DS10

Devoir surveillé du 09/06/2026

Durée : 3h

La qualité de la rédaction, la clarté et la précision des raisonnements interviendront pour une part importante dans l'appréciation des copies. Les résultats doivent être encadrés.
La calculatrice n'est pas autorisée.

Exercice 1 (Marche aléatoire sur $\mathbb{Z}$)

Soit $n \in \mathbb{N}^*$, $k \in [\![0, n]\!]$ et $p \in]0, 1[$. On considère un mobile qui se déplace sur l'axe des réels. On note S_k la position du mobile à l'instant $t = k$ et on pose $X_k = S_k - S_{k-1}$ pour $k \in [\![1, n]\!]$. On fait les hypothèses suivantes :

- $S_0 = 0$ (position initiale du mobile en 0) ;
- pour tout $k \in [\![1, n]\!]$, entre l'instant $t = k-1$ et l'instant $t = k$, le mobile se déplace d'une unité vers la droite avec une probabilité p ou d'une unité vers la gauche avec une probabilité $q = 1-p$;
- les déplacements du mobile entre les différents instants se font indépendamment les uns des autres.

On suppose que les variables aléatoires $S_0, \dots, S_n$ sont définies sur un même espace probabilisé $(\Omega, \mathscr{P}(\Omega), P)$ fini.

1. Vérifier que $S_n = \sum_{k=1}^{n} X_k$ avec $X_1, \dots, X_n$ des variables aléatoires indépendantes.

2. Soit $k \in [\![1, n]\!]$. On pose $X'_k = \dfrac{(1 + X_k)}{2}$ et $U_n = \sum_{k=1}^{n} X'_k$.
   (a) Déterminer la loi de X_k et en déduire la valeur de $E(X_k)$ et de $E(S_n)$.
   (b) Vérifier que X'_k suit une loi de Bernoulli de paramètre p et en déduire $E(X'_k)$ et $V(X'_k)$.
   (c) Retrouver l'expression de $E(X_k)$ et déterminer $V(X_k)$ en fonction de p.
   (d) Justifier que $S_n = 2U_n - n$ et vérifier que U_n suit la loi binomiale $\mathscr{B}(n, p)$.
   (e) En déduire que $E(S_n) = n(2p-1)$ et que $V(S_n) = 4npq$.
   (f) Déterminer à quelle condition sur p la variable aléatoire S_n est centrée et vérifier dans ce cas que $\dfrac{S_n}{\sqrt{n}}$ est une variable aléatoire centrée réduite.

3. (a) Montrer que pour $(m, n) \in \mathbb{N}^2$, $\mathrm{Cov}(S_m, S_n) = 4pq \cdot \min(m, n)$. Le signe de cette covariance est-il prévisible ?
   (b) Pour quels couples $(m, n) \in \mathbb{N}^2$ peut-on dire que S_m et S_n sont indépendantes ?

4. (a) Déterminer $S_n(\Omega)$ en fonction de n et en déduire la valeur de $P(S_n = 0)$ lorsque n est impair.
   (b) Montrer que si n est un entier pair de la forme $n = 2N$, alors $P(S_n = 0) = \binom{2N}{N} (pq)^N$.
   (c) Montrer à l'aide de la formule de Stirling que $P(S_{2N} = 0) \sim \dfrac{(4pq)^N}{\sqrt{\pi N}}$ quand N tend vers $+\infty$.
   (d) Montrer que $4pq \leq 1$ avec égalité si, et seulement si, $p = 1/2$. En déduire que :

$$\lim_{N \to +\infty} (P(S_{2N} = 0)) = 0.$$

5. Dans toute cette question, on suppose que $N \in \mathbb{N}^*$, que $t \in]0,1]$, que $p > 1/2$. On pose $f(t) = p^2 t + 2pq + q^2/t$.

   (a) Montrer que $E\left(t^{U_{2N}}\right) = (pt+q)^{2N}$ et que $P(S_{2N} \leq 0) = P\left(t^{U_{2N}} \geq t^N\right) \leq (f(t))^N$.

   (b) Étudier les variations de f sur $]0,1]$ et en déduire qu'il existe $t_0 \in]0,1]$ tel que $0 \leq f(t_0) < 1$.

   (c) En déduire que $\lim\limits_{N\to+\infty} P(S_{2N} \leq 0) = 0$, puis que $\lim\limits_{N\to+\infty} P(S_{2N} \geq 0) = 1$.

6. Dans toute cette question, on suppose que $N \in \mathbb{N}^*$ et que $p = 1/2$.

   (a) Montrer que $P(S_{2N} > 0) = \dfrac{1}{4^N} \displaystyle\sum_{k=N+1}^{2N} \binom{2N}{k} = \frac{1}{4^N} \sum_{k=0}^{N-1} \binom{2N}{k} = P(S_{2N} < 0)$.

   (b) En déduire que $P(S_{2N} \geq 0) = \dfrac{1 + P(S_{2N} = 0)}{2}$, puis que $\lim\limits_{N\to+\infty} (P(S_{2N} \geq 0)) = 1/2$.

