CB2 — Epreuve spécifique "MP" de Mathématiques — 2 Juin 2018

La clarté des raisonnements, la précision de la rédaction et la présentation entreront pour une part non négligeable dans l'appréciation des copies.

Les résultats non justifiés ou non encadrés ne seront pas pris en compte.

L'utilisation de tout document, de toute calculatrice et de tout matériel électronique est interdite.

Problème 1 — Une application des polynômes de Bernstein : le théorème de Stone-Weierstraß

Problématique. *L'objectif de ce problème est de prouver que toute fonction continue sur un segment peut être approchée arbitrairement près par une fonction polynomiale, sous réserve que cette fonction polynomiale soit de degré suffisamment grand (c'est le théorème de Stone-Weierstraß).*

Cette approximation d'une fonction continue se fait essentiellement par une suite de polynômes, construite à l'aide des polynômes de Bernstein, que vous avez étudiés hier.

Concrètement, la partie I consiste à établir quelques résultats qui pourront intervenir au cours de la seconde partie.

La partie II est le cœur du problème : on y établit le résultat de Stone-Weierstraß, par des arguments reposant sur le cours d'Analyse, et celui de Probabilités.

Partie I — Questions préliminaires

Les questions de cette partie sont indépendantes.

1. Soit f une fonction continue sur $[0,1]$ et à valeurs dans $\mathbb{R}$. Justifier qu'il existe un réel positif M tel que : $\forall\, x \in [0,1],\ |f(x)| \leqslant M$.

2. Etablir que : $\forall\, x \in [0,1]\,, \quad 0 \leqslant x\,(1-x) \leqslant \dfrac{1}{4}$.

3. Soient $x \in [0,1]$ et $n \in \mathbb{N}^*$. On considère une variable aléatoire X qui suit la loi binomiale de taille n et de paramètre x, et on pose : $Y = \dfrac{1}{n}\,X$.

Rappeler sans justification les valeurs de l'espérance $\mathrm{E}\,(X)$ et de la variance $\mathrm{Var}\,(X)$. Puis préciser les valeurs de $\mathrm{E}\,(Y)$ et de $\mathrm{Var}\,(Y)$.

Partie II — Théorème de Stone-Weierstraß

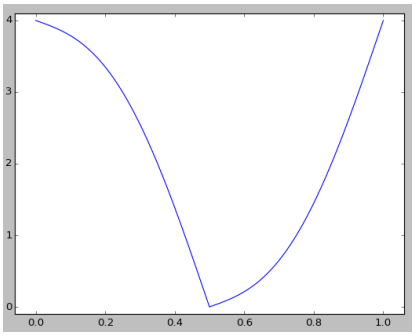
Soit f une fonction continue sur $[0,1]$ et à valeurs dans $\mathbb{R}$. On note M un majorant de $|f|$ sur $[0,1]$.*

Pour tout entier naturel n non nul et pour tout réel $x \in [0,1]$, on pose :

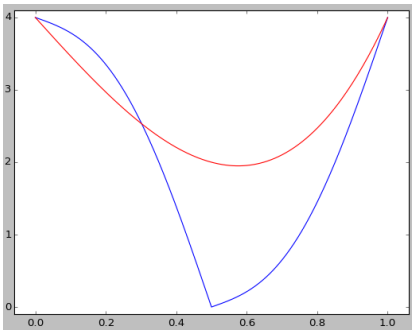
$$B_{f,n}(x) = \sum_{k=0}^{n} \binom{n}{k} x^k (1-x)^{n-k} f\left(\frac{k}{n}\right)$$

On définit de la sorte une fonction polynomiale $B_{f,n}$ sur $[0,1]$ (c'est le n-ième polynôme de Bernstein associé à f).

