.]

5) Soit

$$v_n := Re\left(\left(\frac{3}{2} + i\frac{\sqrt{11}}{2}\right)^n\right).$$

Démontrer que $\lim v_n = \infty$.

Eléments de correction

1) Les premières équations sont évidentes. Pour la seconde on constate que le nombre d'entiers inférieurs ou égaux à m divisibles par p^k est $[m/p^k] \leq m/p^k$. On a donc

$$v_p(m!) = \sum_{k\geq 1} k([m/p^k] - [m/p^{k+1}]) \leq \sum_{k\geq 1}(m/p^k) \leq \frac{m}{p-1}.$$

2) Si

$$P(X) = a_0 + \cdots + a_n X^n \text{ et } R(X) = b_0 + \cdots + b_{n+1}X^{n+1},$$

avec $a_n, b_n \neq 0$, on a

$$P(X) = \frac{R(X)}{X-m} = \left(\sum_{k=0}^{n+1} b_k X^k\right)\left(\sum_{l=0}^{\infty} m^l X^{-l-1}\right)$$

et donc

$$a_j = b_{j+1} + mb_{j+2} + \cdots + m^{n-j}b_{n+1} \text{ pour } j = 0, 1, \ldots.$$

D'après la question 1.

$$v(a_j) \geq \min_{l\geq j+1}(v(b_l)) = v^{(j+1)}(R) \geq v^{(i+1)}(R)$$

si bien qu'en prenant le min sur les $j \geq i$ on obtient

$$v^{(i)}(P) \geq v^{(i+1)}(R).$$

3) Supposons que $\{n : b_n = 0\}$ est infini et montrons que b_n est la suite nulle. Il suffit de démontrer que pour tout $q, u \in \mathbb{N}$ on a $v(b_q) \geq u$. Soit

$$R_n(x) = \sum_{k=0}^{n} \frac{d_k p^k}{k!} x(x-1)\cdots(x-k+1).$$

Pour tous entiers $m \leq n$,

$$R_n(m) = R_m(m) = b_m \tag{2}$$

$$v^{(i)}(R_n) \geq i - \frac{i}{p-1}. \tag{3}$$

En effet, pour $j \geq i$, le coefficient $a_j^{(n)}$ de x^j dans R_n est une combinaison linéaire à coefficients entiers des nombres $d_k p^k/k!$, $k \geq j$. D'après la question 1)

$$v\left(\frac{d_k p^k}{k!}\right) \geq v(d_k p^k) - v(k!) \geq k - \frac{k}{p-1} \geq j - \frac{j}{p-1}; \tag{4}$$

on a donc $v(a_j^{(n)}) \geq j - (j/p-1)$ et par conséquent $v^{(i)}(R_n) \geq i - (i/p-1)$.

Fixons alors q, u dans $\mathbb{N}$ et soit i tel que

$$i - \frac{i}{p-1} \geq u. \tag{5}$$

Notons $m_1 < m_2 \ldots < m_i$ les i premiers éléments de $\{n : b_n = 0\}$ et soit $n_0 = \max(q, m_i)$. D'après (2) on a

$$R_{n_0}(m_1) = \cdots = R_{n_0}(m_i) = 0 \tag{6}$$

et le polynôme R_{n_0} se factorise en

$$R_{n_0}(x) = (x - m_1) \cdots (x - m_i) P(x).$$

Comme $n_0 \geq q$ on a d'après (2) $b_q = R_{n_0}(q)$ et d'après (6) et la question 2. On a

$$v(b_q) = v(R_{n_0}(q)) \geq v(P(q)) \geq v^{(0)}(P) \geq v^{(i)}(R_{n_0}) \geq i - \frac{i}{p-1} \geq u. \tag{7}$$

4) On observe que

$$\begin{pmatrix} u_{k+1} \\ u_k \end{pmatrix} = \begin{pmatrix} 3 & -5 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_k \\ u_{k-1} \end{pmatrix}$$

si bien que

$$u_k = \begin{pmatrix} 0 & 1 \end{pmatrix} A^k \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}.$$

Si on fait la division euclidienne de k par 2 on peut écrire $k = 2n + \epsilon$, $\epsilon = 0, 1$ et

$$u_{2n+\epsilon} = \begin{pmatrix} 0 & 1 \end{pmatrix} (A^2)^n A^\epsilon \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}.$$

On constate que

$$A^2 = \begin{pmatrix} 3 & -5 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & -5 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 4 & -15 \\ 3 & -5 \end{pmatrix} = I + 3B,\ \ B \in M(2, \mathbb{Z})$$

et donc

$$u_{2n+\epsilon} = \begin{pmatrix} 0 & 1 \end{pmatrix} (I + 3B)^n A^\epsilon \begin{pmatrix} u_1 \\ u_0 \end{pmatrix}$$

est de la forme

$$u_{2n+\epsilon} = \sum_{k=0}^{n} \binom{n}{k} d_{k,\epsilon} 3^k \tag{8}$$

avec $d_{k,\epsilon} \in \mathbb{Z}$. Si la suite (u_n) s'annule une infinité de fois alors pour un certain $\epsilon \in \{0, 1\}$ la suite $u_{2n+\epsilon}$ s'annule une infinité de fois ; d'après la question 3. Elle doit être nulle :

$$0 = u_{2n+\epsilon} = u_{2n+2+\epsilon} = 3u_{2n+1+\epsilon} - 5u_{2n+\epsilon} \text{ pour } n \geq 0,$$

c'est-à-dire $2u_{2n+\epsilon} = u_{2n+1+\epsilon}$ et pour tout $n \geq 0$, $u_{n+\epsilon} = 0$. On doit donc avoir $u_0 = u_1 = 0$.

5) On constate que

$$v_n = (\lambda_+^n + \lambda_-^n)/2 \text{ où } \lambda_\pm = \frac{3 \pm i\sqrt{11}}{2}$$

sont les racines de $x^2 - 3x + 5 = 0$ et v_n vérifie la relation

$$v_{n+1} = 3v_n - 5v_{n-1}\ ,\ v_0 = 1\ ,\ v_1 = 3/2.$$

La suite $u_n = 2v_n$ est à coefficients entiers. Si $|u_n|$ ne tend pas vers l'infini, il existe $A > 0$ tel que pour une infinité d'indices n on a $u_n \in \mathbb{Z} \cap [-A, A]$ qui est un ensemble fini. Il existe donc $c \in \mathbb{Z}$ et $\epsilon \in \{0, 1\}$ tel que $u_{2n+\epsilon} - c$ s'annule une infinité de fois. La suite $u_{2n+\epsilon} - c$ est encore de la forme (8) ; elle doit donc être nulle pour tout $n \geq 0$:

$$c = u_{2n+\epsilon} = u_{2n+2+\epsilon} = 3u_{2n+1+\epsilon} - 5u_{2n+\epsilon}\ (n \geq 0)$$

c'est-à-dire $2u_{2n+\epsilon} = u_{2n+1+\epsilon} = 2c$. En particulier $u_{1+\epsilon}/u_\epsilon = 2$. Comme $u_1/u_0 = 3$ et $u_2/u_1 = -1/2$ on voit que c'est impossible.

Exercice 2

Enoncé

1) Soient P et Q deux polynômes unitaires de degré n. On suppose que les racines de P sont toutes de module 1 et que Q est à coefficients entiers. Démontrer que si p est un nombre premier ≥ 3 et si

$$P(X) = p^n Q\left(\frac{X-1}{p}\right)$$

alors $P(X) = (X-1)^n$.

2.a) Démontrer que l'ensemble des matrices de $GL(n, \mathbb{R})$ qui sont, avec leur inverse, à coefficients dans $\mathbb{Z}$, est un groupe et coïncide avec

$$\{A \in M(n, \mathbb{Z}) \cap GL(n, \mathbb{R}),\ \det A = \pm 1\}.$$

On le notera $GL(n, \mathbb{Z})$.

2.b) Soient deux matrices $A = (a_{ij})$ et $B = (b_{ij})$ de $GL(n, \mathbb{Z})$ et p un nombre premier. Démontrer que si pour tout $1 \leq i, j \leq n$, $a_{ij} \equiv b_{ij} \mod p$, alors la matrice AB^{-1} peut s'écrire sous la forme

$$I_n + pM$$

où $M \in M_n(\mathbb{Z})$ (est une matrice à coefficients entiers).

3) Soit G un sous-groupe fini de $GL(n, \mathbb{Z})$.

3.a) Démontrer que si les matrices A et B de la question précédente sont dans G alors $AB^{-1} = I$.

3.b) Démontrer qu'il existe une constante c_n ne dépendant que de n telle que

$$\mathrm{card(G) \leq c_n}.$$

Eléments de correction

1) On a $P(1) = p^n Q(0)$. Comme les racines de P (qui est unitaire) sont sur le cercle unité

$$|P(1)| \leq 2^n.$$

D'autre part, comme Q est à coefficients entiers, $|p^n Q(0)|$ est soit nul soit $\geq 3^n$. Comme $2^n \leq 3^n$ on doit avoir $Q(0) = 0$ et donc $P(1) = 0$. En particulier $X - 1$ divise P et X divise Q. Posons

$$P(X) = \tilde{P}(X)(X-1) \text{ et } Q(X) = X\tilde{Q}(X).$$

On a

$$(X-1)\tilde{P}(X) = p^n \frac{X-1}{p} \tilde{Q}\left(\frac{X-1}{p}\right)$$

où $\tilde{P}$ a toutes ses racines sur le cercle unité et $\tilde{Q}$ est à coefficients entiers. On a ainsi

$$\tilde{P}(X) = p^{n-1} \tilde{Q}\left(\frac{X-1}{p}\right)$$

et à nouveau $\tilde{P}$ est divisible $X - 1$ et $\tilde{Q}$ par X. Par récurrence on obtient donc la conclusion.

2.a) Que ce soit un groupe est clair. Si $A, A^{-1} \in M(n, \mathbb{Z})$ alors $(\det A)^{\pm 1} \in \mathbb{Z}$ et $\det A = \pm 1$. Réciproquement si A à coefficients entiers est inversible et $\det A = \pm 1$ on voit que

$$A^{-1} = (\det(A))^{-1}\, {}^t\text{Com }(A)$$

est à coefficients entiers (en notant Com (A) la comatrice de A).

2.b) On peut écrire $A = B + pL$ où $L \in M(n, \mathbb{Z})$. On a donc

$$AB^{-1} = I + pLB^{-1}$$

et $LB^{-1} \in M(n, \mathbb{Z})$ d'après la question précédente.

3.a) La matrice $C = AB^{-1} = I + pM$ est dans G. Comme G est fini on a d'après le théorème de Lagrange $C^N = I$ où $N =$ card G. Comme le polynôme $X^N - 1$ est scindé à racines simples, la matrice $C = I + pM$ est diagonalisable de valeurs propres les racines N-ièmes de l'unité. Si

$$\chi_C(X) = \det(XI - C) \text{ et } \chi_M(X) = \det(XI - M)$$

sont les polynômes caractéristiques de C et M on a

$$\chi_C(X) = \det(XI - I - pM) = \det((X-1)I - pM) = p^n \det\left(\frac{X-1}{p} - M\right)$$

d'où

$$\chi_C(X) = p^n \chi_M\left(\frac{X-1}{p}\right).$$

On peut appliquer le résultat de la question 1 : $\chi_C(X) = (X-1)^n$. Comme C est diagonalisable cela implique que $C = I$.

3.b) Le résultat de 3.a) montre que l'application qui à une matrice A de G associe la liste de ses coefficients modulo p est injective. Par conséquent G a moins d'éléments que $(\mathbb{Z}/p\mathbb{Z})^{n^2}$. En particulier si on prend $p = 3$ on trouve $c_n \leq 3^{(n^2)}$.

Exercice 3

Enoncé

1) Soit $P(X) \in \mathbb{C}[X]$ un polynôme de degré $n \geq 1$. On suppose que P n'admet pas de racines sur le cercle $C(0, r)$ de centre 0 et de rayon r. Démontrer que le nombre $N_r(P)$ de racines de P dans le disque (ouvert) $\mathbb{D}(0, r)$ de centre 0 et de rayon r est égal à

$$N_r(P) = \frac{1}{2\pi i} \int_0^{2\pi} \frac{P'(re^{i\theta})}{P(re^{i\theta})} ire^{i\theta} d\theta.$$

2) En déduire que si Q est un polynôme de degré $\leq n - 1$ tel que

$$\min_{t \in [0,1]} \min_{|z|=r} |(P + tQ)(z)| \neq 0$$

alors

$$N_r(P) = N_r(P + Q).$$

3) On considère un polynôme de degré n, $P(z) = \sum_{j=0}^{n} a_j z^j$. Supposons que pour $0 \leq k < l \leq n$ on ait la condition $C(k,l)$ suivante :

il existe $s, r \in \mathbb{R}$ tels que:

$$\ln|a_k| = s - kr, \quad \ln|a_l| = s - lr$$
$$h := \min_{\substack{0\leq j\leq n \\ j\neq k,l}} (s - jr - \ln|a_j|) > 0.$$

Démontrer que si $\delta > 0$ est tel que $ne^{\delta n - h} < 1 - e^{-\delta}$ alors le nombre de racines de P dans l'anneau $\{z | e^{r-\delta} < |z| < e^{r+\delta}\}$ est exactement égal à $l - k$.

Eléments de correction

1) On constate que

$$\frac{P'(z)}{P(z)} = \sum_{j=1}^{n} \frac{1}{z - z_j}$$

où les z_j sont les racines de P. On calcule alors

$$\frac{1}{2\pi} \int_0^{2\pi} \frac{re^{i\theta}}{re^{i\theta} - w} d\theta = \begin{cases} 1 \text{ si } |w| < r, \\ 0 \text{ si } |w| > r. \end{cases}$$

(Par exemple si $|w| < r$ on développe le quotient comme série uniformément convergente $\sum_{k=0}^{\infty}((w/r)e^{-i\theta})^k$ et en intégrant on trouve 1 ; si $|w| > r$ on développe le quotient comme série uniformément convergente $-\sum_{k=0}^{\infty}((r/w)e^{i\theta})^{k+1}$ et en intégrant on trouve 0).

2) D'après la question 1)

$$N_r(P + tQ) = \frac{1}{2\pi i} \int_0^{2\pi} \frac{(P + tQ)'(re^{i\theta})}{(P + tQ)(re^{i\theta})} ire^{i\theta} d\theta.$$

Cette dernière quantité est continue (d'après le théorème de continuité sous l'intégrale) et à valeurs entières : elle est donc constante.

3) On introduit

$$P_t(z) = a_k z^k + a_l z^l + t \sum_{j\neq k,l} a_j z^j, \quad 0 \leq t \leq 1.$$

En particulier $P_0(z) = a_k z^k + a_l z^l$ et $P_1(z) = P(z)$. Soit $z \in \mathbb{C}$ tel que $|z| = e^{r-\delta}$. D'après la condition $C(k,l)$ on a

$$t\Big|\sum_{j\neq k,l} a_j z^j\Big| \leq \sum_{j\neq k,l} e^{s-jr-h} e^{j(r-\delta)} < ne^{s-h}.$$

Toujours d'après la condition $C(k,l)$ on a

$$|a_k z^k + a_l z^l| \geq |a_k z^k| - |a_l z^l| = e^s e^{-\delta k}(1 - e^{-\delta(l-k)}) > e^{s-\delta n}(1 - e^{-\delta}).$$

Puisque $ne^{\delta n - h} < 1 - e^{-\delta}$ on pour tout z sur le cercle $|z| = e^{r-\delta}$

$$|a_k z^k + a_l z^l| > t\Big|\sum_{j\neq k,l} a_j z^j\Big|. \tag{9}$$

Comme $P_0(z) = a_k z^k + a_l z^l$ a exactement k zéros dans le disque $|z| \leq e^{r-\delta}$ on déduit de la question 2) qu'il en est de même de $P_1(z) = P(z)$.

Soit maintenant $z \in \mathbb{C}$ tel que $|z| = e^{r+\delta}$. Alors,

$$t\Big|\sum_{j\neq k,l} a_j z^j\Big| \leq \sum_{j\neq k,l} e^{s-jr-h} e^{j(r+\delta)} < ne^{s-h+\delta n}. \tag{10}$$

D'autre part,

$$|a_k z^k + a_l z^l| \geq |a_l z^l| - |a_k z^k| = e^s e^{\delta l}(1 - e^{\delta(k-l)}) > e^s(1 - e^{-\delta}). \tag{11}$$

Par conséquent l'inégalité (9) est vraie sur le cercle $|z| = e^{r+\delta}$. D'après la question 2) le polynôme $P(z)$ a donc exactement l racines (le nombre de racines de P_0) dans le disque $|z| \leq e^{r+\delta}$.

En conclusion, le polynôme P a exactement $l - k$ racines dans l'anneau $e^{r-\delta} \leq |z| \leq e^{r+\delta}$.

Exercice 4

Enoncé

Soient $A \in M_n(\mathbb{R})$, $B \in M_{n,p}(\mathbb{R})$ et $T \in \mathbb{R}$. On note $\mathcal{A}_T$ l'ensemble des $v \in \mathbb{R}^n$ pour lesquels il existe $u : [0,T] \to \mathbb{R}^p$ continue telle que la solution de l'équation différentielle

$$X'(t) = AX(t) + Bu(t) \ , \ X(0) = 0$$

vérifie $X(T) = v$.

1) Démontrer que $\mathcal{A}_T = \mathbb{R}^n$ si et seulement si le rang de la matrice

$$[B, AB, \ldots, A^{n-1}B]$$

est égal à n.

2) On note

$$G = \int_0^T e^{(T-s)A} B \ {}^tB \ {}^t(e^{(T-s)A}) ds.$$

Démontrer que $\operatorname{Im} G = \mathcal{A}_T$.

3) On suppose G inversible. On note

$$\bar{u}(s) = {}^t(e^{(T-s)A} B) G^{-1} v.$$

Démontrer que si $u \in C^0([0,T], \mathbb{R}^p)$ est telle que la solution de $X'(t) = AX(t) + Bu(t)$, $X(0) = 0$ vérifie $X(T) = v$ alors

$$\int_0^T \|u(s)\|^2 ds \geq \int_0^T \|\bar{u}(s)\|^2 ds.$$

Eléments de correction

1) La solution de $X'(t) = AX(t) + Bu(t)$, $X(0) = 0$ vérifie $X(T) = \int_0^T e^{(T-s)A} Bu(s) ds$.

On a $\dim \mathcal{A}_T < n$ si et seulement s'il existe $Y \in \mathbb{R}^n$ non nul tel que $\langle Y, v \rangle = 0$ pour tout $v \in \mathcal{A}_T$. En particulier si on choisit $u(s) = {}^tB^t(e^{(T-s)A})Y$ on a

$$0 = {}^tY \int_0^T e^{(T-s)A} Bu(s) ds = \int_0^T \|{}^tB^t e^{(T-s)A} Y\|^2 ds$$

et donc pour tout $s \in [0,T]$, ${}^tYe^{(T-s)A}B = 0$. Si on dérive successivement cette relation par rapport à s en $s = T$ on obtient ${}^tYA^kB = 0$ c'est-à-dire $\mathrm{rg}[B, AB, \ldots, A^{n-1}B] < n$.

Réciproquement si $\mathrm{rg}[B, AB, \ldots, A^{n-1}B] < n$ il existe $Y \in \mathbb{R}^n$ tel que ${}^tYA^kB = 0$ pour tout k et donc ${}^tYe^{(T-s)A}B = 0$. On a alors, pour tout u continue, ${}^tY \int_0^T e^{(T-s)A}Bu(s)ds = 0$.

2) Même preuve que précédemment.

3) Si on note $E(u) = (1/2)\int_0^T \|u(t)\|^2 dt$ on a

$$E(u) = E(\bar{u}) + \int_0^T \langle {}^t(e^{(T-s)A}B)G^{-1}v, u(s) - \bar{u}(s)\rangle ds + E(u - \bar{u})$$

soit

$$E(u) = E(\bar{u}) + \int_0^T \langle G^{-1}v, e^{(T-s)A}B(u(s) - \bar{u}(s))\rangle ds + E(u - \bar{u}).$$

Mais pour $\bar{X}$ solution associée à $\bar{u}$, on a

$$0 = X(T) - \bar{X}(T) = \int_0^T e^{(T-s)A}B(u(s) - \bar{u}(s))ds.$$

D'où le résultat.