Exercice 2 (Résultant de deux polynômes)

Définition et propriétés

Soient p et q deux entiers naturels non nuls, et

$$P = \sum_{k=0}^{p} a_k X^k \quad \text{et} \quad Q = \sum_{k=0}^{q} b_k X^k$$

deux polynômes de $\mathbb{C}[X]$ avec $a_p \neq 0$ et $b_q \neq 0$. Le *résultant des polynômes P et Q* est le nombre complexe noté $\mathrm{Res}(P,Q)$:

$$\mathrm{Res}(P,Q) = \begin{vmatrix} a_0 & & & & b_0 & & \\ a_1 & \ddots & & & b_1 & \ddots & \\ \vdots & & a_0 & & \vdots & & b_0 \\ a_p & & a_1 & a_0 & \vdots & & b_1 \\ & \ddots & \vdots & a_1 & b_q & & \vdots \\ & & a_p & \vdots & & \ddots & \vdots \\ & & & a_p & & & b_q \end{vmatrix}.$$

C'est un déterminant à $q+p$ colonnes, dont les q premières colonnes représentent les coefficients du polynôme P et les p suivantes représentent les coefficients du polynôme Q, les positions non remplies étant des zéros. Par exemple, si $P = 1 + 2X + 3X^2$ et $Q = 4 + 5X + 6X^2 + 7X^3$:

$$\mathrm{Res}(P,Q) = \begin{vmatrix} 1 & 0 & 0 & 4 & 0 \\ 2 & 1 & 0 & 5 & 4 \\ 3 & 2 & 1 & 6 & 5 \\ 0 & 3 & 2 & 7 & 6 \\ 0 & 0 & 3 & 0 & 7 \end{vmatrix}.$$

On notera $M_{P,Q}$ la matrice de $\mathscr{M}_{p+q}(\mathbb{C})$ servant à définir $\mathrm{Res}(P,Q)$, de sorte que :

$$\mathrm{Res}(P,Q) = \det(M_{P,Q}).$$

Partie I - Premiers calculs

1. Dans cette question, on suppose que $P = a_1X + a_0$ et $Q = b_1X + b_0$ sont de degré 1.
   (a) Quelle est la taille de la matrice $M_{P,Q}$? Expliciter cette matrice.
   (b) Calculer $\text{Res}(P, Q)$. Que dire des polynômes P et Q si $\text{Res}(P, Q) = 0$?
2. On revient au cas général où $\deg(P) = p$ et $\deg(Q) = q$ sont des entiers naturels non nuls. Montrer à l'aide d'opérations élémentaires sur les colonnes que :
$$\text{Res}(P, Q) = (-1)^{pq} \cdot \text{Res}(Q, P).$$

Partie II - Critère de primalité relative

On note $E = \mathbb{C}_{q-1}[X] \times \mathbb{C}_{p-1}[X]$ et $F = \mathbb{C}_{p+q-1}[X]$. Soit u l'application de E dans F définie pour $(A, B) \in E$ par :
$$u(A, B) = PA + QB.$$

3. (a) Démontrer que u est une application linéaire.
   (b) Supposons u bijective. Justifier que 1 appartient à $\text{Im}(u)$. En déduire que P et Q sont premiers entre eux.
   (c) Réciproquement, supposons P et Q premiers entre eux. Montrer que $\text{Ker}(u) = \{0_E\}$. En déduire que u est bijective.
4. On note $\mathscr{B} = \left((1,0), (X,0), \ldots, (X^{q-1},0), (0,1), (0,X), \ldots, (0,X^{p-1})\right)$ une base de E et $\mathscr{B}' = (1, X, \ldots, X^{p+q-1})$ la base canonique de F.
   (a) Montrer soigneusement que la matrice $M_{\mathscr{B},\mathscr{B}'}(u)$ de u par rapport aux bases $\mathscr{B}$ et $\mathscr{B}'$ est égale à $M_{P,Q}$.
   (b) Démontrer que $\text{Res}(P, Q) \neq 0$ si, et seulement si, P et Q sont premiers entre eux.

Partie III - Discriminant

On suppose $p \geq 2$ dans cette section. On appelle *discriminant de* P le nombre complexe noté $\Delta(P)$:
$$\Delta(P) = \frac{(-1)^{p(p-1)/2}}{a_p}\text{Res}(P, P').$$

5. Montrer que P est à racines simples si, et seulement si, $\Delta(P) \neq 0$.
6. Calculer $\Delta(P)$ lorsque $P = aX^2 + bX + c \in \mathbb{C}[X]$ est de degré 2. Quel résultat bien connu retrouve-t-on ici ?
7. Déterminer une condition nécessaire et suffisante pour que le polynôme $X^3 + aX + b$ admette une racine multiple.

Partie IV - Nombres algébriques

Un complexe z est un *nombre algébrique* s'il est racine d'un polynôme non nul à coefficients rationnels.

8. Soient x et y deux nombres algébriques, P et Q des polynômes non nuls à coefficients rationnels qui les annulent. Posons $z = x + y$.
   (a) Justifier que les polynômes $P(X)$ et $Q(z - X)$ ne sont pas premiers entre eux.
   (b) En déduire que z est algébrique.
9. Montrer que le produit de deux nombres algébriques est algébrique.
10. Conclure que l'ensemble des nombres algébriques est un sous-anneau de $\mathbb{C}$.