Devoir surveillé n° 1 – sujet B
MP
samedi 12 septembre 2026

Ce sujet est composé de deux problèmes indépendants. Il n'est pas nécessaire de les traiter dans l'ordre, mais les questions doivent être clairement numérotées.
Si une question n'est pas résolue, il est possible d'en admettre le résultat, que l'on veillera à correctement citer lorsqu'on l'utilisera. La clarté de la rédaction et la précision des raisonnements font partie intégrante de l'évaluation d'une copie.
On veillera notamment à encadrer soigneusement tous les résultats demandés.
Les calculatrices sont interdites.

Problème

Le problème suivant traite des racines d'un polynôme à coefficients réels ou complexes. Les différentes parties sont indépendantes entre elles.

I Autour des racines d'un polynôme

I.1 Localisation des racines par la matrice compagnon

Soit $P \in \mathbb{C}_n[X]$ un polynôme unitaire de degré n, noté

$$P = a_0 + a_1 X + \cdots + a_{n-1}X^{n-1} + X^n$$

On définit la **matrice compagnon** de P comme la matrice $C_P \in \mathcal{M}_n(\mathbb{C})$ égale à

$$C_P = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Soit $A = (a_{i,j})_{i,j\in[\![1,n]\!]}$ une matrice de $\mathcal{M}_n(\mathbb{C})$; on pose, pour tout entier $1 \leqslant i \leqslant n$:

$$r_i = \sum_{j=1}^{n} |a_{i,j}| \quad \text{et} \quad \mathcal{D}_i = \{z \in \mathbb{C} \mid |z| \leqslant r_i\}$$

Pour tout $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathcal{M}_{n,1}(\mathbb{C})$, on note

$$\|X\|_\infty = \max_{1\leqslant i\leqslant n} |x_i|$$

Q1. Soit $\lambda \in \mathrm{Sp}(A)$ et $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ un vecteur propre associé à λ. Montrer que, pour tout entier $1 \leqslant i \leqslant n$, on a $|\lambda x_i| \leqslant r_i \|X\|_\infty$.

Q2. Montrer que $\mathrm{Sp}(A) \subset \bigcup_{i=1}^{n} \mathcal{D}_i$.

Q3. Calculer le polynôme caractéristique de la matrice C_P, montrer qu'il est égal à P.

Q4. Montrer que les racines de P sont toutes dans le disque $\mathcal{D}_R = \{z \in \mathbb{C} \mid |z| \leqslant R\}$, où

$$R = \max\{|a_0|, 1 + |a_1|, 1 + |a_2|, \ldots, 1 + |a_{n-1}|\}$$

I.2 Le théorème d'Eneström-Kakeya

Soit $n \geqslant 2$. Soient $a_0, a_1, \ldots, a_n$ des réels vérifiant

$$0 < a_n \leqslant a_{n-1} \leqslant \cdots \leqslant a_2 \leqslant a_1 \leqslant a_0.$$

On définit le polynôme $P \in \mathbb{R}[X]$ par

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

Le but des questions **Q5** à **Q7** est de montrer que les racines (complexes) du polynôme P sont à l'extérieur du disque unité ouvert, c'est-à-dire de module supérieur ou égal à 1.

Q5. Montrer que, pour tous complexes $z, w \in \mathbb{C}$, on a

$$|z - w| \geqslant ||z| - |w||$$

Q6. Montrer que, pour tout $z \in \mathbb{C}$,

$$|(1 - z)P(z)| \geqslant a_0 - \Big[(a_0 - a_1)|z| + (a_1 - a_2)|z|^2 + \cdots + (a_{n-1} - a_n)|z|^n + a_n|z|^{n+1}\Big]$$

Q7. En déduire que si $|z| < 1$, alors $|(1 - z)P(z)| > 0$.

Q8. En déduire le **théorème d'Eneström-Kakeya** : si z est racine de P, alors $|z| \geqslant 1$.