Exercice 5

Enoncé

Soit P un polynôme unitaire de degré d à coefficients entiers. On suppose qu'il admet d racines $\lambda_1, \cdots, \lambda_d$ telles que $\forall k = 1, \ldots d$, $|\lambda_k| \leq 1$.

1) On pose pour $n \in \mathbb{N}$,

$$f(n) = \sum_{k=1}^{d} \lambda_k^n.$$

Démontrer que f ne prend que des valeurs entières et qu'il existe $p \in \mathbb{N}^*$ tel que pour tout $n \in \mathbb{N}$ assez grand

$$f(n + p) = f(n).$$

2) Démontrer que les λ_k sont des racines de l'unité ou sont nulles.

Eléments de correction

1) On peut supposer que les λ_k sont non-nulles (sinon on met en facteur une puissance de X). On introduit A la matrice compagnon associée à P. Son polynôme caractéristique est P et ses valeurs propres sont les λ_k, comptées avec multiplicité. On a donc

$$f(n) = \sum_{k=1}^{d} \lambda_k^n = \mathrm{tr}(A^n).$$

Comme A est à coefficients entiers on voit que f ne prend que des valeurs entières.

D'autre part, d'après Cayley-Hamilton $A^d = a_1 A^{d-1} + \cdots + a_d I_d$ où les a_k sont entiers et donc $A^{n+d} = a_1 A^{n+d-1} + \cdots + a_d A^n$. Par conséquent pour tout $n \in \mathbb{N}$

$$f(n+d) = a_1 f(n+d-1) + \cdots + a_d f(n)$$

La suite $f(n)$ est bornée (disons par M), prend des valeurs entières et vérifie une relation de récurrence linéaire (à coefficients constants). Elle est déterminée par d valeurs consécutives ; mais comme $([-M,M] \cap \mathbb{Z})^d$ est fini, il existe $n_0 \in \mathbb{N}$ et $p \in \mathbb{N}^*$ tel que

$$(f(n_0), \ldots, f(n_0+d-1)) = (f(n_0+p), \ldots, f(n_0+d-1+p)).$$

Par conséquent pour tout $n \geq n_0$, $f(n) = f(n+p)$.

2) On a d'après la question précédente $f(n) = f(n+lp)$ pour tout $l \geq 0$ et tout $n \in \mathbb{N}$, $n \geq n_0$:

$$f(n) = \sum_{k=1}^{d} \lambda_k^{n+lp}.$$

On somme ces identités sur l et on moyenne :

$$f(n) = \frac{1}{L} \sum_{l=0}^{L} \sum_{k=1}^{d} \lambda_k^{n+lp}$$

soit en intervertissant les sommations

$$f(n) = \sum_{k=1}^{d} \lambda_k^n \frac{1}{L} \sum_{l=0}^{L} \lambda_k^{lp}.$$

On observe que si

$$\begin{cases} \text{si } \lambda_k^p \neq 1, & \lim_{L\to\infty} \frac{1}{L} \sum_{l=0}^{L} \lambda_k^{lp} = \lim_{L\to\infty} \frac{1}{L} \frac{1-\lambda_k^{pL}}{1-\lambda_k^p} = 0 \\ \text{si } \lambda_k^p = 1, & \lim_{L\to\infty} \frac{1}{L} \sum_{l=0}^{L} \lambda_k^{lp} = 1 \end{cases}$$

si bien qu'en notant

$$J = \{\lambda_k,\ k \in \{1, \ldots, d\} :\ \lambda_k^p = 1\}$$

et m_λ la multiplicité de λ

$$f(n) \begin{cases} = \sum_{k=1}^{d} \lambda_k^n & \text{(définition de } f) \\ = \sum_{\lambda \in J} m_\lambda \lambda^n & \text{(d'après ce qui précède)} \end{cases}$$

et donc

$$\forall\ n \geq n_0, \quad \sum_{\lambda \in J^c} m_\lambda \lambda^n = 0.$$

Si le cardinal du complémentaire J^c de J vérifie $\text{card}(J^c) \neq 0$, on peut écrire un système de Vandermonde et voir que tout $\lambda \in J^c$ est nul, ce qui contredit l'hypothèse que les λ_k sont non-nuls. On doit donc avoir $J^c = \emptyset$ et donc toutes les valeurs propres de A (les racines non-nulles de P) sont des racines p-ièmes de l'unité.

Exercice 6

Enoncé

a) Soient $K \subset \mathbb{R}$ un $\mathbb{Q}$-espace vectoriel de dimension finie. Démontrer que pour $a, b \in K$ avec $a/b \notin \mathbb{Q}$, il existe $\varphi : K \to \mathbb{R}$ additive, c'est-à-dire telle que

$$\varphi(x+y) = \varphi(x) + \varphi(y) \text{ pour tous } x, y \in K,$$

et telle que $\varphi(a) = 1 = -\varphi(b)$.

b) Démontrer que si pour tout $(x_1, x_2, y_1, y_2) \in K$ on définit

$$\mu([x_1, x_2] \times [y_1, y_2]) = \varphi(x_2 - x_1)\varphi(y_2 - y_1)$$

alors, pour tous $x_{i,k}, y_{i,k}$, $i = 1, 2$, $k = 0, 1, \ldots, n$ dans K vérifiant

$$[x_{1,0}, x_{2,0}] \times [y_{1,0}, y_{2,0}] = \bigcup_{k=1}^{n} [x_{1,k}, x_{2,k}] \times [y_{1,k}, y_{2,k}],$$

la réunion étant disjointe, on a:

$$\mu([x_{1,0}, x_{2,0}] \times [y_{1,0}, y_{2,0}]) = \sum_{k=1}^{n} \mu([x_{1,k}, x_{2,k}] \times [y_{1,k}, y_{2,k}]).$$

c) En déduire que s'il existe une partition d'un rectangle, de côtés la longueur respectives a, b, en carrés, alors $a/b \in \mathbb{Q}$.

d) Démontrer que s'il existe une partition d'un carré de côté de longueur 1, en carrés, alors ces carrés sont de côtés rationnels.

Eléments de correction

a) La famille $\{a, b\}$ est libre sur $\mathbb{Q}$ et peut être complétée en une base sur $\mathbb{Q}$. Il existe donc une forme $\mathbb{Q}$-linéaire $\varphi \in K^* : K \to \mathbb{Q}$ telle que dans la base $(a, b, *)$, φ prend la forme $(1, -1, *)$.

b) C'est dû à l'additivité de φ.

c) Etant donnée une partition d'un rectangle R (de côtés a, b) en carrés C_i, $i = 1, \ldots, p$, on peut construire, en prolongeant les cotés des carrés à tout le rectangle R, une partition $R = \cup R_k$ en rectangles contigus

$$R = \bigcup_{k=1}^{n} [x_{1,k}, x_{2,k}] \times [y_{1,k}, y_{2,k}]$$

et chaque carré C_i est (modulo les bords) une union disjointe de certains R_k. Soit K le $\mathbb{Q}$-espace vectoriel de dimension finie engendré par les x_k, y_k, a, b. En supposant $a/b \notin \mathbb{Q}$, on peut introduire la forme linéaire du a) et μ construite comme en b). D'après b) on a donc $\mu(R) = \sum_i \mu(C_i)$ et toujours par b)

$$-1 = \varphi(a)\varphi(b) = \sum_i \varphi(C_i)^2.$$

Remarquons que les $\varphi(C_i)$ sont réels (dans $\mathbb{Q}$) et donc $(\varphi(C_i))^2 \geq 0$. On obtient donc $-1 \geq 0$ ce qui est absurde.

d) On procède comme précédemment mais avec le choix suivant pour φ. Etant donné c_i la longueur d'un des côtés de φ qu'on suppose irrationnel, on construit φ de façon que $\varphi(1) = 0$ et $\varphi(c_i) = 1$.

Remarque : Ce sont des résultats dûs à Dehn au début du 20e siècle.

Exercice 7

Enoncé

Soient $m_1, \ldots, m_n$ des constantes positives et $x_1, \ldots, x_n$ des réels strictement positifs. Posons

$$g(x) = \sum_{k=1}^{n} \frac{m_k}{x - x_k}.$$

Montrer que l'ensemble des réels x pour lesquels $g(x)$ est défini et vérifie

$$g(x) > \lambda \text{ (avec } \lambda > 0)$$

est une union finie d'intervalles dont la somme $l(\lambda)$ des longueurs $l_i(\lambda)$ vérifie

$$l(\lambda) = \frac{1}{\lambda} \sum_{k=1}^{n} m_k.$$

Eléments de correction

Si on note $c_k(\lambda)$ les racines de l'équation $g(x) = \lambda$ on a

$$l(\lambda) = \sum_{k=1}^{n} (c_k(\lambda) - x_k).$$

En multipliant $g(x) - \lambda$ par $(x - x_1) \cdots (x - x_n)$ on voit que les $c_i(\lambda)$ sont les racines de

$$0 = \lambda \prod_{k=1}^{n} (x - x_k) - \sum_{k=1}^{n} m_k \sum_{l=1, l \neq k}^{n} (x - x_l).$$

L'examen du coefficient de degré $n - 1$ en x montre que

$$\sum_{k=1}^{n} c_k(\lambda) = \sum_{k=1}^{n} x_k + \frac{1}{\lambda} \sum_{k=1}^{n} m_k,$$

ce qui est le résultat.

Exercice 8

Enoncé

Soit un polynôme

$$P(x) = \sum_{k=0}^{n} a_k x^k$$

à coefficients réels dont les zéros sont réels. Démontrer que pour tout $1 \leq k \leq n - 1$,

$$a_{k-1} a_{k+1} \leq a_k^2.$$

Eléments de correction

On a $a_k = P^{(k)}(0)/k!$ et on observe que

$$(k-1)!(k+1)! \geq (k!)^2.$$

Il suffit donc de démontrer que

$$P^{(k-1)}(0) P^{(k+1)}(0) \leq (P^{(k)}(0))^2.$$

Le polynôme $Q = P^{(k-1)}$ n'a que des zéros réels d'après le théorème de Rolle. Vérifions que $Q(x)''Q(x) \leq (Q'(x))^2$: la fonction $-\log|Q(x)|$ est convexe entre les zéros de Q car sa dérivée seconde est une somme de termes de la forme $1/(x-\lambda)^2$.

Exercice 9

Enoncé

1.a) Soit une suite $(x_n)_{n\in\mathbb{N}}$ de réels positifs telle que pour tous $n, m \in \mathbb{N}$,

$$x_{n+m} \leq x_n + x_m.$$

Démontrer que la suite (x_n/n) converge vers

$$l = \inf_{n\geq 1}(x_n/n).$$

1.b) Soient (y_n) une suite positive telle que pour tous $n, m \in \mathbb{N}^*$

$$y_{n+m} \leq \frac{n^2}{(n+m)^2} y_n + \frac{m^2}{(n+m)^2} y_m + \epsilon_{n,m}$$

où on suppose que $(\epsilon_{n,m})_{n,m}$ est une suite positive telle que

$$\lim_{n,m\to\infty} \epsilon_{n,m} = 0.$$

Démontrer que y_n converge vers 0.

2) On considère une suite de variables aléatoires indépendantes et de même loi

$$U_1, \ldots, U_n, \ldots$$

à valeurs discrètes dans $\mathbb{R}_+$ et $f_n : \mathbb{R}^n \to \mathbb{R}_+$ ($n \geq 1$) des fonctions positives. On suppose que pour tous n, m entiers

$$f_{n+m}(U_1, \ldots, U_{n+m}) \leq f_n(U_1, \ldots, U_n) + f_m(U_{n+1}, \ldots, U_{n+m}). \ (*)$$

On pose $X_n = f_n(U_1, \ldots, U_n)$ et on suppose que $\mathbb{E}(X_n) < \infty$.

2.a) Démontrer que la suite $(1/n)\mathbb{E}(X_n)$ converge vers une limite que l'on notera L.

2.b) Démontrer que pour tout $\epsilon > 0$

$$\lim_{n\to\infty} \mathbb{P}\left(|\frac{X_n}{n} - L| \geq \epsilon\right) = 0.$$

Eléments de correction

1.a) Notons $L = \inf_{n\geq 1}(x_n/n)$. Soit $\epsilon > 0$ et q tel que $L \leq x_q \leq L + \epsilon$. Pour tout $n \in \mathbb{N}$, on fait la division euclidienne de n par q: il existe m tel que $n = mq + r$, $0 \leq r < q$. On a alors

$$x_n \leq mx_q + x_r$$

d'où

$$\begin{aligned} L \leq \frac{x_n}{n} &\leq \frac{qm}{n}\frac{x_q}{q} + \frac{1}{n}\max_{0\leq j\leq q-1} x_j \\ &\leq (L+\epsilon) + \frac{1}{n}\max_{0\leq j\leq q-1} x_j \end{aligned}$$

ce qui donne

$$L \leq (x_n/n) \leq L + 2\epsilon$$

dès que n est assez grand.

1.b) On constate que si $n = m$ on a

$$y_{2n} \leq (1/2)y_n + \epsilon_{n,n}$$

et il n'est pas difficile de voir que y_{2^n} tend vers 0. Cela suggère de procéder de la façon suivante. Notons A_k ($k \in \mathbb{N}$) (la couronne dyadique) :

$$\mathcal{A}_k = [2^k, 3 \times 2^k] \cap \mathbb{N}.$$

Pour tout k, $\mathcal{A}_k \cap \mathcal{A}_{k+1} \neq \emptyset$ et
$$\mathbb{N}^* = \bigcup_{k\geq 0} \mathcal{A}_k.$$
On remarque que tout $l \in \mathcal{A}_{k+1}$ s'écrit comme somme de deux éléments de $\mathcal{A}_k$, $l = n + m$, $n, m \in \mathcal{A}_k$ où n et m sont comparables (c'est-à-dire que leur rapport est dans $[1/2, 2]$). En effet, considérons $l \in \mathcal{A}_{k+1}$. Soit $l = 2l'$ est pair
$$2^{k+1} \leq l = 2l' \leq 3 \times 2^{k+1}$$
et on a $l' \in \mathcal{A}_k$. Soit $l = 2l' + 1$ est impair et
$$2^{k+1} < l = 2l' + 1 < 3 \times 2^{k+1}$$
si bien que $l' + 1 \leq 3 \times 2^k$ et $2^k \leq l'$ et donc $l', l' + 1 \in \mathcal{A}_k$, $2l = l' + (l' + 1)$. Posons $l'' = l'$ si l est pair et $l'' = l' + 1$ si l est impair. On a
$$y_l \leq \frac{l'^2}{l^2} y_{l'} + \frac{l''^2}{l^2} y_{l''} + \epsilon_{l',l''}.$$
Notons $u_k = \max_{n\in\mathcal{A}_k} y_n$ et $\tilde{\epsilon}_k = \max_{n,m\in\mathcal{A}_k} \epsilon_{n,m}$. L'inégalité précédente montre que pour $\lambda = 3/4$ il existe k_0 tel que pour $k \geq k_0$
$$u_{k+1} \leq \lambda u_k + \tilde{\epsilon}_k$$
et
$$u_N \leq \lambda^{N-k_0} u_{k_0} + \sum_{j=1}^{N-k_0} \lambda^{j-1} \tilde{\epsilon}_{N-j}.$$
Comme $\lim_{k\to\infty} \tilde{\epsilon}_k = 0$ on a bien $\lim u_N = 0$ d'où le résultat.

2.a) En prenant l'espérance dans $(*)$ on a
$$\mathbb{E}(X_{n+m}) \leq \mathbb{E}(X_n) + \mathbb{E}(f_m(U_{n+1}, \ldots, U_{n+m})).$$
Comme le vecteur aléatoire $(U_{n+1}, \ldots, U_{n+m})$ a même loi que $(U_1, \ldots, U_m)$ on a
$$\mathbb{E}(f_m(U_{n+1}, \ldots, U_{n+m})) = \mathbb{E}(f_m(U_1, \ldots, U_m)),$$

et donc

$$\mathbb{E}(X_{n+m}) \leq \mathbb{E}(X_n) + \mathbb{E}(X_m).$$

On peut appliquer le résultat de 1.a) :

$$\lim_{n\to\infty}(1/n)\mathbb{E}(X_n) = L := \inf_{n\geq 1}(1/n)\mathbb{E}(X_n).$$

2.b) On essaie de majorer la variance de $X_{n+m}/(n+m)$: en notant $X_m^{(n)} := f_m(U_{n+1},\ldots,U_{n+m})$ on a

$$X_{n+m}^2 \leq X_n^2 + (X_m^{(n)})^2 + 2X_nX_m^{(n)}.$$

Les variables aléatoires X_n et $X_m^{(n)}$ sont indépendantes et on a donc

$$\mathbb{E}(X_{n+m}^2) \leq \mathbb{E}(X_n^2) + \mathbb{E}((X_m^{(n)})^2) + 2\mathbb{E}(X_n)\mathbb{E}(X_m^{(n)}).$$

Comme $X_m^{(n)}$ et X_m ont même loi on a

$$\mathbb{E}(X_{n+m}^2) \leq \mathbb{E}(X_n^2) + \mathbb{E}(X_m^2) + 2\mathbb{E}(X_n)\mathbb{E}(X_m)$$

et donc en notant $Y_n = X_n/n$

$$\mathbb{E}(Y_{n+m}^2) \leq \frac{n^2}{(n+m)^2}\mathbb{E}(Y_n^2) + \frac{m^2}{(n+m)^2}\mathbb{E}(Y_m^2) + \frac{2nm}{(n+m)^2}\mathbb{E}(Y_n)\mathbb{E}(Y_m).$$

On a donc en posant $A_{n,m} := -(\mathbb{E}(Y_{n+m}))^2 + (\frac{n}{n+m}\mathbb{E}(Y_n) + \frac{m}{n+m}\mathbb{E}(Y_m))^2$

$$Var(Y_{n+m}) \leq \frac{n^2}{(n+m)^2}Var(Y_n) + \frac{m^2}{(n+m)^2}Var(Y_m) + A_{n,m}.$$

On sait que $\lim \mathbb{E}(Y_n) = L$; en particulier pour tout $\delta > 0$ il existe N tel que pour tout $k \geq N$, $L \leq \mathbb{E}(Y_k) < L + \delta$. Par conséquent, pour tout $m, n \geq N$ on a

$$L \leq \frac{n}{n+m}\mathbb{E}(Y_n) + \frac{m}{n+m}\mathbb{E}(Y_m) < L + \delta$$

et donc

$$A_{n,m} < (L+\delta)^2 - L^2 \leq 3\delta(1+L)$$

si δ est suffisamment petit. On a donc

$$\lim_{n,m\to\infty} A_{n,m} = 0.$$

En posant $y_n = Var(Y_n)$ on obtient pour $m \geq N$, $n \geq 1$

$$y_{n+m} \leq \frac{n^2}{(n+m)^2} y_n + \frac{m^2}{(n+m)^2} y_m + A_{n,m}$$

et on peut appliquer le résultat du 1.b) :

$$\lim_{n\to\infty} Var(Y_n) = 0.$$

On conclut par l'inégalité de Bienaymé-Tchebychev : pour tout $\epsilon > 0$,

$$\mathbb{P}(|Y_n - L| \geq \epsilon) \leq (1/\epsilon^2) Var(Y_n) \to_{n\to\infty} 0.$$

Exercice 10

Enoncé

Quels sont les idéaux maximaux de l'anneau des fonctions continues $\mathcal{C}^0([0,1])$ qui sont strictement inclus dans $\mathcal{C}^0([0,1])$?

Eléments de correction

Ce sont les parties de la forme

$$M_a = \{f \in \mathcal{C}^0([0,1]),\ f(a) = 0\}$$

avec $a \in [0,1]$. Si un idéal I n'est pas de cette forme, on montre qu'il existe un recouvrement fini de $[0,1]$ par des ouverts V_1, ..., V_n et des fonctions f_1, ..., f_n dans I telles que, pour tout i, f_i ne s'annule pas sur V_i, et on en conclut que la fonction inversible

$$f_1^2 + ... + f_n^2$$

appartient à I, et donc que $I = \mathcal{C}^0([0,1])$.