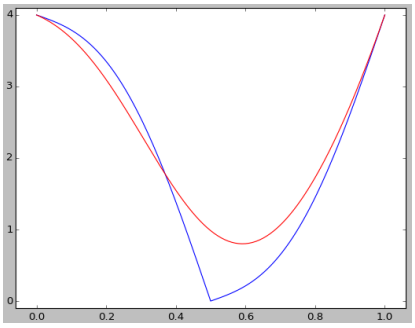
On veut prouver que pour tout réel x dans $[0,1]$, $B_{f,n}(x)$ converge vers $f(x)$ lorsque n tend vers $+\infty$; cette affirmation est illustrée par les figures ci-dessous, dans lesquelles on a fait apparaître les courbes représentatives d'une fonction f continue sur $[0,1]$, et des fonctions polynomiales $B_{f,n}$ pour $n = 3$, 10 et 30.



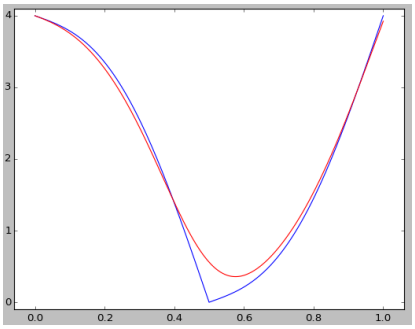
Courbe représentative de f



Représentations de f et de $B_{f,3}$



Représentations de f et de $B_{f,10}$



Représentations de f et de $B_{f,30}$

A cette fin, on choisit un réel $x \in [0,1]$ et un réel strictement positif ε, qui sont donc fixés tout au long de cette partie.

Et on se propose d'établir que :

$$\boxed{\exists\, n_0 \in \mathbb{N},\ [n \geqslant n_0] \Longrightarrow [|f(x) - B_{f,n}(x)| < \varepsilon]}$$

*. L'existence d'un tel réel M est assurée par la question 1.

4. Justifier qu'il existe un réel $\alpha > 0$ tel que :

$$\forall\ (u,v) \in\ [0,1]^2\,,\ [|v-u| < \alpha] \Longrightarrow \left[|f(v)-f(u)| < \frac{\varepsilon}{2}\right]$$

5. Etablir que :

$$|f(x) - B_{f,n}(x)| \leqslant \sum_{k=0}^{n} \binom{n}{k} x^k\,(1-x)^{n-k} \left|f(x) - f\left(\frac{k}{n}\right)\right|$$

6. On note $E = \left\{k \in [\![\ 0,n\ ]\!],\ \left|x - \frac{k}{n}\right| < \alpha\right\}$, $\overline{E} = [\![\ 0,n\ ]\!] \setminus E$ et $\Delta_n(x) = f(x) - B_{f,n}(x)$.

Montrer que :

$$|\Delta_n(x)| \leqslant \frac{\varepsilon}{2} + 2M \sum_{k\in\overline{E}} \binom{n}{k} x^k\,(1-x)^{n-k}$$

7. Soit X une variable aléatoire suivant la loi binomiale de taille n et de paramètre x.

Etablir que :

$$P\left(\left|\frac{X}{n} - x\right| \geqslant \alpha\right) = \sum_{k\in\overline{E}} \binom{n}{k} x^k\,(1-x)^{n-k}$$

8. En déduire que :

$$\sum_{k\in\overline{E}} \binom{n}{k} x^k\,(1-x)^{n-k} \leqslant \frac{x(1-x)}{n\alpha^2}$$

9. Déduire de ce qui précède que :

$$|\Delta_n(x)| \leqslant \frac{\varepsilon}{2} + \frac{M}{2n\alpha^2}$$

10. En déduire que pour n suffisamment grand on a : $|\Delta_n(x)| \leqslant \varepsilon$. Conclure.

Problème 2 — Entiers sommes de deux carrés

Problématique. *L'objectif de ce problème est de décrire l'ensemble des entiers naturels s'écrivant comme somme de deux carrés. Cette description passe par l'étude de l'anneau des entiers de Gauss, qui possède beaucoup de points communs avec l'anneau des entiers relatifs.*