On désire montrer maintenant le résultat suivant.
Soient $b_0, b_1, \ldots, b_n$ des réels strictement positifs. On définit le polynôme

$$Q = b_0 + b_1 X + b_2 X^2 + \cdots + b_n X^n = \sum_{k=0}^{n} b_k X^k.$$

Si l'on pose

$$r = \min_{k \in [\![0, n-1]\!]} \left(\frac{b_k}{b_{k+1}}\right) \quad \text{et} \quad R = \max_{k \in [\![0, n-1]\!]} \left(\frac{b_k}{b_{k+1}}\right)$$

alors les racines de Q sont situées dans la couronne

$$\mathcal{C} = \{z \in \mathbb{C} \mid r \leqslant |z| \leqslant R\}$$

Soit z une racine de Q.

Q9. En utilisant le polynôme

$$P^*(X) = Q(rX) = \sum_{k=0}^{n} b_k r^k X^k$$

et le théorème d'Eneström-Kakeya, montrer que $|z| \geqslant r$.

Q10. On définit $I(X)$ par

$$I(X) = X^n Q\left(\frac{1}{X}\right)$$

Justifier que I est un polynôme. À l'aide du polynôme

$$P^*(X) = I\left(\frac{X}{R}\right)$$

montrer que $|z| \leqslant R$.

I.3 Racines réelles d'un polynôme aléatoire

Dans cette partie, on se donne un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$, un entier $n \geqslant 2$ (que l'on fera varier), un réel $p \in [0,1]$ et des variables aléatoires A_n, B_n, C_n, mutuellement indépendantes, suivant la même loi binomiale $\mathcal{B}(n,p)$.
On note T_n le polynôme aléatoire

$$T_n = A_n X^2 + B_n X + C_n$$

(c'est-à-dire que, pour tout $\omega \in \Omega$, $T_n(\omega)$ est le polynôme $A_n(\omega)X^2 + B_n(\omega)X + C_n(\omega)$).
On prendra bien garde que le symbole X désigne l'indéterminée des polynômes, et non une variable aléatoire.
On définit sur $\mathbb{R}$ la fonction G_n par

$$\forall t \in \mathbb{R}, \quad G_n(t) = \sum_{k=0}^{n} \mathbb{P}(A_n = k) t^k$$

Q11. Calculer $G_n(t)$ pour tout $t \in \mathbb{R}$.

Q12. Calculer la dérivée k-ième en 1 de G_n : $G_n^{(k)}(1)$.

Q13. Exprimer $\mathbb{E}(A_n), \mathbb{E}(A_n(A_n-1)), \mathbb{E}(A_n(A_n-1)(A_n-2))$ et $\mathbb{E}(A_n(A_n-1)(A_n-2)(A_n-3))$ en fonction de G_n et de ses dérivées. On justifiera brièvement que toutes les variables aléatoires mises en jeu admettent une espérance finie.

Q14. Montrer qu'il existe des réels $\alpha, \beta, \gamma, \delta, \varepsilon$ tels que

$$\forall k \in \mathbb{N}, \quad k^4 = \alpha k(k-1)(k-2)(k-3) + \beta k(k-1)(k-2) + \gamma k(k-1) + \delta k + \varepsilon$$

et donner la valeur de α.

Q15. Montrer que $\mathbb{E}(B_n^4) = n^4 p^4 + o(n^4)$ lorsque $n \to +\infty$.

Q16. On note Δ_n le discriminant de T_n. Calculer $\mathbb{E}(\Delta_n)$, ainsi que sa limite lorsque $n \to +\infty$.

Q17. Montrer que $\mathbb{V}(B_n^2) = o(n^4)$ lorsque $n \to +\infty$.

Q18. Montrer que $\mathbb{P}(\Delta_n \geqslant 0) \xrightarrow[n\to+\infty]{} 0$.
Indication : On pourra utiliser l'inégalité de Bienaymé-Tchebychev.
Qu'a-t-on montré quant à l'existence de racines réelles de T_n ?