Commentaire: La propriété de Borel-Lebesgue n'est pas au programme (existence du recouvrement fini de $[0,1]$). Il conviendra donc de l'établir dans ce cas particulier.

Exercice 11

Enoncé

Soit G un groupe fini. Pour $x \in G$, on note

$$\bar{x} = \{gxg^{-1},\ g \in G\}$$

et on dit que x est ambivalent si $x^{-1} \in \bar{x}$ (cette propriété ne dépend pas de l'élément choisi dans une classe $\bar{x}$). On note encore $\rho(x)$ le nombre d'éléments $g \in G$ tels que $x = g^2$.

1) Montrer que le nombre de classes ambivalentes est

$$\frac{1}{|G|}\sum_{x \in G} \rho(x)^2.$$

On note maintenant $\gamma(x)$ le nombre d'éléments $g \in G$ tels que $gx = xg$.

2) Montrer que $\bar{x}$ est ambivalente pour tout x si et et seulement si

$$\sum_{x \in G} \rho(x)^2 = \sum_{x \in G} \gamma(x).$$

3) Montrer que le groupe alterné A_4 des permutations paires à 4 éléments ne vérifie pas cette dernière propriété.

Eléments de correction

1) En utilisant le symbole de Kronecker, on a

$$\rho(x) = \sum_{y \in G} \delta_{x,y^2},$$

et

$$\sum_{x\in G}\rho(x)^2=\sum_{x,y\in G}\rho(x)\delta_{x,y^2}=\sum_{y\in G}\rho(y^2)=\sum_{y,z\in G}\delta_{y^2,z^2}=\sum_{x,z\in G}\delta_{zxzx,z^2}=\sum_{x,z\in G}\delta_{x,zx^{-1}z^{-1}},$$

donc

$$\sum_{x\in G}\rho(x)^2=\sum_{x\,\text{ambivalent}}\frac{|G|}{|\bar{x}|}=|G|\alpha,$$

où α est le cardinal recherché.

Remarque : il n'est pas attendu que le candidat connaisse a priori la relation entre le cardinal de la classe de conjugaison d'un élément x et celui du sous-groupe des éléments commutant avec x.

2) Supposons que

$$\sum_{x\in G}\rho(x)^2=\sum_{x\in G}\gamma(x).$$

D'après la première question, $\sum_{x\in G}\gamma(x)=\alpha|G|$ et, par ailleurs, $\gamma(x)=|G|/|\bar{x}|$, donc

$$\sum_{x\in G}\gamma(x)=|G|\sum_{x\in G}\frac{1}{|\bar{x}|}=|G|\,\left|\{\bar{x},\,x\in G\}\right|.$$

Donc

$$\alpha=|\{\bar{x},\,x\in G\}|$$

et G est ambivalent. La réciproque est analogue.

3) Si $x\in A_4$ est une permutation circulaire avec un point fixe (disons qui permute les éléments (a,b,c)), les éléments $\sigma\in S_4$ tels que $\sigma x\sigma^{-1}=x^{-1}$ sont impairs (par exemple la transposition (ab)). Donc x est ambivalent dans S_4, mais pas dans A_4.

Exercice 12

Enoncé

Soit x une fonction $\mathcal{C}^1$ au voisinage de 0, telle que

$$x'(t)=3x(t)+85\cos(x(t))\text{ et }x(0)=77.$$

Montrer que x se prolonge en une solution de cette équation différentielle sur $\mathbb{R}$ entier.

Eléments de correction

La fonction $x(t)$ est strictement monotone dans un voisinage de 0, et sa bijection réciproque $t(x)$ vérifie

$$t(x) = \int_{77}^{x} \frac{dy}{3y + 85\cos y}$$

au voisinage de $x = 77$. Soit α la première racine de $3x + 85\cos x$ à gauche de 77. Alors t est bien définie (au moins) sur $]\alpha, +\infty[$. Au voisinage de α,

$$3x + 85\cos x = (3 - 85\sin\alpha)(x - \alpha) + \mathcal{O}(x - \alpha)^2,$$

donc l'application

$$x \mapsto \frac{3x + 85\cos x}{x - \alpha}$$

a une limite non nulle en α, et égale à 3 en $+\infty$. Donc $t(x)$ tend vers $-\infty$ en α et vers $+\infty$ en $+\infty$. Sa bijection réciproque est donc bien définie sur $\mathbb{R}$, et l'on vérifie qu'elle est une solution de l'équation différentielle, qui prolonge la solution locale initiale.

Exercice 13

Enoncé

Soient E un espace vectoriel complexe de dimension finie et $\mathcal{F}$ une famille d'endomorphismes diagonalisables de E, qui commutent deux à deux. Montrer qu'il existe un endomorphisme g de E tel que tout endomorphisme de $\mathcal{F}$ soit un polynôme en g.

Eléments de correction

On commence par constater que les sous-espaces propres d'un endomorphisme $f \in \mathcal{F}$ sont stables pour tous les $f' \in \mathcal{F}$. Dès lors, les restrictions des f' à ces sous-espaces propres sont diagonalisables, puisqu'elles annulent un polynôme scindé non nul dont toutes les racines sont simples. Par récurrence sur la dimension, on en déduit qu'il existe une base qui diagonalise simultanément tous les endomorphismes de la famille. Dans une telle base, si g est un endormorphisme diagonal de valeurs propres distinctes, et si $f \in \mathcal{F}$, il suffit de choisir un polynôme P qui envoie exactement l'ensemble des valeurs propres de g sur l'ensemble des valeurs propres de f pour avoir $f = P(g)$.

Exercice 14

Enoncé

Soit $f : \mathbb{R}_+ \to \mathbb{C}$ de classe $\mathcal{C}^1$, telle que $\int_0^\infty |f'| < \infty$. Montrer que

$$\sum_{n \geq 0} f(n) \text{ et } \int_0^\infty f$$

sont de même nature.

Quelle est la nature de $\sum \frac{\cos \ln n}{\ln n}$?

Eléments de correction

La première affirmation découle de l'identité

$$\sum_{n=2}^{N} f(n) = \int_1^N \left(f(t) + \{t\} f'(t)\right) \, dt,$$

où $\{t\} = t - [t]$ est la partie fractionnaire de t.

Elle ne s'applique pas directement à la fonction

$$f(t) = \frac{\cos \ln t}{\ln t}$$

parce que

$$f'(t) = -\frac{\sin \ln t}{t \, \ln t} - \frac{\cos \ln t}{t \, \ln^2 t},$$

où le premier terme n'est pas absolument intégrable. Mais le même type de calcul à l'ordre deux (puisque cette fonction f est de classe $\mathcal{C}^2$) conduit à la formule

$$\sum_{n=2}^{N} f(n) = \frac{f(N) - f(1)}{2} + \int_1^N \left(f(t) + \left(\{t\} - \{t\}^2\right) f''(t)\right) \, dt,$$

de laquelle on peut déduire que la série demandée a même nature que $\int^\infty f$. En intégrant sur les intervalles de la forme $[a_k, b_k]$ avec

$$a_k = e^{-\pi/4+2k\pi}, \quad b_k = e^{\pi/4+2k\pi}$$

et en faisant le changement de variable $t = e^s$, on voit que l'intégrale, et donc aussi la série, divergent.

Exercice 15

Enoncé

Soient $v : \mathbb{R}^2 \to \mathbb{R}^2$ de classe C^∞ et, pour tout $t \in \mathbb{R}$, $\varphi_t : \mathbb{R}^2 \to \mathbb{R}^2$ de classe C^∞, tels que

$$\varphi_0 = id \text{ et } \frac{d\varphi_t(x)}{dt} = v(\varphi_t(x))$$

pour tous x, t.

1) Justifier, par un calcul au premier ordre au voisinage de $x \in \mathbb{R}^2$, que la dérivée par rapport au temps, de l'accroissement de l'aire par φ_t en x et en $t = 0$ est

$$\frac{\partial v_1}{\partial x_1}(x) + \frac{\partial v_2}{\partial x_2}(x).$$

2) Que vaut ce taux pour $v(x) = (x_2, -\sin x_1)$?

Déterminer une méthode numérique approchée pour calculer $\varphi_t(x)$ quand t est petit, qui préserve l'aire au sens de la question précédente.

Eléments de correction

1) On a

$$\varphi_t(x + \xi) = \varphi_t(x) + d\varphi_t(x) \cdot \xi + o(\|\xi\|).$$

Au premier ordre, un petit carré au voisinage de x est donc envoyé sur un parallélogramme, et l'aire est multipliée par $\det \varphi_t(x)$. On vérifie que $d(det)(I)$ est la trace, après quoi on voit, en permutant les dérivées temporelle (en t) et spatiale (en x_1, x_2) :

$$\frac{d}{dt}\det d\varphi_t(x)|_{t=0} = \operatorname{tr} dv(x).$$

2) Avec l'exemple proposé, cette quantité est nulle. Si t est petit, on peut faire l'approximation

$$v(\varphi_t(x)) \simeq v(x),$$

ce qui conduit à approcher $\varphi_t(x)$ par

$$E_t(x) = (x_1 + tx_2, x_2 - t\sin x_1).$$

Mais

$$\det dE_t(x) = 1 + t^2\cos x_1 \neq 1,$$

ce qui signifie (par un raisonnement analogue à celui de la première question) que, si $t \neq 0$, E_t ne préserve pas l'aire. En revanche, on voit que la variante

$$S_t(x) = (x_1 + t(x_2 + t\sin x_1), x_2 - t\sin x_1)$$

a un déterminant jacobien égal à 1, ce qui permet d'espérer qu'il s'agit d'une meilleure approximation de $\varphi_t(x)$.

Exercice 16

Enoncé

Dans ce qui suit on appelle difféomorphisme croissant de $\mathbb{R}$ une application bijective $\mathbb{R} \to \mathbb{R}$, strictement croissante qui, avec son inverse (pour la composition), est $\mathcal{C}^\infty$.

1) Soit $v : \mathbb{R} \to \mathbb{R}$ une fonction de classe $\mathcal{C}^\infty$ et $h : \mathbb{R} \to \mathbb{R}$ un difféomorphisme croissant. On note h_*v la fonction $\tilde{v}$ vérifiant

$$\tilde{v}(h(x)) = h'(x)v(x).$$

Démontrer que si h, g sont deux difféomorphismes croissants de $\mathbb{R}$ on a

$$(h \circ g)_*v = h_*(g_*v).$$

Que vaut $(h^{-1})_* v$?

2) Soit $v : \mathbb{R} \to \mathbb{R}_+^*$ une fonction de classe $\mathcal{C}^\infty$ telle que

$$\forall\, x \in \mathbb{R},\ 0 < v(x) \leq A|x| + B \text{ (ici } A, B > 0).$$

a) Démontrer qu'il existe un difféomorphisme croissant de $\mathbb{R}$ tel que $h_* v = 1$.

b) En déduire que l'équation différentielle

$$x'(t) = v(x(t)) \text{ avec } x(0) = x_0$$

admet une unique solution définie sur $\mathbb{R}$ tout entier.

3) Soit $f : \mathbb{R} \to \mathbb{R}$ un difféomorphisme croissant n'admettant pas de point fixe. Démontrer qu'il existe h un difféomorphisme croissant de $\mathbb{R}$ tel que

$$h \circ f \circ h^{-1} = T \text{ où } T : x \mapsto x + 1.$$

[On pourra se ramener au cas où $f(0) > 0$ et chercher un $v : \mathbb{R} \to \mathbb{R}_+^*$, f-équivariant c'est-à-dire tel que $f_* v = v$.]

Eléments de correction

1) C'est immédiat et résulte de la formule de dérivation des fonctions composées : Si $v_1 = g_* v$, $v_2 = h_* v_1$ on a $v_2 \circ h = h' v_1$ et donc

$$v_2 \circ (h \circ g) = (h' \circ g)(v_1 \circ g) = (h' \circ g) g' v = (h \circ g)' v.$$

Pour l'inverse : si $\tilde{v} \circ h^{-1} = (h^{-1})' v$ on a $\tilde{v} \circ h^{-1} = (1/h' \circ h^{-1}) v$ d'où

$$\tilde{v} = (1/h') \times (v \circ h).$$

2.a) On doit résoudre $h'(x)v(x) = 1$ et donc $h'(x) = 1/v(x)$. Posons

$$h(x) = \int_0^x \frac{1}{v(t)} dt.$$

C'est une application C^∞ strictement croissante et il faut vérifier qu'elle établit une bijection de $\mathbb{R} \to \mathbb{R}$ ou de façon équivalente que $\lim_{x \to \pm\infty} = \pm\infty$. Or

$$1/v(x) \geq (A|x| + B)^{-1}$$

et l'intégrale de cette dernière fonction diverge en $+\infty$ (même chose en $-\infty$).

2.b) Si $x'(t) = v(x(t))$, en posant $y(t) = h(x(t))$ on a

$$y'(t) = h'(x(t))x'(t) = h'(x(t))v(x(t)) = (h' \circ h^{-1})(y(t))(v \circ h^{-1})(y(t))$$

et donc

$$y'(t) = (h_* v)(y(t)).$$

Avec le difféomorphisme de la question précédente, on voit que $y'(t) = 1$, $y(0) = h(x_0)$ qui s'intègre facilement !

3) On peut toujours supposer $f(0) > 0$ car sinon on remplace f par $s \circ f \circ s^{-1}$ où $s : x \mapsto -x$ (l'application ainsi construite reste strictement croissante).

Construisons un "champ de vecteur" v tq $f_* v = v$. Pour cela on considère un domaine fondamental de f c'est-à-dire un intervalle I tel que les $f^n(I)$ forment une partition de $\mathbb{R}$. Il suffit de choisir $I = [0, f(0)[$, le seul point à vérifier étant que l'on couvre $\mathbb{R}$ par les $f^n(I)$; mais c'est une conséquence du fait que f est sans point fixe et donc pour tout x (en particulier $x = 0$) $\lim_{n \to \pm\infty} f^n(x) = \pm\infty$ (suite strictement monotone). Pour construire v on procède de la façon suivante. on choisit v égale à 1 sur $] - \delta, \delta[$ ($\delta > 0$ petit) ; on doit avoir $v(f(x)) = f'(x)v(x)$ ce qui force les valeurs de v sur $f(] - \delta, \delta)[)$ qui est un voisinage de $f(0)$ de la forme $]f(0) - a_\delta, f(0) + b_\delta[$. Si δ est suffisamment petit on a

$$0 < \delta < 2\delta < f(0) - a_\delta < f(0) \text{ et } [f(0), f(0) + b_\delta[\subset f(I).$$

On peut alors construire (en utilisant des fonctions e^{-1/x^2}) une fonction v_1 C^∞ sur $J :=]-\delta, f(0)+b_\delta[$, égale à 1 sur $]-\delta,\delta[$ et qui vaut $f'(x)\times 1$ sur $f(]-\delta,\delta[)$. On définit finalement v sur $\mathbb{R}$ en posant pour $n \in \mathbb{Z}$

$$v_{|\ f^n(J)} = (f^n)_* v_1.$$

Comme v_1 et $f_* v_1$ coïncident sur $J \cap f(J)$ on en déduit que v est bien définie, C^∞ et vérifie $f_* v = v$.

Pour conclure on introduit h tel que $h_* v = 1$ (défini en 2.a) et on a

$$h_*(f_* v) = 1 = h_* v$$

si bien que

$$(h^{-1} \circ f \circ h)_* 1 = 1.$$

Mais cette dernière relation impose que

$$\frac{d}{dx}(h^{-1} \circ f \circ h) = 0$$

c'est-à-dire que $h^{-1} \circ f \circ h$ est une translation $x \mapsto x + \alpha$. En conjuguant par l'application $x \mapsto \alpha x$ on obtient le résultat voulu.

Exercice 17

Enoncé

1) Soient (x_n) et (y_n) deux suites réelles périodiques de périodes a et b. Soit d le PGCD de a et b. Montrer que si $x_n = y_n$ pour $a + b - d$ entiers consécutifs, alors $x = y$.

Indication: on pourra introduire les séries $\sum_n x_n T^n$ et $\sum_n y_n T^n$.

2) Soient f et g deux fonctions continues périodiques $\mathbb{R} \to \mathbb{R}$, de périodes $\alpha, \beta > 0$ telles que α/β soit un rationnel a/b, avec a, b entiers > 0 premiers entre eux. Montrer que si $f(t) = g(t)$ sur un intervalle de longueur $\alpha + \beta - \frac{\beta}{b}$, alors $f = g$.

Eléments de correction

1) Soient F et G les séries précédentes, qui sont convergentes par périodicité. On peut supposer que $x_n = y_n$ pour $n = 0, 1, ..., a+b-d$, puisque si $x_n = y_n$ pour $n \geq n_0$, on a égalité pour tout n par périodicité. La suite x étant a-périodique, on a

$$F(T) = \frac{P(T)}{1-T^a},$$

pour un polynôme P de degré au plus $a-1$. De même

$$G(T) = \frac{Q(T)}{1-T^b},$$

avec $\deg(Q) < b$. Le polynôme $1-T^d$ divise à la fois $1-T^a$ et $1-T^b$, on a

$$F - G = \frac{R}{S},$$

où R est un polynôme de degré $< a+b-d$: si

$$1-T^a = A(1-T^d) \text{ et } 1-T^b = B(1-T^d),$$

poser $R = PB - QA$ et $S = (1-T^d)AB$.

Puisque les $a+b-d$ premiers coefficients de la série $F-G$ sont nuls, il en est de même de $R = S(F-G)$, qui est donc le polynôme nul.

2) On peut supposer $\beta = 1$. Soit $t \in [0, b^{-1}]$. Considérons

$$x_n = f\left(t + \frac{n}{b}\right) \text{ et } y_n = g\left(t + \frac{n}{b}\right).$$

Elles sont a et b-périodiques car f et g sont a/b et 1-périodiques. D'après (i), si $x_n = y_n$ pour $n = 0, \cdots, a+b-2$, alors $x = y$. Or

$$\frac{a+b-2}{b} + t \in \left[0, \alpha + \beta - \frac{\beta}{b} = \alpha + 1 - \frac{1}{b}\right[$$

donc $f(t+n/b) = g(t+n/b)$ pour tout n. Comme c'est vrai pour chaque $t \in [0, 1/b[$ et qu'on a égalité sur $[0, \frac{a}{b} + 1 - \frac{1}{b} > \frac{1}{b}]$, on a $f = g$.

Exercice 18

Enoncé

1) Soient a, b, x, y des entiers relatifs non nuls, et $k \in \mathbb{Z}$. Montrer que

$$a.\text{arctg}\left(\frac{1}{x}\right) + b.\text{arctg}\left(\frac{1}{y}\right) = k\frac{\pi}{4} \mod \pi$$

si et seulement si le produit

$$(1-i)^k (x+i)^a (y+i)^b \qquad \text{est réel.}$$

2) Trouver des entiers $a, x > 0$ tels que

$$a.\text{arctg}\left(\frac{1}{x}\right) - \text{arctg}\left(\frac{1}{239}\right) = \frac{\pi}{4}.$$

On pourra admettre que dans l'anneau

$$\mathbb{Z}[i] = \{a + ib; (a, b) \in \mathbb{Z}^2\}$$

tout élément non nul s'écrit comme un produit d'éléments irréductibles, de façon unique si on néglige l'ordre des facteurs et la multiplication par des éléments inversibles.

On précise qu'un élément est dit irréductible si ses seuls diviseurs sont les inversibles et l'élément fois un inversible.

Par exemple, $-239 + i = (1+i)(3+2i)^4$ est une décomposition en facteurs irréductibles.

Eléments de correction

1) <u>Première méthode</u> On a $\exp(2ix) = \frac{1+i\tan(x)}{1-i\tan(x)}$ donc $\text{arctg}(1/x) = \frac{1}{2i}\log(\frac{x+i}{x-i})$, où pour chaque $z \in \mathbb{C}^*$, on note $w = \log(z)$ un nombre complexe, bien défini modulo $2i\pi$, tel que $e^w = z$. La formule se réécrit donc:

$$\frac{1}{2i}\log\left(\left(\frac{x+i}{x-i}\right)^a \left(\frac{y+i}{y-i}\right)^b \left(\frac{1+i}{1-i}\right)^{-k}\right) \in \pi\mathbb{Z}.$$

Si l'on pose

$$z = (1-i)^k (x+i)^a (y+i)^b$$

et $\zeta = z/\bar{z}$ de module 1, on a donc $\log(\zeta) \in 2i\pi\mathbb{Z}$, c'est-à-dire $\zeta = 1$ d'où $z = \bar{z}$.