Notations : tout au long du problème, on notera $\mathbb{Z}[\mathrm{i}]$ l'anneau des **entiers de Gauss**, c'est-à-dire l'anneau des nombres complexes à parties réelle et imaginaire entières. Explicitement :

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

Par ailleurs, on définit une "norme"[†] sur $\mathbb{C}$, l'application $\left[\begin{array}{c} N : \mathbb{C} \longrightarrow \mathbb{R}_+ \\ z \longmapsto z\overline{z} \end{array}\right]$

Partie I — Quelques propriétés de l'anneau des entiers de Gauss

1. **Description des inversibles de $\mathbb{Z}[\mathrm{i}]$**. Un entier de Gauss u est **inversible** s'il existe $v \in \mathbb{Z}[\mathrm{i}]$ tel que : $uv = 1$.

   a. Soient u et v deux éléments de $\mathbb{Z}[\mathrm{i}]$. Montrer que : $N(uv) = N(u)\,N(v)$, et justifier brièvement que pour tout $u \in \mathbb{Z}[\mathrm{i}]$, $N(u) \in \mathbb{N}$.

   b. Etablir que : $[u \text{ est inversible dans } \mathbb{Z}[\mathrm{i}]\,] \iff [N(u) = 1]$.

   c. Donner en extension l'ensemble des éléments inversibles de $\mathbb{Z}[\mathrm{i}]$.

2. **Divisibilité dans $\mathbb{Z}[\mathrm{i}]$**. Soient u et v deux éléments de $\mathbb{Z}[\mathrm{i}]$. On dit que u **divise** v dans $\mathbb{Z}[\mathrm{i}]$ s'il existe $s \in \mathbb{Z}[\mathrm{i}]$ tel que : $v = us$. Lorsque c'est le cas, on le note : $u|v$.

   Montrer que si $u|v$ dans $\mathbb{Z}[\mathrm{i}]$, alors $N(u)\,|N(v)$ dans $\mathbb{Z}$.

3. **Division euclidienne dans $\mathbb{Z}[\mathrm{i}]$**.

   a. Montrer que pour tout $z \in \mathbb{C}$, il existe $u \in \mathbb{Z}[\mathrm{i}]$ tel que $N(u - z) < 1$. Ce u est-il unique ?[‡]

   b. Montrer que pour tout $u \in \mathbb{Z}[\mathrm{i}]$ et pour tout $v \in \mathbb{Z}[\mathrm{i}]^*$, il existe $(q,r) \in \mathbb{Z}[\mathrm{i}] \times \mathbb{Z}[\mathrm{i}]$ tel que $u = vq + r$ avec $N(r) < N(v)$.

Partie II — PGCD dans l'anneau des entiers de Gauss

Soient u et v dans $\mathbb{Z}[\mathrm{i}]$. On note $I(u,v) = \{uz + vz' \,/\, z \text{ et } z' \in \mathbb{Z}[\mathrm{i}]\}$.[§]

4. On suppose $(u,v) \neq (0,0)$. Montrer que l'ensemble $A = \{N(w) \,/\, w \in I(u,v) \setminus \{0\}\}$ possède un plus petit élément $d > 0$.

5. Soit δ un élément de $I(u,v)$ tel que $N(\delta) = d$. Etablir que : $I(u,v) = \delta\mathbb{Z}[\mathrm{i}]$.
   *On pourra utiliser la division euclidienne présentée en **3.b**.*

†. Attention : ce n'est pas la norme usuelle que vous connaissez, puisque pour tout complexe z, on a : $N(z) = |z|^2$.
‡. Une figure claire pourra constituer une réponse à cette question.
§. Ou ce qui revient au même : $I(u,v) = u\mathbb{Z}[\mathrm{i}] + v\mathbb{Z}[\mathrm{i}]$.