I.4 Une preuve du théorème de d'Alembert

Le but de cette partie est de démontrer le théorème de d'Alembert :

Tout polynôme non constant de $\mathbb{C}[X]$ admet au moins une racine dans $\mathbb{C}$

Soit $P \in \mathbb{C}[X]$ un polynôme de degré $n \geqslant 1$. Quitte à le diviser par son coefficient dominant, on le supposera **unitaire**. On procède par l'absurde, en supposant que P ne s'annule pas sur $\mathbb{C}$.

Q19. Donner un équivalent simple de $|P(z)|$ lorsque $|z| \to +\infty$.

Q20. En déduire que la fonction $z \mapsto 1/|P(z)|$ est bornée sur $\mathbb{C}$.
Dans la suite, on notera M un majorant sur $\mathbb{C}$ de $1/|P|$.

Q21. On définit la fonction

$$h : [0, +\infty[\times [0, 2\pi] \to \mathbb{C}, \quad (r,t) \mapsto \frac{1}{P(re^{\mathrm{i}t})}$$

et on pose, pour tout $r \geqslant 0$:

$$f(r) = \int_0^{2\pi} h(r,t)\,\mathrm{d}t = \int_0^{2\pi} \frac{1}{P(re^{\mathrm{i}t})}\,\mathrm{d}t$$

Montrer que f est définie et continue sur $\mathbb{R}^+$.

Q22. Déterminer $f(0)$ et $\lim\limits_{r\to+\infty} f(r)$.

Q23. Montrer que f est de classe $\mathcal{C}^1$ sur $\mathbb{R}^+$.
Indication : On pourra montrer que f est de classe $\mathcal{C}^1$ sur tout segment $[0,R]$ de $\mathbb{R}^+$.

Q24. Montrer qu'il existe un complexe α à déterminer tel que, sur $\mathbb{R}^+ \times \mathbb{R}$, on ait l'égalité :

$$\alpha r \frac{\partial h}{\partial r} = \frac{\partial h}{\partial t}$$

Q25. En déduire $f'(r) = 0$ pour tout $r > 0$.

Q26. Conclure.

Exercice

Le domaine de la cryptographie requiert l'utilisation de très grands nombres premiers, dont l'écriture décimale comporte plusieurs centaines de chiffres. Un double problème mathématique et informatique se pose : comment vérifier si un entier donné est un nombre premier, et comment fabriquer un grand nombre premier ?
On rappelle qu'un entier positif n est dit **premier** s'il n'est divisible par aucun entier positif autre que 1 et lui-même. On dit qu'il est **composé** dans le cas contraire.
Exemple : 17 est premier, tandis que $42 = 2 \cdot 3 \cdot 7$ est composé.
On remarquera que, si n est divisible par un entier d tel que $1 < d < n$, c'est-à-dire si on peut l'écrire sous la forme $n = d \cdot q$, alors q est également un diviseur de n, et l'un des deux entiers d ou q au moins est inférieur ou égal à $\sqrt{n}$.

Aucune autre connaissance des nombres premiers n'est utilisée dans ce problème.

Du point de vue informatique, on rappelle que $a\%b$ renvoie le reste de la division euclidienne de a par b. Notamment, a est divisible par b si et seulement si $a\%b$ est égal à 0.
Remarque : un appendice, situé à la fin du problème, récapitule quelques fonctions du langage Python.

1. Soit N un entier, $N \geqslant 2$. Expliquer ce que fait la fonction suivante.

```
def test_naif(N):
    borne = ceil(sqrt(N))
    for k in range(2, borne + 1):
        if N % k == 0:
            return False
    return True
```

2. Si N est un entier premier de l'ordre de 10^{400}, donner un *ordre de grandeur* du temps d'exécution de `test_naif(N)`. On utilisera une unité de temps adaptée (seconde, heure, mois, année...).