<u>Seconde méthode</u> Partir de l'égalité triviale

$$a + ib = \sqrt{a^2+b^2}\exp(i\mathrm{arctg}(b/a))$$

et en déduire que

$$\prod_j (a_j + ib_j) = (\text{réel } > 0)\exp\big(i\sum_j \mathrm{arctg}(b_j/a_j)\big).$$

2) On veut déduire de l'égalité

$$(x+i)^a(1-i)(-239+i) = (x-i)^a(1+i)(-239-i)$$

les valeurs de x et a. (On va trouver: $x = 5$, $a = 4$, et le produit vaut $-228488 = -2^3.13^4$.)

Pour commencer, on peut vérifier que $1+i$ et $3+2i$ sont bien irréductibles. Ceci résulte du fait que si $N(z) = z\bar{z}$, on a :

(1) $N(zz') = N(z)N(z')$

(2) $N(z) = 1$ si et seulement si z est un inversible de $\mathbb{Z}[i]$.

La conclusion résulte alors du fait que $N(1+i)$ et $N(3+2i)$ sont premiers, respectivement égaux 2 et 13.

On en tire que les inversibles sont exactement les 1, i, et que $3+2i$ et $3-2i$ sont premiers entre eux. Par contre, $1+i$ et $1-i$ sont associés au sens où l'on passe de l'un (irréductible) à l'autre (irréductible) en multipliant par un élément inversible, soit $-i$.

Compte tenu de ce qui précède, et de l'équation

$$(x+i)^a(1-i)(1+i)(3+2i)^4 = (x-i)^a(1+i)(1-i)(3-2i)^4$$

il est naturel de considérer $a = 4$ et $x + i$ multiple de $(3 - 2i)$. Si $x + i = z(3 - 2i)$, l'équation devient [pour $a = 4$]

$$z^4 = \bar{z}^4,$$

soit $(\frac{z}{\bar{z}})^4 = 1$ c'est-à-dire $\frac{z}{\bar{z}}$ racine quatrième de l'unité; le choix de i et $z = (1 + i)$ convient. Comme $(1 + i)(3 - 2i) = 5 + i$, on a donc trouvé la solution et la formule de Machin:

$$\frac{\pi}{4} = 4.\text{arctg}\left(\frac{1}{5}\right) - \text{arctg}\left(\frac{1}{239}\right).$$

Exercice 19

Enoncé

Soit $A \in M_n(\mathbb{C})$.

1) Montrer que les conditions suivantes sont équivalentes:

(i) Toutes les valeurs propres (complexes) de A sont égales à 1.

(ii) $A = \text{Id} + N$ où $N^n = 0$.

2) On suppose A à coefficients rationnels. Montrer qu'il existe une matrice $B \in M_n(\mathbb{Q})$ telle que $A = B^2$.

(On peut commencer par le cas réel.)

Eléments de correction

1) Il faut montrer qu'une matrice de valeurs propres toutes nulles est nilpotente. On peut la trigonaliser avec des zéros sur la diagonale. Il est clair que sa puissance n-ième est nulle. Réciproque: si $\lambda \neq 1$, on a

$$A - \lambda\,\text{Id} = (\lambda - 1)\,\text{Id} + N$$

qui est inversible.

2) On peut choisir
$$B = (\mathrm{Id} + N)^{1/2}.$$
Plus précisément, on a envie de définir
$$\mathrm{Id} + \sum_{r \geq 0} \binom{\alpha}{r} N^r.$$
Pour $\alpha = \frac{1}{2}$, c'est
$$\mathrm{Id} + \frac{1}{2} N - \frac{1}{8} N^2 + \cdots .$$
La formule
$$((\mathrm{Id} + N)^{\frac{1}{2}})^2 = \mathrm{Id} + N$$
est valable car les coefficients obtenus en développant $1, 1, 0, 0, 0, \cdots$ sont les mêmes que ceux obtenus en élevant au carré la série entière sur $\mathbb{R}$.

Exercice 20

Enoncé

Soit u un endomorphisme d'un $\mathbb{C}$-espace vectoriel V de dimension finie. On suppose qu'il existe une constante $C \geq 0$ telle que pour tout $n \geq 0$, on ait $|Tr(u^n)| \leq C$. Montrer que l'on a $|Tr(u^n)| \leq \dim(V)$ pour tout $n \geq 0$.

Indication : on pourra considérer la série entière $\sum_{n>0} Tr(u^n) \frac{t^n}{n}$ et montrer qu'elle coincide avec $\log \det(\mathrm{Id} - tu)^{-1}$ sur un voisinage de zéro.

Eléments de correction

Il s'agit de montrer que chaque valeur propre de u est de module ≤ 1. Suivant l'indication, on considère:
$$t \mapsto \det(\mathrm{Id} - tu)^{-1} = \prod_{i=1}^{\dim(V)} (1 - t\lambda_i)^{-1},$$

bien définie dans le disque $|t| < 1/\rho$, où $\rho = \max |\lambda_i|$ (avec la convention $1/0 = +\infty$). Son logarithme [complexe ; considérer seulement la série entière sinon] est

$$\sum_{i=1}^{\dim(V)} \log(1 - t\lambda_i)^{-1} = \sum_{i=1}^{\dim(V)} \sum_{n>0} \lambda_i^n \frac{t^n}{n} = \sum_{n>0} \left(\sum_{i=1}^{\dim(V)} \lambda_i^n \right) \frac{t^n}{n},$$

la série entière de l'indication. L'hypothèse entraîne que cette série a un rayon de convergence ≥ 1. Pourtant, si $\rho = |\lambda_i| > 1$, on aurait une divergence de la fonction pour t approchant $1/\lambda_i$. On a donc $\rho \leq 1$.

Remarque : si u trigonalisable sur $\mathbb{R}$, on peut prendre n pair et majorer par positivité $|\lambda_i| \leq 1$.

Exercice 21

Enoncé

1) Soit $(x)_{n\geq 1}$ une suite réelle. Montrer que si elle converge vers $l \in \mathbb{R}$, elle converge aussi *logarithmiquement* vers l :

$$\frac{1}{\log(n)} \sum_{1\leq k\leq n} \frac{x_k}{k} \to l.$$

2) Soit (c_n) la suite définie par $c_0 = 1$ si l'écriture de n (en base 10) commence par un 1, et 0 sinon.

La suite $\frac{1}{n} \sum_{1\leq k\leq n} c_k$ est-elle convergente ?

3) Montrer que (c_n) converge logarithmiquement vers $\log_{10}(2)$.

Eléments de correction

1) C'est essentiellement identique au cas classique de la limite de Cesaro, bien connu (mais pas explicitement au programme). Par linéarité, on peut supposer que $l = 0$ car la suite constante égale à 1 tend logarithmiquement vers 1. La conclusion dans ce cas est alors immédiate, par l'argument classique.

2) Si $n = 2.10^k - 1 = 1999\cdots 9$, la moyenne est au moins $1/2$: les $(n+1)/2$ nombres de 10^k à n commencent par 1. Si $n = 10^k - 1 = 999\cdots 9$, il y a au moins 8.10^{k-1} nombres inférieurs [à k chiffres] qui ne commencent pas par 1. La moyenne est donc majorée par environ $2/10 = 1/5$. Il n'y a donc pas convergence.

3) Si $K = \lfloor \log_{10}(n) \rfloor$ (le nombre de chiffres de n, moins 1), la somme à calculer, avant de diviser par le logarithme de n, est :

$$\sum_{0 \le k \le K} \sum_{0 \le j < 10^k} \frac{1}{10^k + j} + \sum_{j=10^K}^{\min\{n, 2.10^K - 1\}} \frac{1}{j}.$$

Le second terme est un $\mathcal{O}(1)$: comparer avec $\int\limits_{10^K}^{2.10^K} \frac{dt}{t} = \log(2)$. Pour chaque k (= nombre de chiffres après le 1), la somme $\sum\limits_{0 \le j < 10^k} \frac{1}{10^k + j}$ se compare aussi à une intégrale : c'est $\int_0^1 \frac{dx}{1+x}$ à une erreur majorée par le sup de l'oscillation de la fonction (décroissante) $x \to 1/(1+x)$ sur un intervalle de longueur 10^{-k}, qui vaut $1/(10^k + 1) \le 10^{-k}$. Finalement, la somme est

$$(K+1)\log(2) + \mathcal{O}(\sum_k 10^{-k}) + \mathcal{O}(1) = \lfloor \log_{10}(n) \rfloor \log(2) + \mathcal{O}(1).$$

Il reste alors à diviser par $\log(n)$.

Exercice 22

Enoncé

Soit p un nombre premier. On considère l'anneau $A := \mathbb{Z}/p\mathbb{Z}[T]$ des polynômes à coefficients dans l'anneau des entiers modulo p: c'est l'ensemble des sommes finies $\sum\limits_i a_i T^i$ munies de la somme et du produit usuels: $(\sum_i a_i T^i)(\sum\_j b_j T^j) = \sum_k (\sum_{i+j=k} a_i b_j) T^k$, où les produits et sommes des coefficients sont calculés dans le corps $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire modulo p.

Pour tout polynôme unitaire $f \in A$, notons $|f|$ (valeur absolue de f) l'entier $p^{\deg(f)}$; en particulier, $|1| = 1$. On dit que f est "sans facteur carré" si le seul polynôme unitaire g tel que $g^2 | f$ est $g = 1$.

1) Montrer que si $s \in \mathbb{C}$ est de partie réelle > 1, la famille des $|f|^{-s}$ (pour f unitaire) est sommable et calculer sa somme $\zeta(s)$.

2) Soit $\zeta_2(s) := \sum_f |f|^{-s}$ où f parcourt l'ensemble des polynômes unitaires sans facteur carrés. Montrer que:

$$\zeta_2(s) = \frac{\zeta(s)}{\zeta(2s)}.$$

Indication: en ignorant les questions de convergence, on pourra réécrire ces sommes comme des produits en admettant le fait que tout polynôme unitaire s'écrit de manière unique [à l'ordre près] comme un produit de polynômes unitaires irréductibles.

3) En déduire que pour tout entier $d \geq 2$, la proportion de polynômes $f \in A$ unitaires de degré d, sans facteur carré, est $1 - p^{-1} = \dfrac{1}{\zeta(2)}$.

Eléments de correction

1) On a

$$\zeta(s) = \sum_{d \geq 0} \frac{p^d}{p^{ds}} = \frac{1}{1 - p.p^{-s}}$$

car il y a exactement p^d polynômes unitaires de degré d.

2) On montre que

$$\zeta(s) = \prod_{P irr. unit.} \frac{1}{1 - |P|^{-s}}.$$

Cela résulte de l'existence et l'unicité de la décomposition en produit d'irréductibles. En effet, on a

$$\prod_P \big(\sum_{n \geq 1} |P|^{-ns} \big) = \sum_f |f|^{-s}.$$

Si $f = P_1^{n_1} \cdots P_r^{n_r}$, on a $|f|^{-s} = |P_1|^{-n_1 s} \cdots |P_r|^{-n_r s}$.

[Variante : Ecrire $\zeta(s) = \sum_{P|f} + \sum_{P\nmid f}$, d'où $\zeta(s) = \zeta_{P\nmid f}(1-|P|^{-s})^{-1}$ et par récurrence $\zeta(s) = \zeta_{P_1,\cdots,P_n\nmid f} \times \prod_i (1-|P_i|^{-s})^{-1}$, d'où la formule.]

De même, on a trivialement $\zeta_2(s) = \sum_P (1+|P|^{-s})$ (via variante de la variante si l'on veut), où P parcourt l'ensemble des polynômes unitaires irréductibles.

De l'identité $1+z = \frac{1-z^2}{1-z}$ appliquée aux $z = |P|^{-s}$, on tire l'égalité désirée.

3) Compte-tenu de l'expression de $\zeta(s)$, on obtient, en posant $x = p^{-s}$, l'égalité:

$$\frac{1-px^2}{1-px} = \sum_{d\geq 0} a_d x^d,$$

où a_d est le nombre de polynômes unitaires sans facteur carré de degré d. En développant le terme de gauche (série géométrique), on trouve que pour chaque $d > 1$, on a $a_d = p^d - p^{d-1}$, d'où le résultat en divisant par p^d.

Exercice 23

Enoncé

1) Montrer qu'il n'existe pas de fonction rationnelle $g(x) \in \mathbb{R}(x)$ telle que $g(x)e^{-x^2}$ soit une primitive de e^{-x^2}.

2) Soient $g \in \mathbb{R}(x)\backslash\mathbb{R}$ et $H \in \mathbb{R}[X,Y]$ tels que

$$H(x, \exp(g(x))) = 0$$

sur un intervalle ouvert non vide de $\mathbb{R}$. Montrer que $H = 0$.

Eléments de correction

1) En dérivant, on obtient $g' - 2xg = 1$. Si $g = u/v$ avec $u \wedge v = 1$ et v unitaire, on a

$$u'v - uv' - 2xuv = v^2$$

d'où $v \mid uv'$, d'où $v|v'$ (car $u \wedge v = 1$) et donc $v = 1$. Finalement, $u' - 2xu = 1$ n'a pas de solution polynomiale pour des raisons de degré.

2) Par hypothèse, il existe un entier $n > 0$ et des fractions rationnelles $a_i \in \mathbb{R}(x)$ telles que

$$e^{ng} + \sum_{0 \leq k < n} a_k e^{kg} = 0$$

sur l'intervalle considéré, privé des pôles des fractions rationnelles. Considérons une telle relation pour n *minimal*. En dérivant la relation, et en divisant par ng' (qui est non nulle car g est non constante), on obtient

$$e^{ng} + \sum_k \frac{a_k' + a_k.kg'}{ng'} e^{kg} = 0.$$

Par minimalité de n, on a donc $\dfrac{a_k' + a_k.kg'}{ng'} = a_k$ pour tout k. Soit $a = a(x) \in \mathbb{R}(x)$ un des a_k non nul. D'après ce qui précède, on a l'égalité, dans $\mathbb{R}(x)$,

$$g' = \lambda \frac{a'}{a},$$

avec $\lambda \in \mathbb{R}^*$. (En l'occurrence, c'est $(n-k)^{-1}$ mais peu importe.) Or, le terme de droite est de la forme

$$\sum_\alpha \frac{c_\alpha}{x - z_\alpha},$$

où les $z_\alpha \in \mathbb{C}$ sont les racines et pôles de a et les $c_\alpha \neq 0$. (Calcul usuel de dérivée logarithmique, en factorisant la fraction rationnelle sur $\mathbb{C}$.)

Une telle égalité est impossible : si z est l'un des z_α, on a $g(x) = h(x)/(x-z)^m$ pour un $m \in \mathbb{N}_{>0}$ (avec $h(z) \notin \{0, \infty\}$) et

$$g' = g.\frac{g'}{g} = \frac{h}{(x-z)^m}\left(\frac{-m}{x-z} + \cdots\right) = \frac{-mh}{(x-z)^{m+1}} + \cdots \neq \frac{c}{x-z} + \cdots = \lambda \frac{a'}{a}.$$

En bref : la dérivée d'une fraction rationnelle n'a jamais un comportement en $1/x$ au voisinage de 0.

Exercice 24

Enoncé

Soit

$$P(x) = \prod_{k\geq 1} \frac{1}{1-x^k},$$

c'est-à -dire la limite du produit

$$P_n(x) = \prod_{k=1}^{n} (1-x^k)^{-1}$$

lorsque $n \to +\infty$.

1)Montrer que le produit converge bien pour $|x| < 1$ et que $P(x) = \sum_n p(n)x^n$, où $p(n)$ est le nombre de partitions de n en somme d'entiers strictement positifs.

2) Montrer que pour $x \to 1^-$, on a:

$$P(x) = \exp\left(\frac{\zeta(2)}{(1-x)}(1+o(1))\right),$$

où

$$\zeta(2) = \sum_{n>0} n^{-2}.$$

3) En utilisant la majoration triviale

$$p(n) \leq x^{-n} P(x),$$

pour un bon choix de $x \in]0, 1[$, montrer que

$$p(n) \leq \exp\left(\sqrt{\frac{2n}{3}}(1+o(1))\right).$$

On admettra que $\zeta(2) = \frac{\pi^2}{6}$.

Eléments de correction

1) Pour $|x|<1$, on peut regarder

$$\log P_n(x) = \sum_{k=1}^{n} \log(1-x^k)^{-1}.$$

Comme $-\log(1-y) = \sum\limits_{r>0} y^r/r$ est majoré en valeur absolue par $|y|\big(1+|y|+|y^2|+\cdots\big)$, on a $|\log(1-y)| \leq 2|y|$ pour $|y| \leq \frac{1}{2}$. Pour $|x|<1$, on a $|x^k| \leq \frac{1}{2}$ à partir d'un certain rang donc $\sum\limits_{k>0} |\log(1-x^k)|$ converge.

Définissons des entiers $p_r(n)$ par $P_r(x) = \sum\limits_{n} p_r(n)x^n$ (polynôme). Par définition, on a $P(x) = \lim_r P_r(x)$ et $p_r(n) = p_{r+1}(n)$ si $r \geq n$. ($p_r(n)$ correspond aux partitions dont les sommants sont $\leq r$.)

On a donc $P(x) = \sum\limits_{n} p(n)x^n$, où $p(n)$ est la valeur limite de $p_r(n)$, qui est clairement le nombre de façons d'écrire n comme une somme d'entiers non nuls (sans prendre en compte l'ordre des facteurs).

2) On a

$$P(x) = \exp\big(\sum_{k>0} \log[(1-x^k)^{-1}]\big) = \exp\big(\frac{x}{1-x} + \frac{1}{2}\frac{x^2}{1-x^2} + \frac{1}{3}\frac{x^3}{1-x^3} + \cdots\big),$$

que l'on peut réécrire, pour mettre le $1-x$ attendu en facteur,

$$P(x) = \exp\big((\frac{1}{1-x})(\frac{x}{1} + \frac{x^2}{2(1+x)} + \frac{x^3}{3(1+x+x^2)} + \cdots)\big)$$

Pour $0<x<1$, on a $kx^{k-1} < 1+x+x^2+\cdots+x^{k-1} < k$, d'où

$$\frac{1}{1-x}\sum_{k>0}\frac{x}{k^2} > \log(P(x)) > \frac{1}{1-x}\sum_{k>0}\frac{x^k}{k^2},$$

et immédiatement:

$$P(x) = \exp\left(\frac{\zeta(2)}{1-x}(1+o(1))\right).$$

(La minoration est suffisante pour avoir la convergence normale.)

3) Posons $c = \zeta(2)$. Si l'on considère $x_n = 1 - \sqrt{\frac{c}{n}}$, on a

$$p_n \leq \left(1 - \sqrt{\frac{c}{n}}\right)^{-n} \exp\left(\sqrt{cn}(1+o(1))\right) =$$

$$= \exp\left((\sqrt{cn} + O(1)) + \sqrt{cn}(1+o(1))\right) = \exp\left(2\sqrt{cn}(1+o(1))\right).$$

La première égalité est un développement limité du log (c'est-à-dire $x + \frac{x^2}{2}$) et la seconde est une simple réécriture. Le choix de x_n est naturel: si on dérive $\exp\left(c/(1-x)\right)/x^n$, on a un zéro lorsque $n(1-x)^2 = xc$, soit $(1-x)^2 = xc/n$, dont $1 - \sqrt{\frac{c}{n}}$ est presque solution (x très proche de 1).

Exercice 25

Enoncé

Soit $n \geq 2$.

1) Montrer que le nombre moyen de points fixes d'une permutation de $\{1, \cdots, n\}$ est 1.

2) Calculer l'écart-type.