6. Montrer que $\delta|u$ et $\delta|v$. Puis établir l'équivalence : $\forall\, w \in \mathbb{Z}[\mathrm{i}]\,,\ [w|u \wedge w|v] \iff [w|\delta]$

➤ **Terminologie** : dans cette situation, on dit que δ est **un pgcd** de u et v (dans $\mathbb{Z}[\mathrm{i}]$).

Partie III — Entiers de Gauss premiers entre eux

Soient u et v dans $\mathbb{Z}[\mathrm{i}]$, avec $u \neq 0$ ou $v \neq 0$.

On dit que u et v sont **premiers entre eux** si le nombre δ défini dans la partie précédente appartient à $\{\pm 1; \pm \mathrm{i}\}$. Il revient au même de dire que les seuls diviseurs communs à u et v sont les entiers de Gauss de module 1.

Dans les deux questions ci-dessous, on suppose que u et v sont deux entiers de Gauss premiers entre eux.

7. Justifier qu'il existe deux entiers de Gauss z et z' tels que : $1 = uz + vz'$.

8. Soit $w \in \mathbb{Z}[\mathrm{i}]$. Montrer que si $u|vw$, alors $u|w$.

Partie IV — Entiers de Gauss irréductibles

Soit $u \in \mathbb{Z}[\mathrm{i}] \setminus \{0; \pm 1; \pm \mathrm{i}\}$.

On dit que u est **irréductible** si ses seuls diviseurs dans $\mathbb{Z}[\mathrm{i}]$ sont ± 1, $\pm \mathrm{i}$, $\pm u$ et $\pm \mathrm{i}u$. ¶

9. Soit $v \in \mathbb{Z}[\mathrm{i}]$. On suppose que u est irréductible et ne divise pas v. Montrer que u et v sont premiers entre eux.

10. Soient v et $w \in \mathbb{Z}[\mathrm{i}]$. On suppose que u est irréductible et divise vw. Montrer que $u|v$ ou $u|w$.

Partie V — Entiers sommes de deux carrés

On note $S = \{a^2 + b^2 \,/\, (a,b) \in \mathbb{Z}^2\}$. L'ensemble S est donc l'ensemble des entiers (naturels) s'écrivant comme sommes de deux carrés. L'objet de cette partie est de donner une description de S.

11. Soit $n \in \mathbb{N}$. Montrer que : $[n \in S] \iff [\exists\, u \in \mathbb{Z}[\mathrm{i}]\,,\ N(u) = n]$.

12. En déduire que S est stable par produit, càd : $\forall\ (n,n') \in S^2,\ nn' \in S$.

13. Soit p un nombre premier impair.

a. Montrer que : $[p \in S] \Longrightarrow [p \equiv 1\,[4]]$.

Dans la suite du problème, on admettra que la réciproque de cette propriété est vraie.

b. Montrer que si p n'est pas irréductible, alors $p \in S$.

14. Soient a et b deux entiers, et $n = a^2 + b^2 \in S$. Soit p un nombre premier diviseur de n, avec $p \equiv 3\,[4]$.

a. Montrer que p divise $a + \mathrm{i}\,b$ (dans $\mathbb{Z}[\mathrm{i}]$).

b. En déduire que p^2 divise n dans $\mathbb{Z}$.

15. Montrer que les entiers n supérieurs ou égaux à 2 appartenant à S sont ceux dont la décomposition en facteurs premiers est de la forme : $n = \prod_{i=1}^{m} p_i^{\alpha_i}$, où les p_i sont des nombres premiers deux à deux distincts, et où les α_i sont des entiers naturels tels que : $[p_i \equiv 3\,[4]] \Longrightarrow [\alpha_i \text{ pair}]$.

¶. La notion d'entier de Gauss irréductible étend à $\mathbb{Z}[\mathrm{i}]$ celle de nombre premier dans $\mathbb{Z}$.