3. Tout nombre entier peut se diviser un certain nombre de fois par 2, jusqu'à ce que l'on obtienne un entier impair. Par exemple,

$$168 = 2 \cdot 84 = 2^2 \cdot 42 = 2^3 \cdot 21$$

le nombre 21 étant impair et donc non divisible par 2.
Écrire une fonction `q_m(n)` prenant en entrée un entier n et renvoyant l'unique couple (q, m) tel que : q est impair et $n - 1 = 2^m q$.

Nous étudions ici une méthode permettant, d'une part, de déterminer si un nombre donné est premier ; et d'autre part, de trouver un grand nombre premier.
Plus précisément, la méthode que nous allons mettre en œuvre est basée sur le théorème de Miller qui permet dans certains cas d'affirmer qu'un entier donné $n \geqslant 1$ est **composé**, c'est-à-dire non premier.
Voici ce théorème, que nous admettons :

THÉORÈME 1 (Miller)

Soit $n \geqslant 3$ un entier impair, que l'on décompose sous la forme $n - 1 = 2^m \cdot q$ avec q impair.
S'il existe un entier $1 < a < n$ tel que

$$\begin{cases} n \text{ ne divise pas } a^q - 1 \\ n \text{ ne divise pas } a^{2^i q} + 1, \text{ pour } i = 0, \dots, m-1 \end{cases}$$

alors n est composé.

Un entier $a \in [\![2, n-1]\!]$ vérifiant les relations (1) est appelé un **témoin de Miller** pour n. L'existence d'un tel témoin permet donc d'affirmer que n est composé.

4. Écrire une fonction `Temoin_Miller(a, n)` déterminant si un entier a est un témoin de Miller de n.

Jusqu'à là, la méthode des témoins de Miller ne peut servir qu'à prouver qu'un entier est composé. Or, un second théorème stipule que si n est composé, non seulement il existe des témoins de Miller, mais qu'il en existe beaucoup :

THÉORÈME 2 (Rabin, 1976)

Si n est composé, alors au moins les trois quarts des entiers $1 < a < n$ sont des témoins de Miller de n.

Le principe de la méthode de Miller-Rabin est alors le suivant : on tire au hasard des entiers $a_1, a_2, \dots, a_k$ dans l'intervalle $[\![2, n-1]\!]$. Si l'entier n est composé, il est très probable qu'on finisse par trouver un témoin.

5. Si n est composé, majorer la probabilité $p(k)$ que, en tirant k entiers de $[\![2, n-1]\!]$, indépendamment et selon une loi uniforme, aucun de ces nombres ne soit un témoin de Miller.
6. En déduire une fonction `Miller_Rabin(n, r)` déterminant si n est premier, avec un risque égal au plus à $r \in [0, 1[$.
   Par exemple, si n est composé, l'instruction `Miller_Rabin(n, r)` renverra `True` dans une proportion inférieure à r des cas, et si n est premier, alors cette même instruction renverra `True` dans tous les cas.

Appendice : quelques fonctions Python

Pour toute la partie probabiliste du problème, on utilisera la bibliothèque `random` de la librairie `numpy` :

```
1 import numpy.random as rd
```

On a alors accès aux instructions suivantes :

Instruction	Valeur retournée
`ceil(x)`	$\lceil x \rceil$, partie entière supérieure de x : unique entier k tel que $k-1 < x \leqslant k$
`log(x)`	logarithme népérien de x ($\ln x$)
`sqrt(x)`	racine carrée de x ($\sqrt{x}$)
`a % b`	reste de la division euclidienne de a par b
`a // b`	quotient de la division euclidienne de a par b
`rd.random()`	un réel (flottant) de $[0, 1[$, avec probabilité uniforme
`rd.randint(a, b)`	un entier de $\{a, a+1, \dots, b-1\}$, avec probabilité uniforme