Eléments de correction

1) si $F(\pi)$ est le nombre de points fixes de la permutation π, on a

$$F(\pi) = F_1(\pi) + F_2(\pi) + \cdots + F_n(\pi),$$

où $F_i(\pi) = 1$ si et seulement si i est fixé par π. On a donc $E(F) = \sum_i E(F_i)$. Or

$$E(F_i) = (n-1)!/n! = 1/n.$$

2) On a

$$E(F^2) = \sum_{i,j} E(F_i F_j) = \sum_k E(F_k^2) + 2\sum_{i<j} E(F_i F_j).$$

Or, $F_k^2 = F_k$ donc $E(F_k^2) = 1/n$ et

$$E(F_iF_j) = (n-2)!/n! = 1/n(n-1).$$

Finalement,

$$E(F^2) = \frac{n}{n} + \binom{n}{2}\frac{2}{n(n-1)} = 2$$

pour $n \geq 2$. Ainsi, la variance est $E(F^2) - E(F)^2 = 1$ et l'écart-type, sa racine carrée, est également égal à 1.

Exercice 26

Enoncé

1) Soit X une variable aléatoire de moyenne nulle, à valeurs réelles dans un intervalle $[a, b]$. Montrer que pour tout $t \in \mathbb{R}$, on a

$$E(\exp(tX)) \leq \exp\left(t^2\frac{(b-a)^2}{8}\right).$$

Indication : on pourra utiliser la convexité de la fonction $x \mapsto \exp(tx)$.

2) Soient $X_1, \cdots, X_n$ des variables aléatoires indépendantes, telles que X_i soit à valeurs dans l'intervalle $[a_i, b_i]$. Montrer que pour tout $s > 0$, on a:

$$P\left(\sum_i (X_i - E(X_i)) \geq s\right) \leq \exp\left(-\frac{2s^2}{\sum_i |b_i - a_i|^2}\right).$$

3) En déduire que la probabilité de tirer au moins $\frac{3}{4}$ de "face" en N lancers de pile ou face est majorée par $\exp(-N/8)$. Que donnerait l'inégalité de Tchebychev ?

Eléments de correction

1) La fonction $x \mapsto \exp(tx)$ étant convexe, on a la majoration

$$e^{tx} \leq \frac{b-x}{b-a}e^{ta} + \frac{x-a}{b-a}e^{tb}$$

pour tout $x \in [a,b]$. En prenant l'espérance/moyenne, et en utilisant $E(X) = 0$, on obtient une majoration par

$$E(e^{tX}) \leq (1-\mu)e^{ta} + \mu e^{tb}$$

[avec $\mu = -\frac{a}{b-a} > 0$]

$$= e^{ta}(1 - \mu + \mu e^{t(b-a)}) = e^{-t\mu(b-a)}(1 - \mu + \mu e^{t(b-a)}),$$

soit encore, en mettant tout dans l'exponentielle, par $\exp(f(\lambda))$, où $\lambda = t(b-a)$ et

$$f(y) = -\mu y + \log(1 - \mu + \mu e^y).$$

On a $f(0) = 0$ (c'est trivial) mais aussi $f'(0) = 0$ et $f"(y) \leq 1/4$ car c'est le produit $z(1-z)$ pour $z = \frac{\mu e^y}{1-\mu+\mu e^y}$. Par la formule de Taylor, on a

$$f(\lambda) = f(0) + \lambda f'(0) + \frac{\lambda^2}{2} f''(l)$$

pour un $0 \leq l \leq \lambda$ et, finalement,

$$E(e^{tX}) \leq \exp\left(\frac{\lambda^2}{2} \times \frac{1}{4}\right).$$

On obtient le résultat.

2) Soit $S = \sum_i X_i$. On peut supposer $E(X_i) = 0$: cela ne change pas les $b_i - a_i$. On a, pour chaque $t, s > 0$:

$$P(S \geq s) = P(e^{tS} \geq e^{ts}) \leq e^{-st} E(e^{tS}),$$

par l'inégalité de Markov. Ce dernier terme est, par indépendance, égal au produit

$$e^{-st} \prod_i E(e^{tX_i}) \leq e^{-st} \prod_i \exp\left(\frac{t^2}{8}(b_i - a_i)^2\right)$$

grâce à la question précédente. Il reste à trouver t pour que le polynôme de degré 2 en t

$$-st + \frac{\|b-a\|^2}{8} t^2$$

soit le plus petit possible. On trouve immédiatement $t = \frac{4s}{\|b-a\|^2}$ et la majoration demandée.

3) La moyenne est $\frac{1}{2}N$ et on prend $s = \frac{1}{4}N$. On obtient le résultat demandé, bien meilleur que celui donné par l'inégalité de Tchebychev, linéaire en N^{-1}.

Exercice 27

Enoncé

Deux joueurs A et B effectuent des lancers consécutifs d'une pièce non biaisée. A gagne si FFP sort avant FPP, et B gagne si FPP sort avant FFP.

1) Trouver un équivalent de la probabilité que A gagne *exactement* au n-ième lancer.

Indication : on pourra considérer la série entière des cardinaux des lancers faisant gagner A au n-ième lancer, la série analogue pour B et enfin celle pour laquelle personne ne gagne, puis établir trois relations entre ces séries.

2) Montrer que A a deux fois plus de chance de gagner que B.

Eléments de correction

1) Soit $A(x)$ la série entière $\sum_n a_n x^n$ où a_n est le nombre de motifs de longueur n faisant gagner A. La probabilité que A gagne au n-ième lancer est donc $a_n/2^n$ et celle que A gagne (à un moment quelconque) est $A(\frac{1}{2})$. On peut définir pour B la série $B(x)$ comme pour A et $Z(x)$ la série correspondant aux lancers/mots sans FFP ni FPP pour lesquels personne ne gagne. (On compte le mot vide de longueur 0 de sorte que $Z(x) = 1 + \cdots$.)

On a les relations suivantes.

1. $1 + Z(x).2x = Z(x) + A(x) + B(x)$: si l'on ajoute à un mot de type $Z(x)$ un F ou un P à droite, on obtient un mot type $Z(x)$, $A(x)$ ou $B(x)$ et c'est une bijection, si ce n'est qu'il manque le mot vide $[2z_{n-1} = z_n + a_n + b_n]$.
2. $Z(x).x^3 = A(x)$: un mot de $A(x)$ est obtenu en ajoutant FFP à un mot de $Z(x)$.

3. $Z(x).x^3 = A(x)x + B(x)$: si l'on ajoute FPP à un mot de $Z(x)$, on obtient un mot de type $A(x)P$, si celui de $Z(x)$ se termine par F, ou bien un mot de type $B(x)$, si celui de Z se termine par P.

On trouve

$$1 + 2xZ(x) = Z(x)(1 + x^3 + x^3(1 - x))$$

d'où, en factorisant, que a_n est le coefficient de z^n dans la série $\frac{z^3}{(1-z)^3(1+z)}$.

On notera $[z^n]g(z)$ le coefficient de z^n dans la série $g(z)$.

Comme

$$\frac{1}{(1-z)^3(1+z)} = \frac{\frac{1}{8}}{1+z} + \frac{\frac{7}{8} - \frac{1}{2}z + \frac{1}{8}z^2}{(1-z)^3},$$

et que

$$[z^n]\frac{1}{(1-z)^3} = \frac{1}{2}(n+1)(n+2),$$

on trouve que

$$[z^{n+1}]\frac{z^3}{(1-z)^3(1+z)} = \frac{1}{4}n^2 - \frac{1}{8}(1 - (-1)^n)$$

est l'entier le plus proche de $n^2/4$. La probabilité demandée est donc équivalente à $n^2/2^{n+2}$. (On trouve bien $\frac{1}{8}$ pour $n = 3$ et $n = 4$.)

2) En évaluant en $x = \frac{1}{2}$, les deux dernières relations [b),c)] du système obtenu ci-dessus, on trouve

$$A\left(\frac{1}{2}\right) = \frac{1}{2}A\left(\frac{1}{2}\right) + B\left(\frac{1}{2}\right),$$

d'où

$$A\left(\frac{1}{2}\right) = 2B\left(\frac{1}{2}\right).$$

Pour cette question, on pourrait certainement le faire directement, en observant que B gagne si FPP apparaît mais que lorsque le FP correspondant sort, il y avait une chance sur deux qu'il soit précédé d'un F, ce qui fait gagner A, ...

Exercice 28

Enoncé

Soient $X = [-1,1]^n$, $A = C^0(X, \mathbf{R})$, $f_1, ..., f_{n+1} \in A$ et $\epsilon > 0$. Montrer qu'il existe $g_1, ..., g_{n+1}$ sans zéro commun, telles que

$$\sup_X |f_i - g_i| < \epsilon \text{ pour tout } i.$$

On admettra le théorème de Weierstrass dans A: les éléments de A peuvent être approchés arbitrairement près en norme supérieure par des fonctions polynomiales.

Eléments de correction

Il suffit de montrer la conclusion pour ϵ assez petit, c'est là la difficulté.

D'après le théorème de Weierstrass, il existe des fonctions polynomiales φ_i telles que

$$\sup_X |f_i - \varphi_i| < \epsilon \text{ pour tout } i.$$

Notons $B_r^n(x)$ la boule euclidienne de $\mathbf{R}^n$ de centre x et de rayon r.

On se convainc que X peut être recouvert par $N \leq C/r^n$ boules euclidiennes de rayon r/M, où C est une constante qui ne dépend pas de r petit. En effet, le nombre minimal de boules est majoré par le nombre maximal de points de X distants au moins de r. Les boules de rayon $r/2$ centrées en ces points sont disjointes. En écrivant que la somme des volumes de ces boules est majorée par le volume de X, on obtient l'estimation cherchée.

Or, les fonctions φ_i sont lipschitziennes, et donc l'application

$$\varphi = (\varphi_1, ..., \varphi_{n+1}) : X \to \mathbf{R}^{n+1}$$

aussi: : il existe $M > 0$ tel que

$$\|\varphi(x) - \varphi(y)\| < M\|x - y\| \text{ pour tous } x, y.$$

Donc il existe C' indépendante de r telle que l'image $\varphi(X)$ puisse être recouverte par $\frac{C'}{r^n}$ boules de rayon r.

Par ailleurs la boule euclidienne $B_\epsilon^{n+1}(0)$ dans $\mathbf{R}^{n+1}$ ne peut pas être recouverte par $\frac{C'}{r^n}$ boules de rayon r pour des r arbitrairement petits, comme de nouveau un simple argument de volume le montre.

Donc, quand $r \leq \epsilon$ est assez petit il existe un point $z \in B_\epsilon^{n+1}(0)$ qui ne soit pas dans l'image de $(\varphi_1, ..., \varphi_{n+1})(X)$. Alors la fonction $g(x) = \varphi(x) - z$ n'a pas de zéro, et ses composantes $g_i(x) = \varphi_i(x) - z_i$ n'ont pas de zéros communs. De plus pour tout i,

$$|z_i| \leq \|z\| \leq \epsilon,$$

donc

$$\sup_X |f_i - g_i| \leq 2\epsilon.$$

Exercice 29

Enoncé

1) Existe-t-il deux fonctions rationnelles non constantes $x(t), y(t) \in \mathbb{C}(t)$ telles que

$$x^2(t) + y^2(t) = 1 \ ?$$

2) Comment rendre rigoureux l'argument suivant?

> les trois bissectrices d'un triangle quelconque se coupent en un même point car il en est ainsi pour un nombre fini de triangles.

Indication: on pourra utiliser une variante, à énoncer, du fait qu'un polynôme de degré au plus n ayant $n+1$ racines est nul.

3) (facultatif) Existe-t-il deux fonctions rationnelles non constantes $x(t), y(t) \in \mathbb{C}(t)$ telles que $x^3(t) + y^3(t) = 1$?

Eléments de correction

1) Le point $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ est sur le cercle unité. Interprétation géométrique via la droite de pente t passant par $(-1, 0)$ ou paramétrisation de cosinus et sinus via la tangente de l'arc moitié; cf. question suivante. (Il en résulte qu'il existe une infinité de points du cercle unité à coordonnées rationnelles.)

2) La variante envisagée dans l'indication est le lemme suivant:

Soit $n \geq 1$ un entier et

$$P(x, y) = \sum_{0 \leq i,j \leq n} a_{ij} x^i y^j$$

une fonction polynomiale $\mathbb{C}^2 \to \mathbb{C}$. On suppose qu'il existe des nombres complexes distincts $x_1, \cdots, x_{n+1}$ et des nombres complexes distincts $y_1, \cdots, y_{n+1}$ tels que $P(x_i, y_j) = 0$ pour chaque $1 \leq i, j \leq n+1$. Alors, $P = 0$.

Démonstration du lemme.

Ecrivons

$$P(x, y) = c_n(x) y^n + c_{n-1}(x) y^{n-1} + \cdots + c_0(x),$$

où les $c_i(x)$ sont de degré $\leq n$. Fixons j. Le polynôme $P(x_j, y)$ a $n+1$ racines donc ses coefficients sont nuls: $c_n(x_j) = \cdots = c_0(x_j) = 0$. Ceci est vrai pour chaque x_j. On a donc $c_n(x) = \cdots = c_0(x) = 0$ à nouveau pour des raisons de degré.

Pour faire le lien avec le problème géométrique, il suffit de montrer qu'il existe un polynôme $P(x, y)$ à coefficients réels satisfaisant la condition suivante: si ABC est le triangle dont les sommets sont de coordonnées $A = (0, 0)$, $B = (0, 1)$ et $C = (u, v)$ avec $0 < u < 1$ et $v > 0$, les trois bissectrices s'intersectent en un même point si et seulement si on a $P(a, b) = 0$, où $a = \tan(\frac{1}{2}\widehat{BAC})$ et $b = \tan(\frac{1}{2}\widehat{ABC})$. Cela résulte du lemme et du fait que l'on peut tout exprimer en des fractions rationnelles en a, b: les coordonnées du point d'intersection (x_{AB}, y_{AB}) des bissectrices en A et B en fonction de a et b, les coordonnées (u, v) et enfin les coefficients de l'équation de la bissectrice en C.

L'appartenance de (x_{AB}, y_{AB}) à cette dernière se traduit donc (pour $a \neq b$, sans quoi c'est d'ailleurs trivial car le triangle est isocèle) sous la forme d'une équation:

$$y_{AB}(a,b) - v(a,b) = \lambda(a,b)\big(x_{AB}(a,b) - u(a,b)\big) \quad (1).$$

En mettant cette expression, qui est dans $\mathbb{Q}(a, b)$, au même dénominateur, cela revient bien à une égalité du type annoncé.

En écrivant $y = ax = (1-x)b$ on trouve immédiatement $x_{AB}(a, b) = \frac{b}{a+b}$ et $y_{AB} = \frac{ab}{a+b}$. Les coordonnées (u, v) de C sont obtenues en écrivant $y = a_2 x = (1-x)b_2$, où $a_2 = \tan(\hat{A})$ et $b_2 = \tan(\hat{B})$. Finalement, comme $a_2 = \frac{2a}{1-a^2}$, et de même pour b_2, on trouve

$$u(a,b) = \frac{b(1-a^2)}{(a+b)(1-ab)} \ , \ v(a,b) = \frac{2ab}{(a+b)(1-ab)}.$$

Lorsque $a \neq b$, la pente $\lambda(a, b)$ de la bissectrice en C est

$$\tan\left(\frac{1}{2}\pi + \frac{1}{2}(\hat{A} - \hat{B})\right) = \frac{1+ab}{b-a},$$

via

$$\tan\left(\frac{1}{2}\pi + x\right) = 1/\tan(x) \text{ et } \tan(x+y) = \frac{\tan(x) + \tan(y)}{1 - \tan(x)\tan(y)}.$$

Pour vérifier que 64 triangles suffisent, il faut montrer que le degré de P est au plus 8 en chacune des variables.

Sans effectuer le calcul exact, on voit que l'équation (1) donne un polynôme de degré au plus 7 en chaque variable. (Cela résulte du fait que l'on peut trivialement majorer les degrés des numérateurs et dénominateurs d'une somme de deux fractions rationnelles.) Le résultat demandé en découle, et il suffit de le tester sur 64 triangles.

Notons que si on effectue précisément le calcul jusqu'au bout, on obtient bien une démonstration du théorème, sans avoir besoin de le traiter "seulement" sur des exemples.

Exercice 30

Enoncé

Soient $n \geq 3$ et $A_1, \cdots, A_n$ les sommets d'un polygone régulier à n côtés inscrit dans un cercle centré en l'origine. Pour tout point P du plan, on considère la somme

$$\sum_{i=1}^{n} PA_i^2.$$

Montrer qu'elle ne dépend que de la distance de P à l'origine.

Indication de solution

Eléments de correction

Il s'agit de montrer que si

$$z_k = \exp\left(2i\pi \frac{k}{n}\right),$$

la somme

$$\sum_{k=1}^{n} |z - z_k|^2$$

ne dépend que de $|z|$. On développe et on trouve

$$\sum_k z\bar{z} - (\sum_k z_k)\bar{z} - (\sum_k \bar{z_k})z + \sum_k z_k \bar{z_k}$$

$$= n|z|^2 - 0.\bar{z} - 0.z + n = n(1 + |z|^2).$$

Exercice 31

Enoncé

Soit f une fonction positive, continue partout et dérivable deux fois en 0, de limite nulle en $\pm\infty$, telle que

$$f(x) = 1 \Leftrightarrow x = 0$$

et

$$\int_{\mathbb{R}} x^2 f(x) dx < +\infty$$

1) Justifier de l'existence et du caractère fini des quantités $A_n, \ n \geq 1$ définies par :

$$A_n = \int (f(x))^n \, x^2 dx$$

et donner la limite de A_n lorsque n tend vers l'infini.

2) On note $\alpha = -f''(0)$ et on suppose $\alpha \neq 0$. Donner un équivalent de A_n lorsque n tend vers l'infini en fonction des dérivées de f en zéro.

Indication: on donne

$$\int e^{\frac{-x^2}{2}} x^2 dx = \sqrt{2\pi}.$$

Eléments de correction

1) Comme f est continue et vaut 1 seulement en 0, on en déduit que $f(x) < 1$ pour $x \neq 0$. Les fonctions

$$x \mapsto (f(x))^n \, x^2$$

sont donc dominées par

$$f(x)x^2$$

De plus $f(x)^n x^2$ tend, pour tout x, vers 0. Le théorème de convergence dominée peut être appliqué et donne $\lim_{n\to\infty} A_n = 0$.

2) D'abord $f'(0)$ est nulle car f atteint son maximum en 0. De plus $\alpha = -f''(0)$ est la limite de la quantité

$$2\frac{1 - f(x)}{x^2}$$

qui est toujours positive. Donc $\alpha \geq 0$.

Pour la même raison $\exists \delta > 0$ tel que

$$|x| < \delta \Rightarrow \frac{1 - f(x)}{x^2} > \frac{\alpha}{4} (\text{ soit } f(x) \leq 1 - \frac{\alpha}{4} x^2).$$

Comme f tend vers 0 en l'infini f admet un maximum ρ sur l'ensemble $]-\infty, -\delta] \cup [\delta, +\infty[$, et $\rho < 1$.

Si bien que $\forall \eta > 0$

$$\int_{|x|>\eta} f(x)^n x^2 dx \leq M\beta^{n-1} \tag{12}$$

où

$$M = \int f(x) x^2 dx \text{ et } \beta = \max(\rho, 1 - \alpha \frac{\eta^2}{4})$$

(entre η et δ, f est plus petite que $1 - x^2\alpha/4 \leq 1 - \alpha\eta^2/4$, et après δ, c'est ρ qui majore).

On propose la stratégie suivante :

On va fixer un $\epsilon > 0$, choisir un $\eta > 0$ tel que f soit entre deux paraboles de dérivée seconde proche de $-\alpha$ à ϵ près. Au-delà de $\pm\eta$ la majoration exponentielle ci-dessus sera utilisée, et sur $[-\eta, \eta]$ on utilisera le théorème de convergence dominée pour exprimer l'intégrale comme une intégrale de gaussienne.

Soit $\epsilon > 0$. $\exists \eta > 0$ tel que

$$|x| \leq \eta \Rightarrow 1 - \frac{\alpha + \epsilon}{2} x^2 \leq f(x) \leq 1 - \frac{\alpha - \epsilon}{2} x^2. \tag{13}$$

Intéressons-nous à

$$C_n = \int_{-\eta}^{\eta} \left(1 - \frac{\alpha - \epsilon}{2} x^2\right)^n x^2 dx$$

(cette quantité majore l'intégrale sur $[-\eta, \eta]$ de $f^n x^2$).

Par le changement de variable $x = u/\sqrt{n}$ on a

$$C_n = \frac{1}{n\sqrt{n}} \int_{-\eta\sqrt{n}}^{\eta\sqrt{n}} \left(1 - \frac{\alpha - \epsilon}{2} \frac{u^2}{n}\right)^n u^2 du.$$

Or pout tout t la quantité $(1-t/n)^n$ converge vers e^{-t} et

$$n\ln\left(1-\frac{t}{n}\right)\leq -t=\ln(e^{-t})$$

On peut donc appliquer le théorème de convergence dominée qui donne que

$$\lim_{n\to\infty} n\sqrt{n}C_n=\int_{-\infty}^{\infty} e^{\left(-u^2\frac{\alpha-\epsilon}{2}\right)}u^2du. \tag{14}$$

De plus la fonction qui à z associe

$$F(z)=\int e^{-u^2\frac{z}{2}}u^2du=\sqrt{2\pi}\frac{1}{z\sqrt{z}}$$

est continûment dérivable en α. Il vient donc que, à partir d'un n assez grand

$$n\sqrt{n}C_n\leq\frac{\sqrt{2\pi}}{\alpha\sqrt{\alpha}}+\epsilon+9\alpha^{-\frac{5}{2}}\sqrt{2\pi}\epsilon$$

avec le ϵ provenant de la convergence (14), et le dernier terme du théorème des accroissements finis sur un intervalle autour de α pour la fonction $z^{-3/2}$.

On revient à A_n

$$n\sqrt{n}A_n=\int_{|x|<\eta}(f(x))^nx^2dx+n\sqrt{n}\int_{|x|\geq\eta}(f(x))^nx^2dx.$$

Vu la majoration (12), le terme

$$n\sqrt{n}\int_{|x|\geq\eta}(f(x))^nx^2dx$$

tend vers 0 et devient plus petit que ϵ à partir d'un certain rang.

On a donc, à partir d'un certain rang

$$n\sqrt{n}A_n\leq\frac{\sqrt{2\pi}}{\alpha\sqrt{\alpha}}+\epsilon+9\alpha^{-\frac{5}{2}}\sqrt{2\pi}\epsilon+\epsilon.$$

En faisant de même avec la partie minoration de (13) on a que, à partir d'un certain rang

$$n\sqrt{n}A_n \geq \frac{\sqrt{2\pi}}{\alpha\sqrt{\alpha}} - \epsilon - 9\alpha^{-\frac{5}{2}}\sqrt{2\pi}\epsilon - \epsilon.$$

Tout cela prouve que A_n est équivalent à

$$\frac{\sqrt{2\pi}}{\alpha\sqrt{\alpha}}\frac{1}{n\sqrt{n}}.$$

Exercice 32

Enoncé

Les réels a_n et b_n vérifient, $\forall n, 0 \leq a_n < b_n \leq 1$, les intervalles $[a_n, b_n[$ sont deux à deux disjoints et

$$\bigcup_n [a_n, b_n[= [0,1[.$$

1) Montrer que

$$\sum_n (b_n - a_n) = 1.$$

2) Si $A \subset [0,1[$ s'écrit $A = \cup_n [a_n, b_n[$ (non forcément disjoints), on appelle

$$l(A) = \lim_{N\to\infty} l(\cup_{n=0}^N A_n).$$

(on dit que $l(A)$ est la longueur de A). Montrer que $l(A)$ est bien définie (ne dépend pas du choix des a_i, b_i).

Eléments de correction

1) Le candidat peut appliquer le théorème de convergence dominée du programme en considérant:

$$\varphi_N = \mathbb{1}_{\cup^N [a_n, b_n[}$$

les φ_N convergent ponctuellement vers $\mathbb{1}_{[0,1[}$ et sont dominées par cette même fonction qui est **continue par morceau**. Leurs intégrales qui sont les sommes des $b_n - a_n$ tendent donc vers l'intégrale de la limite, qui est 1.

2) Le théorème de convergence dominée du programme **ne s'applique plus ici**.

Traitons d'abord le cas $A = [0,1[$ (en montrant que la limite est 1, ce qui montrera que la limite ne dépend pas des a_n, b_n). Si on note $A_N = \cup_{n=0}^{N} [a_n, b_n[$ et $B_{N+1} = A_{N+1} \backslash A_N$ et $B_0 = A_0$, alors chaque B_N est une union finie d'intervalles semi-ouverts disjoints

$$B_N = \cup_{k=1}^{K_N} [\alpha_N^k, \beta_N^k[$$

(Eventuellement $K_N = 0$ si B_N est vide) et les B_N sont disjoints deux à deux. De plus

$$l(A_N) = l(\cup_{n=0}^{N} B_n) = \sum_{n=0}^{N} l(B_n) = \sum_{n=0}^{N} \sum_{k=1}^{K} (\beta_n^k - \alpha_n^k).$$

Mais les $[\alpha_n^k, \beta_n^k[$ forment une partition de $[0,1[$ et en vertu de la question 1) leur somme vaut 1. (Remarque: nous n'avons manipulé que des longueurs d'unions finies pour lesquelles les notions intuitives d'additivité sont admises, on peut éventuellement les montrer).

Passons au cas général

D'abord si on note

$$u_n = l(\cup_{n=0}^{N} [a_n, b_n[)$$

alors u_n est une suite croissante majorée par 1 et elle converge.

Il reste à voir que si

$$\cup_n [a_n, b_n[= \cup_n [a'_n, b'_n[$$

et si

$$u_n = l(\cup_{n=0}^{N} [a_n, b_n[) \text{ et } v_n = l(\cup_{n=0}^{N} [a'_n, b'_n[)$$

alors u_n et v_n tendent vers la même limite.

Notons $A_N = \cup_{n=0}^N [a_n, b_n[$ et $A'_N = \cup_{n=0}^N [a'_n, b'_n[$. Ce sont des unions finies d'intervalles et ont peut les écrire comme

$$A_N = \cup_{k=1}^{K_N} [c_k^N, d_k^N[$$

avec les $[c_k^N, d_k^N[$ disjoints deux à deux (pour N fixé) et on peut choisir $K_N \leq N$ Comme u et v jouent des rôles symétriques, il suffit de montrer

$$\forall N, \exists N' \quad (n \geq N' \Rightarrow v_n \geq u_N).$$

Fixons N et abrégeons $K = K_N$ et $A_N = \cup_{k=1}^K [c_k, d_k[$. On note $C_n^k = A'_n \cap [c_k, d_k[$ (pour $k = 1 \dots K$). On remarque que pour n fixé les C_n^k sont disjoints et que la somme de leurs longueurs est plus petite que $l(A'_n)$. Remarquons également que (k fixé)

$$\cup_n C_n^k = (\cup_n A'_n) \cap [c_k, d_k[= A \cap [c_k, d_k[= [c_k, d_k[.$$

D'après la remarque du début de cette question (qui s'adapte à $A = [c_k, d_k[$) il vient que la limite des longueurs des $l(\cup_{i=0}^n C_i^k)$ (à k fixé et n tendant vers l'infini) est $d_k - c_k$. En sommant sur tous les k on voit que

$$\lim v_n \geq \sum_{k=1}^K (d_k - c_k) = u_N.$$

Exercice 33

Enoncé

Dans la suite on utilise comme norme sur les matrices la norme euclidienne canonique de $\mathbb{R}^{N \times N}$.

1) Soit A une matrice symétrique fixée. On suppose que toutes ses valeurs propres sont distinctes. Décrire toutes les matrices symétriques B de norme 1 qui maximisent la quantité

$$\|AB - BA\|^2.$$

2) Les matrices A et B sont tirées aléatoirement: Chaque coefficient sous la diagonale est tiré indépendamment de tous les autres et vaut -1 avec probabilité $\frac{1}{2}$ et +1 avec probabilité $\frac{1}{2}$. La

diagonale est tirée de la même manière. Les coefficients au-dessus de la diagonale sont des copies afin d'obtenir des matrices symétriques. Calculer

$$E\left[\|AB - BA\|^2\right]$$

et

$$E\left[\|AA\|^2\right].$$

3) On note λ_{max} et λ_{min} les valeurs propres maximale et minimale de A (ce sont des variables aléatoires). Montrer que

$$E\left[(\lambda_{max} - \lambda_{min})^2\right] \geq 2(N-1).$$

Eléments de correction

1) On commence par remarquer que la norme proposée ne change pas lorsque l'on fait un changement de base orthonormale, par exemple en remarquant qu'elle provient du produit scalaire $Tr(A^tB)$. Si $A = P^t\Lambda P$ avec P orthogonale et Λ la matrice diagonale portant les valeurs propres de A dans l'ordre croissant, on note alors $B_\lambda = PBP^t$ (la matrice (symétrique) exprimant B dans la B.O.N adaptée à A). Par abus de notation, on appelle b_{ij} les coefficients de B_λ. La somme de leurs carrés est toujours 1 car B est de norme 1. On veut maximiser

$$\|\Lambda B_\lambda - B_\lambda\Lambda\|^2 = \sum_{i,j}(\lambda_i - \lambda_j)^2 b_{ij}^2.$$

Cette somme est maximale lorsque les seuls b_{ij} non nuls sont en face du maximum possible pour $(\lambda_i - \lambda_j)^2$ (c'est une combinaison convexe de réels (positifs) $(\lambda_i - \lambda_j)^2$). Or, comme on a classé $\lambda_1 < \cdots < \lambda_N$, seuls b_{1N} et b_{N1} sont non nuls. Ils sont égaux (symétrie) et valent alors $\epsilon\sqrt{2}/2$ ($\epsilon = \pm 1$).

On note $v_1, \ldots, v_N$ les vecteurs propres de A. On peut donc décrire les matrices qui maximisent la quantité donnée: Il y en a deux en faisant varier $\epsilon = \pm 1$. Elle envoie v_1 sur $\epsilon\sqrt{2}/2 v_N$ et v_N sur $\epsilon\sqrt{2}/2 v_1$ et tous les autres v_i sur 0.

On peut aussi dire

$$B = \epsilon\frac{\sqrt{2}}{2}\left(v_N v_1^t + v_1 v_N^t\right).$$

(avec la convention qu'un vecteur est une matrice colonne)

Notons aussi que le maximum est $(\lambda_{max} - \lambda_{min})^2$. Et cela reste vrai même si les valeurs propres de A ne sont pas toutes distinctes.

2) Les deux se traitent de manière similaire. La diagonale de la matrice $AB - BA$ est nulle. Un coefficient non diagonal de la matrice $AB - BA$ s'écrit $< A_i|B_j > - < B_i|A_j >$ où A_i est la ligne (ou colonne) numéro i de A. Prenons, par exemple $i = 1$ et $j = 2$ (pour simplifier les notations), on s'intéresse à quatre vecteurs aléatoires A_1, A_2, B_1, B_2. Les composantes $3, 4 \ldots$ de ces quatre vecteurs sont indépendantes de toutes les autres. On remarque aussi que le produit de deux variables indépendantes valant ± 1 avec probabilité $1/2$ est encore une variable de même loi.

Si on singularise les composantes $A_1(2) = A_2(1) = \alpha$, $B_1(2) = B_2(1) = \beta$ et $A_1(1) = x$, $A_2(2) = y$, $B_1(1) = t$, $B_2(2) = z$ la composante $(1, 2)$ de $AB - BA$ s'écrit

$$\alpha(t - z) + \beta(y - x) + \sum_k \gamma_k$$

où les γ_k sont des variables ± 1 proba $1/2$ indépendantes de toutes les autres et remplacent les termes $A_1(k)B_2(k)$ et $-A_2(k)B_1(k)$ pour tous les $k \geq 3$. Il y a en tout $2(N - 2) = 2N - 4$ telles variables.

Si on élève au carré et que l'on prend l'espérance on a

$$E[(\alpha(t - z) + \beta(y - x) + \sum_k \gamma_k)^2] = E[\alpha^2(t - z)^2 + \beta^2(y - x)^2 + \sum_k \gamma_k^2]$$

$$= 2 + 2 + 2N - 4 = 2N$$

car les termes en jeu sont indépendants et de moyenne nulle.

Donc l'espérance du carré d'un terme hors diagonale est $2N$. (il y a $N^2 - N$ tels coefficients).

Les termes diagonaux sont nuls.

L'espérance de la norme au carré est la somme de ces espérances et donc

$$E[\|AB - BA\|^2] = 2N(N^2 - N) = 2N^2(N-1).$$

On procède de même pour la norme au carré de A^2. Cette fois les termes diagonaux ne sont pas nuls, ils valent exactement N. Les termes en dehors de la diagonale ont une espérance de leur carré valant N (c'est encore plus simple que ci-dessus, il ne reste que deux vecteurs A_1 et A_2 à considérer). Et enfin

$$E[\|A\|^2] = N^2N + (N^2 - N)N = 2N^3 - N^2 = N^2(2N-1).$$

3) Comme d'après la première question 1 on a que

$$\|AB - BA\|^2 = N^2\|A\frac{B}{N} - \frac{B}{N}A\|^2 \leq N^2(\lambda_{max} - \lambda_{min})^2$$

(on a divisé B par N pour la normer à 1 pour utiliser la première question). Le résultat est vérifié.

Exercice 34

Enoncé

Soit u_n ($n \in \mathbb{Z}$) une suite de nombre réels à support fini. On définit f_u sur $[-1/2, 1/2]$ par

$$f_u(t) = \sum u_n e^{-2i\pi nt}.$$

1) Exprimer $\int_0^1 f(t)dt$ et $\int_0^1 |f_u(t)|^2 dt$ en fonction des u_n.

2) On définit les quantités σ^2 et $\hat{\sigma}^2$ par

$$\begin{aligned} \sigma^2 &= \sum m^2(u_m + u_{m+1})^2, \\ \hat{\sigma}^2 &= \int_0^1 \sin(2\pi t)^2 |f_u(t)|^2 dt. \end{aligned}$$

On suppose que

$$\sum (u_m - u_{m-1})(u_{m-1} - u_{m-2}) \geq (1-\epsilon) \sum (u_m - u_{m-1})^2.$$

Montrer que

$$\sigma\hat{\sigma}\sqrt{\frac{1}{1-\frac{1}{2}\epsilon}} \geq \sum u_m^2. \tag{15}$$

3) Pour $N \geq 2$ on définit

$$u_n^N = \binom{2N}{N+n}$$

(Il s'agit d'une suite à support fini dépendant de N. Ce N n'est pas une puissance.)

Donner des expressions simples pour les quantités suivantes et en donner un équivalent

$$A_N = \sum u_n^2,$$

$$B_N = \hat{\sigma}^2,$$

$$C_N = \sum n^2 u_n^2.$$

Eléments de correction

1) On a facilement $\int_0^1 f_u(t)dt = u_0$ (intégrales d'exponentielles complexes de période 1, seule la puissance 0 reste).

On remarque que $|z|^2 = z\bar{z}$ et on écrit (toutes les sommes sont finies et les u_n sont réels).

$$\int_0^1 f_u(t)\overline{f_u(t)}dt = \sum_k \sum_l \int_0^1 u_k u_l e^{2i\pi t(l-k)}dt = \sum_{k=l} u_k u_l = \sum u_n^2.$$

2) On cherche à appliquer ce qui précède à

$$\hat{\sigma}^2 = \int_0^1 \sin(2\pi t)^2 |f_u(t)|^2 dt = \int_0^1 \left|\left(\frac{e^{2i\pi t} - e^{-2i\pi t}}{2i}\right) f_u(t)\right|^2 dt$$

$$= \frac{1}{4}\int_0^1 \left|\left(e^{2i\pi t} f_u(t) - e^{-2i\pi t} f_u(t)\right)\right|^2.$$

Or

$$e^{2i\pi t} f_u(t) = \sum u_n e^{-2i\pi t(n-1)} = \sum u_{m+1} e^{-2i\pi tm}$$

(et de même pour $e^{-2i\pi t} f_u(t)$ qui donne des u_{m-1}).

En appliquant la question 1 on trouve

$$\hat{\sigma}^2 = \frac{1}{4} \sum (u_{m+1} - u_{m-1})^2.$$

On montrera plus tard que, grâce à l'hypothèse,

$$\sum (u_{m+1} - u_{m-1})^2 \geq (4 - 2\epsilon) \sum (u_n - u_{n-1})^2. \tag{16}$$

On peut écrire

$$\sum u_m^2 = \sum u_m^2 (m - (m-1))$$

Puis en changeant les indices, on trouve, (toutes les sommes sont finies, bien sûr)

$$\sum u_m^2 = \sum m(u_m^2 - u_{m+1}^2) = \sum m(u_m + u_{m+1})(u_m - u_{m+1}).$$

Il s'agit d'un produit scalaire entre les suites $m(u_m + u_{m+1})$ et $(u_m - u_{m+1})$, on applique Cauchy-Schwartz et on a

$$\left(\sum u_m^2\right)^2 \leq \left(\sum m^2 (u_m + u_{m+1})^2\right) \left(\sum (u_m - u_{m+1})^2\right) = \sigma^2 \left(\sum (u_m - u_{m+1})^2\right).$$

Si on admet (16) on a

$$\left(\sum u_m^2\right)^2 \leq \sigma^2 \frac{4}{4 - 2\epsilon} \hat{\sigma}^2$$

qui est ce qui est demandé.

Montrons (16). Il est commode d'introduire $u_n^k = u_{n-k}$. La suite u^k est la décalée de la suite u de k positions vers la droite. Il nous faut montrer

$$\|u^{-1} - u^1\|^2 \geq (4 - 2\epsilon) \|u^1 - u^0\|^2,$$

(Où $\|u\|^2 = \sum_n u_n^2$).

On écrit

$$\|u^{-1} - u^1\|^2 = \|u^{-1} - u^0 + u^0 - u^1\|^2 = \|u^{-1} - u^0\|^2 + \|u^1 - u^0\|^2 + 2\left\langle u^{-1} - u^0, u^0 - u^1 \right\rangle. \tag{17}$$

Mais par changements d'indices on a

$$\|u^{-1} - u^0\|^2 = \|u^1 - u^0\|^2$$

et

$$\langle u^{-1} - u^0, u^0 - u^1 \rangle = \sum (u_m - u_{m-1})(u_{m-1} - u_{m-2}) \geq (1 - \epsilon)\|u^1 - u^0\|^2$$

la dernière inégalité étant l'hypothèse.

En remplaçant dans (17), on a finalement,

$$\|u^{-1} - u^1\|^2 \geq (4 - 2\epsilon)\|u^1 - u_0\|^2.$$

3) On calcule $f_u(t)$ dans ce cas

$$f_u(t) = \sum_{n=-N}^{N} e^{-2i\pi nt} \binom{2N}{N+n} = \sum_{m=0=N+n}^{2N} e^{i\pi t(2N-2m)} \binom{2N}{m}$$

$$= \sum_{m=0}^{2N} e^{i\pi t(2N-m)} e^{-i\pi tm} \binom{2N}{m} = \left(e^{i\pi t} + e^{-i\pi t}\right)^{2N} = (2\cos(\pi t))^{2N}.$$

Attention c'est bien $\cos(\pi t)$ et non pas $\cos(2\pi t)$.

Il vient, par la question 1 que $\int f_u dt = \binom{2N}{N}$ et donc la formule qui servira par la suite

$$\int_0^1 (2\cos(\pi t))^{2N} dt = \binom{2N}{N}.$$

On a

$$A_N = \int f_u^2 = \binom{4N}{2N}$$

dont un équivalent est (Stirling)

$$A_N \sim 2^{4N} \frac{1}{\sqrt{2\pi N}}.$$

Pour le calcul de $\hat{\sigma}^2$ on remarque que $\sin(2\pi t)^2 = 4\cos(\pi t)^2 - 4\cos(\pi t)^4$ ce qui donne (on note $c = \cos(\pi t)$)

$$B_N = \hat{\sigma}^2 = \int_0^1 4c^2(2c)^{4N} - 4c^4(2c)^{4N} = \int (2c)^{4N+2} - \frac{1}{4}(2c)^{4N+4} = \binom{4N+2}{2N+1} - \frac{1}{4}\binom{4N+4}{2N+2}$$

dont un équivalent est

$$B_N = \binom{4N+2}{2N+1}\left[1 - \frac{1}{4}\frac{(4N+4)(4N+3)}{(2N+2)^2}\right] = \binom{4N+2}{2N+1}\frac{4N+4}{4(2N+2)^2} \sim 2^{4N}\frac{1}{N\sqrt{2\pi N}}.$$

Enfin, on remarque que la fonction f_u' s'écrit

$$f_u' = \sum -2i\pi n e^{-2i\pi n t} u_n.$$

Le module au carré ne change par en divisant par i, et en appliquant la question 1 on a

$$C_N = \sum m^2 u_n^2 = \frac{1}{4\pi^2}\int |f_u'|^2,$$

$$f_u' = 2N(-\pi)2\sin(\pi t)(2\cos(\pi t))^{2N-1}.$$

Soit en élevant au carré et reprenant $c = \cos(\pi t)$

$$|f_u'|^2 = 4N^2\pi^2 4(1-c^2)(2c)^{4N-2}.$$

Ce qui donne

$$C_N = 16N^2\left[\binom{4N-2}{2N-1} - \frac{1}{4}\binom{4N}{2N}\right]$$

dont un équivalent est (on fait comme pour B_N)

$$C_N \sim 4 \times 2^{4N}\frac{N}{\sqrt{2\pi N}}.$$

On remarque que l'on a $\frac{B_N C_N}{A_N^2}$ tend bien vers 4. C'est plus fort que le résultat de la question 2. Ici u_n^2 dans la définition de C_N joue le rôle de $\frac{1}{2}(u_m + u_{m+1})$ dans la définition de σ^2. C'est l'"optimalité" de la gaussienne discrète dans le principe d'incertitude.

Exercice 35

Enoncé

Dans tout cet exercice f est une fonction continue sur $[0, 1]$ et n un entier destiné à tendre vers l'infini.

1) Quelle est la limite ($n \to \infty$) de

$$n \int_0^1 f(t) t^n dt \ ?$$

2) Donner un équivalent de

$$\int_0^1 f(t) \left(\cos(2\pi t)\right)^{2n} dt$$

(pour cette question $f > 0$ pour éviter un premier ordre nul.)

3) Même question pour:

$$\int_0^1 \left(\cos(2\pi n t)\right)^{2n} f(t) dt$$

avec f de la forme

$$f(t) = C + \sum_{k=1}^{N} \alpha_k \cos(2\pi k t)$$

où $C \neq 0$ est non nulle. Commentaire.

Eléments de correction

1) La limite est: $f(1)$. On note $A_n(f) = n \int_0^1 t^n f(t) dt$. La fonction A_n est linéaire en f. Si f est constante $A_n(f) = n/(n+1) f(1)$. Montrons que si $f(1) = 0$ alors $A_n(f)$ tend vers 0. Cela aura démontré le résultat en écrivant

$$A_n(f) = n/(n+1) f(1) + A_n(f - f(1)).$$

Donc, $f(1) = 0$ et soit $\epsilon > 0$. On note $M = \max |f(t)|$

$$\exists \eta, \quad \text{tel que } t \geq 1 - \eta, |f(t)| \leq \epsilon.$$

On a

$$\int_0^{1-\eta} f(t) t^n dt \leq M(1-\eta)^n \text{ et } \left| \int_{1-\eta}^1 f(t) t^n dt \right| \leq \epsilon \int_{1-\eta} t^n dt \leq \epsilon \int_0^1 t^n dt = \frac{\epsilon}{n+1} \leq \epsilon.$$

Mais $nM(1-\eta)^n$ tend vers 0 en l'infini. Ceci démontre le résultat.

2) La réponse est: $\sim \sqrt{\frac{1}{\pi n}}\frac{f(0)+2f(\frac{1}{2})+f(1)}{4}$.

Une rapide investigation graphique fait comprendre que les points importants sont $0, 1/2$ et 1, car ailleurs la fonction $\cos(2\pi t)^{2n}$ écrase exponentiellement la fonction f. On note $M = \max|f(t)|$ et soit $\epsilon > 0$ et η un module d'uniforme continuité associé à ϵ. On va regarder la partie entre 0 et $1/4$, les autres parties de l'intégrale se comporteront de la même manière.

D'abord on a

$$\int_0^1 (\cos(2\pi t))^{2n}\, dt = \frac{1}{2^{2n}}\binom{2n}{n} \sim \frac{1}{\sqrt{\pi n}}.$$

En effet, il suffit d'écrire $\cos(2\pi t) = \frac{1}{2}(e^{2i\pi t} + e^{-2i\pi t})$ et de développer le binôme de Newton. La seule intégrale qui n'est pas nulle est celle correspondant au coefficient $\binom{2n}{n}$ (et l'équivalent est donné par la formule de Stirling).

De plus, en raison des symétries de la fonction cosinus, on a:

$$\int_0^{1/4} (\cos(2\pi t))^{2n}\, dt = \frac{1}{4}\int_0^1 (\cos(2\pi t))^{2n}\, dt \sim \frac{1}{4\sqrt{\pi n}}.$$

Soit donc A_n la partie de l'intégrale entre 0 et $1/4$

$$A_n = \int_0^{1/4} f(t)\,(\cos(2\pi t))^{2n}\, dt$$

et on a

$$\left|A_n - f(0)\frac{1}{4}\frac{1}{2^{2n}}\binom{2n}{n}\right| \le \int_0^{1/4} |f(t) - f(0)|\,(\cos(2\pi t))^{2n}\, dt$$

$$\le \int_0^{\eta} \epsilon\,(\cos(2\pi t))^{2n}\, dt + \int_{\eta}^{1/4} 2M\,(\cos(2\pi\eta))^{2n}\, dt$$

car $\cos(2\pi t)$ est décroissante sur $[0, 1/4]$

$$\le \epsilon\frac{1}{4}\frac{1}{2^{2n}}\binom{2n}{n} + \frac{M}{2}\,(\cos(2\pi\eta))^{2n}.$$

En multipliant par $4\sqrt{\pi n}$ on a

$$4\sqrt{\pi n}A_n \le (f(0)+\epsilon)\frac{1}{4}\frac{1}{2^{2n}}4\sqrt{\pi n} + \frac{M}{2}\,(\cos(2\pi\eta))^{2n}\,4\sqrt{\pi n}.$$

Pour n assez grand on a

$$4\sqrt{\pi n}A_n \leq (f(0)+\epsilon)\frac{1}{4}\frac{1}{2^{2n}}4\sqrt{\pi n}+\epsilon.$$

On a aussi pour n assez grand

$$4\sqrt{\pi n}A_n \geq (f(0)-\epsilon)\frac{1}{4}\frac{1}{2^{2n}}4\sqrt{\pi n}-\epsilon.$$

Tout cela prouve que $4\sqrt{\pi n}A_n$ tend vers $f(0)$.

En faisant de même autour de 1/2 (attention contribution double) et de 1 on a le résultat

$$\int_0^1 (\cos(2\pi nt))^{2n} f(t)dt \sim \frac{1}{4\sqrt{\pi n}}\left(f(0)+2f(1/2)+f(1)\right).$$

3) $\sim \frac{1}{\sqrt{\pi n}}\int_0^1 f(t)dt$

On a encore une fois

$$(\cos(2\pi nt))^{2n} = \frac{1}{2^{2n}}\sum_{m=-n}^{n}\binom{2n}{n+m}e^{-2i\pi t(2n).m}. \tag{18}$$

Et pour f de la forme proposée, dès que $2n > N$ on a

$$\int_0^1 (\cos(2\pi nt))^{2n} f(t)dt = C\frac{1}{2^{2n}}\binom{2n}{n} \sim C\frac{1}{\sqrt{\pi n}}$$

car toutes les exponentielles dans (18) ont une puissance strictement plus grande que N sauf le coefficient 0.

On note que par rapport à la question précédente, la constante n'est plus des valeurs ponctuelles de f mais $\int f(t)dt$.

Exercice 36

Enoncé

On appelle dérangement de taille $n \geq 1$ une permutation σ de l'ensemble $[\![1,n]\!]$ telle que pour tout i $\sigma(i) \neq i$. On appelle $D(n)$ le nombre de dérangements de taille n.

1) Montrer que $D(n)$ est le plus proche entier de $\frac{n!}{e}$.

2) On note

$$S(n) = \sum_{\sigma \text{ dérangement}} \epsilon(\sigma)$$

(la somme des signatures des dérangements de taille n). Donner une expression simple de $S(n)$.

3) Pour $m \geq 1$, on note $D_m(n)$ le nombre de permutations de taille n qui n'ont aucun cycle de taille inférieure ou égale à m. Donner une expression simple de

$$f_m(t) = 1 + \sum_{n \geq 1} \frac{D_m(n)}{n!} t^n.$$

4) En déduire, pour m fixé, que pour tout N et tout $0 < \gamma < 1$ il existe un $n \geq N$ tel que $D_m(n) \geq \gamma^n n!$

Eléments de correction

1) On peut commencer par chercher une formule pour l'entier le plus proche de $n!/e$

$$\frac{n!}{e} = n! \sum_k \frac{(-1)^k}{k!} = \sum_{k \leq n} (-1)^k \frac{n!}{k!} + n! \sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}.$$

Le premier terme de la somme est un entier. Le second est $n!$ fois la somme d'une série alternée dont la valeur absolue est toujours plus petite que celle du premier terme. Le second terme est donc plus petit (en valeur absolue) que $n!/(n+1)! = 1/(n+1) < 1$.

L'entier le plus proche de $n!/e$ a donc pour formule:

$$\sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$

et on nous demande de démontrer que:

$$D(n) = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}, \tag{19}$$

$D(1) = 0$ (il n'y a que l'identité comme permutation de taille 1) et $D(2) = 1$ (il n'y a que la transposition de taille 2 qui n'ait pas de points fixes) sont bien égaux à la formule ci-dessus.

Par ailleurs, on montre la formule de récurrence suivante

$$D(n+1) = \sum_{l=2}^{n+1} (l-1)! \binom{n}{l-1} D(n-l+1) \tag{20}$$

avec la convention $D(0) = 1$.

En effet, pour passer de n à $n+1$ on choisit la longueur l du cycle contenant $n+1$. Cette longueur doit être au moins 2. On choisit $l-1$ éléments dans $[\![1, n]\!]$ et le l-ième est $n+1$ lui-même. Il y a $(l-1)!$ manière d'arranger un cycle de support fixé de taille l. Il y a $\binom{n}{l-1}$ manière de choisir les $l-1$ éléments qui ne sont pas $n+1$ et enfin il faut trouver sur le reste de l'ensemble un dérangement ce qui donne le facteur $D(n-l+1)$.

Faisons la récurrence (passage de n à $n+1$, dans la formule (20) je singularise le cas $l = n+1$ car $D(0) = 1$ correspondant ne vérifie pas la formule (19))

$$D(n+1) = n! + \sum_{l=2}^{n} \frac{n!}{(n-l+1)!} D(n-l+1) = n! + n! \sum_{l=2}^{n} \sum_{k=0}^{n-l+1} \frac{(-1)^k}{k!}$$

$$= n! + n! \sum_{t=1}^{n-1} \sum_{k=0}^{t} \frac{(-1)^k}{k!}.$$

Le terme $k = 0$ apparait en tout $n-1$ fois, le terme $k = 1$ apparait $n-1$ fois également, le terme $n-1 \geq k \geq 1$ apparait $n-k$ fois.

$$D(n+1) = n! + n! \left[-1 \times (-1)^0/0! + \sum_{k=0}^{n-1} (n-k) \frac{(-1)^k}{k!} \right] = n! \left[\sum_{k=0}^{n-1} (n-k) \frac{(-1)^k}{k!} \right]$$

$$= n! \left[\sum_{u=0}^{n-2} \frac{(-1)^u}{u!} + n \sum_{k=0}^{n-1} \frac{(-1)^k}{k!} \right] = n! \left[(n+1) \sum_{u=0}^{n-2} \frac{(-1)^u}{u!} + n \frac{(-1)^{n-1}}{(n-1)!} \right]$$

$$= (n+1)! \sum_{u=0}^{n-2} \frac{(-1)^u}{u!} + (-1)^{n-1} n^2.$$

Or les trois derniers termes de (19) quand on remplace par $n+1$ sont

$$(n+1)!\left((-1)^{n-1}/(n-1)! + (-1)^{n}/n! + (-1)^{n+1}/(n+1)!\right)$$

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

La récurrence est donc démontrée.

2) On a $S(1) = 0$, $S(2) = -1$ par la suite on fera la convention $S(0) = 1$. Comme ci-dessus, on va établir une formule de récurrence. Pour passer de n à $n+1$, on choisit le cycle dans lequel sera $n+1$, ce cycle sera de taille l. On doit avoir $l \geq 2$ car sinon notre permutation aurait un point fixe. Il y a $\binom{n}{l-1}$ tels supports de cycles et $(l-1)!$ manières de les arranger quand le support est choisi. Puis on somme sur tous les dérangements de taille $n+1-l$ les signatures que l'on multiplie par la signature du cycle de taille l qui est $(-1)^{l-1}$. Il vient:

$$S(n+1) = \sum_{l=2}^{n+1}(l-1)!\binom{n}{l-1}(-1)^{l-1}S(n+1-l) = \sum_{l=2}^{n+1}\frac{n!}{(n-l+1)!}(-1)^{l-1}S(n+1-l)$$

avec la convention $S(0) = 1$. Quelques applications numériques suggèrent la formule

$$S(n) = (-1)^{n-1}(n-1)$$

(pour $n \geq 0$)

On va la montrer par récurrence. On la vérifie jusqu'à $n = 3$ et on passe de n à $n+1$. Le terme $l = n+1$ donne $(-1)^n n!$ et le terme $l = n$ donne 0

$$S(n+1) = (-1)^n n! + \sum_{l=2}^{n-1}(-1)^{n-l+l-1}\frac{n!(n-l)}{(n-l+1)!} = (-1)^n n!\left[1 - \sum_{l=2}^{n-1}\frac{n-l}{(n-l+1)!}\right]$$

$$S(n+1) = (-1)^n n!\left[1 - \sum_{l=2}^{n-1}\frac{1}{(n-l+1)(n-l-1)!}\right]$$

$$S(n+1) = (-1)^n n!\left[1 - \sum_{u=0}^{n-3}\frac{1}{u+2}\frac{1}{u!}\right].$$

Il ne reste plus qu'à montrer que

$$\sum_{u=0}^{n-3} \frac{1}{u+2}\frac{1}{u!} = \frac{(n-1)!-1}{(n-1)!}$$

ce qui ne présente pas de difficulté.

3) La fonction f_m est une série entière de rayon de convergence au moins 1 car $D_m(n) \leq n!$. Elle vaut 1 en 0. Elle est strictement positive sur $[0,1]$ car les coefficients $D_m(n)$ sont positifs. Elle est $\mathcal{C}^\infty$ sur $]-1,1[$.

On écrit l'équation de récurrence (comme ci-dessus, on choisit des cycles de taille $> m$)

$$D_m(n+1) = \sum_{l=m+1}^{n+1} \binom{n}{l-1}(l-1)!D_m(n+1-l)$$

avec la convention $D_m(0) = 1$ qui est compatible avec la définition de f_m. En simplifiant $(l-1)!$ et en divisant par $(n+1)!$ on a

$$(n+1)\frac{D_m(n+1)}{(n+1)!} = \sum_{l=m+1}^{n+1} \frac{D_m(n+1-l)}{(n-l+1)!} = \sum_{u=0}^{n-m} \frac{D(u)}{u!}.$$

Le coefficient

$$(n+1)\frac{D_m(n+1)}{(n+1)!}$$

est le n-ième coefficient de f_m'.

Le coefficient

$$\sum_{u=0}^{n-m} \frac{D(u)}{u!}$$

est le $(n-m)$-ième coefficient de $\frac{f_m(t)}{1-t}$. C'est aussi le n-ième coefficient de $\frac{f_m(t)}{1-t} \times t^m$.

On en déduit l'équation différentielle

$$f_m'(t) = \frac{f_m(t)t^m}{1-t}.$$

Soit, au moins sur $t \in [0,1[$,

$$\frac{f'_m(t)}{f_m(t)} = \frac{t^m}{1-t} = -(1+t+t^2+\cdots+t^{m-1}) + \frac{1}{1-t}.$$

On intègre et on trouve

$$\ln(f_m(t)) = -\ln(1-t) - (t + t^2/2 + \cdots + t^m/m) + C$$

mais la constante C doit être nulle car $f_m(0) = 1$ (Convention $D_m(0) = 1$ qui rend possible la formule de récurrence).

Au final

$$f_m(t) = \frac{1}{1-t} e^{-\left(t+\frac{t^2}{2}+\cdots+\frac{t^m}{m}\right)}.$$

Cette formule est démontrée pour l'intervalle $[0,1[$ mais comme les deux fonctions sont dévelopables en série entière de rayon au moins 1, elle est valable sur tout $]-1,1[$.

4) La négation de ce qui est demandé est

$$\exists 0 < \gamma < 1, N \quad \forall n \geq N \quad D_m(n) < \gamma^n n!.$$

Mais dans ce cas la série définissant f_m serait de rayon de convergence au moins $1/\gamma > 1$ en particulier $f_m(1)$ serait fini. Or la fonction

$$\frac{1}{1-t} e^{-\left(t+\frac{t^2}{2}+\cdots+\frac{t^m}{m}\right)}$$

diverge en $t = 1$ (tend vers $+\infty$ en 1^-). Absurde.

Exercice 37

Enoncé

1) Pour n un nombre premier, montrer que

$$n \mid 1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} + 1.$$

2) Trouver tous les nombres entiers $n \geq 1$ tels que

$$n \mid 1^n + 2^n + \cdots + (n-1)^n.$$

Eléments de correction

1) Par le théorème de Lagrange $a^{n-1} \equiv 1[n]$ pour tout a premier avec p, car a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et car l'ordre du groupe des inversibles est $n-1$. Donc la somme considérée vaut $1 + 1 + \cdots + 1 + 1 \equiv n \equiv 0$ modulo n.

2) On peut regarder d'abord le cas n impair.

Si n est impair on regroupe k avec $n-k$ (on n'aura jamais $k = n-k$) et on a

$$k^n + (n-k)^n = k^n + \sum_l n^l (-1)^{n-l} k^{n-l} \binom{n}{l}.$$

Modulo n seul le terme $l = 0$ reste dans la somme et vaut $-k^n$ car n est impair. Donc n divise bien la somme. Tous les entiers impairs vérifient la propriété. Ce sont les seuls comme on va le voir.

Maintenant n est pair de la forme $n = 2^s m$ avec $s > 0$ et m impair. On se demande quel est le reste modulo 2^s de k^n.

Si k est impair alors $k^{2^{s-1}} \equiv 1[2^s]$. En effet le groupe des inversibles de $\mathbb{Z}/2^s\mathbb{Z}$ est de cardinal 2^{s-1} (i.e. les nombres impairs) et par le théorème de Lagrange on conclut. Il vient que $k^n \equiv 1[2^s]$ car n est multiple de 2^{s-1}.

Si $k = 2l$ est pair, on a que $n \geq 2^s$ et donc $k^n = 2^n l^n$ est divisible par 2^{2^s}. Donc $k^n \equiv 0[2^s]$.

On en conclut que

$$1^n + 2^n + \cdots + (n-1)^n \equiv \frac{n}{2}[2^s]$$

car il y a exactement $n/2$ nombres impairs entre 1 et $n-1$.

Si n divisait $1^n + 2^n + \cdots + (n-1)^n$ alors cette somme serait congrue à 0 modulo 2^s (qui divise n) et on aurait $n/2 \equiv 0[2^s]$ et 2^{s+1} diviserait n ce qui est contradictoire avec la définition de s.

Exercice 38

Enoncé

On commence un jeu avec $n_b > 0$ boules bleues et $n_r > 0$ boules rouges. On lance une pièce dont une face est bleue et l'autre rouge. Lorsque le lancer de la pièce donne bleu, on enlève une boule bleue, de même lorsque le lancer donne rouge. La probabilité de lancer bleu est p et celle de lancer rouge $1-p$. On appelle $T(k)$ le nombre total de boules restantes au bout de k étapes.

1) Trouver la probabilité p_0 qui minimise $E[T(n_b+n_r)^2]$.

2) On appelle K_0 le nombre d'étapes avant la fin du jeu. Dans le cas où $n_b = n_r = K$, montrer que

$$E[K_0 - 2K] = \left(\frac{1}{2}\right)^{2K} 4 \sum_{k=1}^{K} k \binom{2K}{K+k}.$$

Eléments de correction

1) On va noter $N = n_b + n_r = T(0)$.

Après $n_b + n_r = N$ opérations l'une des deux catégories (rouge ou bleue) sera éliminée, et il restera un certain nombre de boules de l'autre catégorie. Après N opérations, si on note k le nombre de lancers donnant la couleur bleue, il va rester

$$\begin{aligned} &n_b - k \text{ boules bleues, si } k \leq n_b, \\ &n_r - (N-k) \text{ boules rouges, si } N-k \leq n_r. \end{aligned}$$

Soit

$$n_b - k \text{ boules bleues, si } k \leq n_b,$$
$$k - n_b \text{ boules rouges, si } k \geq n_b.$$

Comme on a toujours $(n_b - k)^2 = (k - n_b)^2$ et que la probabilité d'avoir k tirages bleus est $p^k(1-p)^{N-k}\binom{N}{k}$. Il vient que l'espérance de $T(N)^2$ est

$$E[T(n_b + n_r)^2] = \sum_{k=0}^{N} p^k (1-p)^{N-k} \binom{N}{k} (k - n_b)^2.$$

On appelle $P(x)$ le polynôme

$$P(x) = \sum_{k=0}^{N} x^k p^k (1-p)^{N-k} \binom{N}{k} = (1 - p + px)^N.$$

On voit que

$$P(1) = 1,\ P'(1) = \sum_{k=0}^{N} k p^k (1-p)^{N-k} \binom{N}{k},\ P''(1) = \sum_{k=0}^{N} k(k-1) p^k (1-p)^{N-k} \binom{N}{k}.$$

Et on a (noter que $k^2 = k(k-1) + k$)

$$E[T(n_b + n_r)^2] = P''(1) - (2n_b - 1)P'(1) + n_b^2 P(1).$$

Par ailleurs,

$$P(1) = 1,\ P'(1) = Np,\ P''(1) = N(N-1)p^2.$$

Soit

$$E[T(n_b + n_r)^2] = P''(1) + (2n_b - 1)P'(1) + n_b^2 = N(N-1)p^2 - (2n_b - 1)Np + n_b^2$$

qui est minimale pour

$$p_0 = \frac{2n_b - 1}{2(N-1)}$$

(bien que non intuitif, le résultat est bien symétrique car en échangeant n_r et n_b, on aurait $(2n_r - 1)/2(N-1) = 1 - (2n_b - 1)/2(N-1)$).

2) On suppose qu'il reste k boules (rouges ou bleues importe peu, on va supposer qu'il reste des bleues) après $N = 2K$ étapes.

On commence par montrer que l'espérance du nombre d'étapes, après $2K$ tirages, pour finir le jeu est exactement $2k$.

Si $k = 0$, c'est fini.

Sachant qu'il reste k boules, la probabilités de finir en $l + k$ est donnée par

$$\left(\frac{1}{2}\right)^{k-1} \left(\frac{1}{2}\right)^{l} \binom{l+k-1}{l} \frac{1}{2}$$

(il faut tirer $k - 1$ bleues parmi les $l + k - 1$ premières étapes et tirer une bleue finale).

L'espérance du nombre d'étapes est donc

$$\sum_{l=0}^{\infty} (k+l) \left(\frac{1}{2}\right)^{k} \left(\frac{1}{2}\right)^{l} \binom{l+k-1}{l} = k \sum_{l=0}^{\infty} \left(\frac{1}{2}\right)^{k} \left(\frac{1}{2}\right)^{l} \binom{l+k}{l}.$$

Il faut montrer que la quantité S_k définie par

$$S_k = \sum_{l=0}^{\infty} \left(\frac{1}{2}\right)^{k} \left(\frac{1}{2}\right)^{l} \binom{l+k}{l}$$

vaut toujours 2. On vérifie bien que $S_0 = 2$. Puis par récurrence

$$S_{k+1} = \sum_{l=0}^{\infty} \left(\frac{1}{2}\right)^{k+1} \left(\frac{1}{2}\right)^{l} \binom{l+k+1}{l} = \left(\frac{1}{2}\right)^{k+1} + \sum_{l=1}^{\infty} \left(\frac{1}{2}\right)^{k+1} \left(\frac{1}{2}\right)^{l} \binom{l+k+1}{l}$$

$$= \left(\frac{1}{2}\right)^{k+1} + \sum_{l=1}^{\infty} \left(\frac{1}{2}\right)^{k+1} \left(\frac{1}{2}\right)^{l} \left[\binom{l+k}{l-1} + \binom{l+k}{l}\right]$$

$$= \left(\frac{1}{2}\right)^{k+1} + \sum_{t=0}^{\infty} \left(\frac{1}{2}\right)^{k+1} \left(\frac{1}{2}\right)^{t+1} \binom{t+k+1}{t} + \sum_{l=1}^{\infty} \left(\frac{1}{2}\right)^{k+1} \left(\frac{1}{2}\right)^{l} \binom{l+k}{l}$$

$$= \sum_{t=0}^{\infty} \left(\frac{1}{2}\right)^{k+1} \frac{1}{2} \left(\frac{1}{2}\right)^{t} \binom{t+k+1}{t} + \frac{1}{2} \left(\frac{1}{2}\right)^{k} + \sum_{l=1}^{\infty} \frac{1}{2} \left(\frac{1}{2}\right)^{k} \left(\frac{1}{2}\right)^{l} \binom{l+k}{l}.$$

$$S_{k+1} = \frac{1}{2} S_{k+1} + \frac{1}{2} S_k = \frac{1}{2} S_{k+1} + 1.$$

D'où $S_{k+1} = 2$.

Enfin, il nous reste à évaluer l'espérance

$$E[K_0 - 2K] = \sum_{k=0}^{K} Proba(T(2K) = k) E[\text{ nombre de coups restant sachant } T(2K) = k]$$
$$= \sum_{k=0}^{K} Proba(T(2K) = k) 2k.$$

Mais (pour $k > 0$)

$$Proba(T(2K) = k) = 2 \binom{2K}{K+k} \left(\frac{1}{2}\right)^{2K}.$$

Il y a un facteur 2 car on peut avoir k boules bleues ou k boules rouges après $2K$ étapes. Puis il faut choisir $K + k$ positions pour les tirages rouges (ou bleus) parmi les $2K$ tirages. La proba $T(2K) = 0$ est inutile puisqu'elle ne change pas l'espérance. On a donc:

$$E[K_0 - 2K] = 4 \left(\frac{1}{2}\right)^{2K} \sum_{k=1}^{K} \binom{2K}{K+k} k.$$

Exercice 39

Enoncé

1) Soient A et B deux matrices symétriques définies positives. Montrer qu'il existe une unique matrice C symétrique telle que

$$B = AC + CA$$

Montrer que C est définie positive.

2) Décrire toutes les matrices A et C de taille 2, symétriques et définies positives, telles que $AC + CA$ ne soit pas définie positive.

Eléments de correction

1) On note b'_{ij} les coefficients de B après changement de base orthonormée qui diagonalise A. On note c'_{ij} les coefficients de C dans cette même base. On a nécessairement

$$b'_{ij} = c'_{ij}(\lambda_i + \lambda_j)$$

où les $\lambda_i > 0$ sont les valeurs propres de A. Et donc C est bien unique (ses coefficients dans la base orthonormée diagonalisant A sont $\frac{b'_{ij}}{\lambda_i+\lambda_j}$).

Il reste à voir que C est définie positive. On sait que toute matrice symétrique définie positive a des coefficients diagonaux strictement positifs. En effet,

$$a_{ii} = \langle Ae_i, e_i \rangle > 0$$

((e_i) est la base canonique).

Si on appelle a''_{ij} et b''_{ij} les coefficients de A et B dans une base orthonormée qui diagonalise C alors on a

$$b''_{ii} = a''_{ii} 2\gamma_i$$

où γ_i sont les valeurs propres de C. Comme les a''_{ii} et les b''_{ii} sont strictement positifs, il en va de même de γ_i.

2) Pour décrire toutes les matrices demandées, on suppose d'abord A diagonale. Si A n'a qu'une seule valeur propre, alors A est une homothétie de rapport λ et $AC + CA = 2\lambda C$ est définie positive. Pour la même raison C ne peut pas être diagonale.

Quitte à diviser par la plus petite valeur propre de A et par le coefficient $(1,1)$ de C on cherche des matrices de la forme

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1+\lambda \end{pmatrix}, \ \lambda > 0 \text{ et } C = \begin{pmatrix} 1 & \alpha \\ \alpha & \beta \end{pmatrix}, \alpha \neq 0.$$

Pour que C soit définie positive il faut et il suffit que son déterminant et sa trace soient positifs (somme et produit des valeurs propres). Cela s'écrit

$$1 + \beta > 0 \text{ et } \beta - \alpha^2 > 0.$$

Mais cela revient à $\beta > \alpha^2$ (alors $1 + \beta > 1 + \alpha^2 > 0$).

On a donc que C est de la forme

$$C = \begin{pmatrix} 1 & \alpha \\ \alpha & \alpha^2 + \gamma \end{pmatrix}$$

avec $\gamma > 0$.

On calcule maintenant

$$AC + CA = \begin{pmatrix} 2 & \alpha(2+\lambda) \\ \alpha(2+\lambda) & 2(1+\lambda)(\alpha^2+\gamma) \end{pmatrix}.$$

Comme la trace de cette dernière matrice est positive, elle ne peut avoir deux valeurs propres négatives. Pour qu'elle ne soit pas définie positive il faut et il suffit que son déterminant soit négatif ou nul. Ce qui s'écrit

$$4(1+\lambda)(\alpha^2+\gamma) - \alpha^2(2+\lambda)^2 \leq 0.$$

Soit, en fixant λ et α

$$\gamma \leq \frac{\alpha^2\lambda^2}{4(1+\lambda)}.$$

Si on note

$$\tau = \gamma\frac{4(1+\lambda)}{\alpha^2\lambda^2} \in]0,1],$$

les matrices A et C telles que $AC + CA$ ne soit pas définie positive sont celles pour lesquelles il existe des réels $\alpha \neq 0$, $\lambda > 0$, $\tau \in]0,1]$ et $t_1, t_2 > 0$ ainsi qu'une matrice orthogonale P tels que

$$A = t_1 P^t \begin{pmatrix} 1 & 0 \\ 0 & 1+\lambda \end{pmatrix} P \text{ et } C = t_2 P^t \begin{pmatrix} 1 & \alpha \\ \alpha & \alpha^2\left(1+\tau\frac{\alpha^2\lambda^2}{4(1+\lambda)}\right) \end{pmatrix} P.$$

On peut se poser la question de l'unicité des paramètres. Étant données A et C : t_1 est la plus petite valeur propre de A, λ s'en déduit

$$\lambda = (\lambda_2 - t_1)/t_1$$

où λ_2 est la plus grande valeur propre de A. à une symétrie près P est fixée par la base de diagonalisation de A. Puis, t_2 est le coefficient $(1,1)$ de C dans cette base (il ne dépend pas du signe du déterminant de P) enfin α et τ se déduisent de manière unique du reste des coefficients de C dans cette base.

Exercice 40

Enoncé

On considère les matrices aléatoires suivantes (de taille $N \geq 2$): A est tirée en choisissant une position dans chaque colonne, on y place un 1 et tous les autres coefficients sont nuls. La matrice B est tirée avec deux éléments par colonne égaux à 1 et les autres nuls. La matrice C est tirée avec un élément hors diagonale égal à 1 par colonne. La diagonale est à 1 et tous les autres coefficients sont nuls. À chaque fois les colonnes sont tirées indépendamment. On précise que l'on tire uniformément les matrices parmi l'ensemble des matrices qui conviennent.

1) Quelle est la probabilité d'inversibilité d'une matrice A? On la note p_N.

2) Montrer que la probabilité d'inversibilité de B est plus petite que $2^N p_N$ et que cela tend vers 0 à l'infini (en N). (On rappelle la formule donnant le déterminant d'une matrice et la définition du permanent

$$\begin{array}{l} Det(A) = \sum_\sigma \epsilon(\sigma) \prod_i a_{\sigma(i)i} \\ Perm(A) = \sum_\sigma \prod_i a_{\sigma(i)i} \end{array} \tag{21}$$

où σ parcourt les permutations de taille N et $\epsilon(\sigma)$ désigne la signature d'une permutation).

3) On appelle $D(k)$ le nombre de permutations de $[\![1, k]\!]$ sans point fixe et $m(k)$ la somme de leurs signatures. Donner une formule de l'espérance du déterminant et du permanent de C faisant intervenir ces quantités.

4) Montrer qu'il existe des constantes strictement positives telles que

$$c_1\sqrt{N} \leq E[Perm(C)] \leq c_2\sqrt{N}.$$

(on admet que $k!/e - 1/2 < D(k) < k!/e + 1/2$).

Eléments de correction

1) Les matrices A inversibles sont celles dont la position des 1 forme une permutation. Il y a

$N!$ telles matrices et le nombre total de matrices possibles est N^N. On a donc

$$p_N = \frac{N!}{N^N}.$$

2) Comme le déterminant d'une matrice B inversible est un entier (non nul), il vient que $E[|\,Det(B)|] \geq P(B \text{ inversible})$. Majorons donc cette espérance.

$$E[|\,Det(B)|] = E\left[\left|\sum_\sigma \epsilon(\sigma)\prod_i b_{\sigma(i)i}\right|\right] \leq \sum_\sigma E\left[\prod_i b_{\sigma(i)i}\right] = N!\left(\frac{2}{N}\right)^N = 2^N p_N.$$

Car l'espérance d'un produit est le produit des espérances quand les variables sont indépendantes (le point important a été de fixer le σ).

La formule de Stirling permet d'avoir l'équivalence

$$N!\left(\frac{2}{N}\right)^N \sim \sqrt{2\pi}\sqrt{N}\left(\frac{2}{e}\right)^N$$

qui tend bien vers 0 en l'infini.

3) On développe les deux espérances demandées en somme portant sur σ (comme ci-dessus), et on range les σ en classes dépendant de leur ensemble de points fixes (alors σ n'a pas de points fixes sur le complémentaire: c'est un dérangement du complémentaire). Il y a $\binom{N}{k}$ choix possibles du support de dérangement (sans points fixes) et une fois le support de dérangement de taille k fixé, on a

$$E\left[\prod_i c_{\sigma(i)i}\right] = \left(\frac{1}{N-1}\right)^k.$$

Il vient

$$E\left[Perm(C)\right] = 1 + \sum_{k=1}^N \binom{N}{k} D(k)\left(\frac{1}{N-1}\right)^k$$

et

$$E\left[Det(C)\right] = 1 + \sum_{k=1}^N \binom{N}{k} m(k)\left(\frac{1}{N-1}\right)^k. \tag{22}$$

(On a singularisé le 1 au début des deux formules, il provient de $\sigma = Id$. Noter que $m(1) = D(1) = 0$ car il n'y a pas de dérangement de taille 1.)

4) Au vu de l'encadrement demandé, on remarque que l'on peut soustraire une constante (un nombre fini de fois pendant le calcul) sans changer l'encadrement. Par exemple, on peut ajouter 1 ou retrancher 1 à $D(k)$ et cela ne change la somme que de plus ou moins

$$\sum_k \binom{N}{k} \left(\frac{1}{N-1}\right)^k \leq (1+\frac{1}{N-1})^N$$

qui tend vers e.

On remplace donc $D(k)$ par $k!/e$. Quitte à retrancher le 1 au début et à multiplier par e qui ne change que les constantes c_1 et c_2, on s'intéresse à la quantité

$$\sum_{k=1}^{N} k! \binom{N}{k} \left(\frac{1}{N-1}\right)^k = \sum_{k=1}^{N} \prod_{m=0}^{k-1} \frac{N-m}{N-1} = \frac{N}{N-1} \sum_{l=0}^{N-1} \prod_{m=0}^{l-1} \frac{N-1-m}{N-1}.$$

Le terme $N/(N-1)$ ne changera rien à l'encadrement ni le terme en $l=0$ et on note

$$\alpha_l^N = \prod_{m=0}^{l-1} \frac{N-1-m}{N-1}.$$

On peut montrer que les termes avec $l > (N-1)/10$ seront négligeables. On procède ainsi:

$\alpha_l^N \leq \left(\frac{9}{10}\right)^{l-N/10}$ (les premiers facteurs pour $m < (N-1)/10$ sont majorés par 1, et les autres par $9/10$ et on met à la bonne puissance). La somme de tous ces termes α_l^N pour l allant de $(N-1)/10$ jusqu'à l'infini serait ainsi plus petite que 10.

Il nous reste la somme suivante:

$$\sum_{l=0}^{l \leq N/10} \alpha_l^N.$$

La convexité du logarithme implique que pout tout x entre 0 et $1/10$ on a

$$-cx \leq \ln(1-x) \leq -x$$

où c est la pente de la corde joignant les points $(9/10, \ln(9/10))$ et $(1,0)$. On en déduit que (on prenant le log des α_l^N) que

$$-c\frac{l(l-1)}{2(N-1)} \leq \ln(\alpha_l^N) \leq -\frac{l(l-1)}{2(N-1)}.$$

Soit
$$e^{-c\frac{l(l-1)}{2(N-1)}} \leq \alpha_l^N \leq e^{-\frac{l(l-1)}{2(N-1)}}$$

par ailleurs on constate que la quantité
$$\frac{e^{-\frac{x^2}{N-1}}}{e^{-\frac{x(x-1)}{N-1}}} = e^{-\frac{x}{N-1}}$$

est encadrée par des constantes lorsque $x \leq (N-1)/10$ (1 et $e^{-9/10}$) (on fait de même avec $e^{-c\cdots}$). Soit
$$C_0 e^{-c\frac{l^2}{2(N-1)}} \leq \alpha_l^N \leq C_1 e^{-\frac{l^2}{2(N-1)}}.$$

Maintenant on utilise une comparaison série intégrale pour se ramener à
$$C_0 \int_0^{(N-1)/10} e^{-c\frac{x^2}{2(N-1)}} dx \leq \sum_{l=0}^{(N-1)/10} \alpha_l^N \leq 1 + C_1 \int_0^{(N-1)/10} e^{-\frac{x^2}{2(N-1)}} dx$$

(le 1+ à droite correspond au terme α_0^N).

Par un changement de variable $x/\sqrt{N-1}$, les deux termes d'encadrement sont équivalents à $\sqrt{N-1}$ (fois $\int_0^{\sqrt{N-1}/10} e^{-c'u^2/2} du$ qui tend vers une limite). Ceci démontre le résultat.

Exercice 41

Enoncé

Pour toute fonction $f : \mathbb{N}_{\geq 1} \to \mathbb{R}$, on considère sa fonction moyenne
$$Mf : \mathbb{N}_{\geq 1} \to \mathbb{R}$$

définie par
$$Mf(n) = \frac{1}{n} \sum_{k=1}^{n} f(k).$$

Montrer que pour tout $n \geq 1$, on a
$$(M^m f)(n) \to f(1) \quad \text{quand} \quad m \to +\infty.$$

Eléments de correction

On peut se restreindre aux fonctions $[1, n] \to \mathbb{R}$, pour chaque n. Dans la base $\delta_1, \cdots, \delta_n$ des masses de Dirac (qui ne sont non nulles qu'en un point et valent 1 en ce point), la matrice de M est une matrice triangulaire inférieure dont la diagonale est $(1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{n})$. En particulier:

(1) elle est diagonalisable,

(2) l'espace propre associé à la valeur propre 1 est $\mathbb{R}\delta'_1$ où $\delta'_1 = 1$ (fonction constante),

(3) les autres droites propres $\mathbb{R}\delta'_2, \cdots, \mathbb{R}\delta'_n$ sont dans $\mathrm{Vect}(\delta_2, \cdots, \delta_n)$, avec des valeurs propres de valeur (absolue) < 1.

Il en résulte immédiatement que si

$$f = \sum_k f(k)\delta_k = \sum_k f'(k)\delta'_k,$$

avec $f'(1) = f(1)$, on a $M^m f \to f(1)\delta'_1$. D'où le résultat.