Énoncé

Dans tout le problème, n désigne un entier naturel non nul et ξ le complexe $\xi = e^{\frac{2i\pi}{n}}$.

Partie I Calcul d'un déterminant circulant

Soient $a_0, ..., a_{n-1} \in \mathbb{C}$ et P le polynôme :

$$P = \sum_{k=0}^{n-1} a_k X^k \in \mathbb{C}[X].$$

Cette partie a pour but de calculer le déterminant de $C(a_0, ..., a_{n-1})$ défini par

$$C(a_0, ..., a_{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & & a_{n-3} \\ \vdots & & & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix}.$$

1. Notons $V = (\xi^{(j-1)(i-1)})_{(i,j)\in[\![1,n]\!]^2}$:

$$V = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \xi & \xi^2 & \dots & \xi^{n-1} \\ 1 & \xi^2 & \xi^4 & \dots & \xi^{2(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \xi^{n-1} & \xi^{2(n-1)} & \dots & \xi^{(n-1)(n-1)} \end{pmatrix}$$

   a. Donner sans démonstration une expression de $\det(V)$.

   b. Soit $z_1, \cdots, z_n$ des nombres complexes et $Q = (X - z_1)\cdots(X - z_n)$. Montrer que

$$\prod_{\substack{(i,j)\in[\![1,n]\!]^2 \\ i\neq j}} (z_j - z_i) = \prod_{i\in[\![1,n]\!]} Q'(z_i)$$

   c. En factorisant $X^n - 1$, montrer que $\prod_{k=0}^{n-1} \xi^k = (-1)^{n-1}$.

   d. En déduire que $\det(V) = \varepsilon n^{\frac{n}{2}}$ avec $\varepsilon \in \{1, -1, i, -i\}$.

   e. Pour tout $p \in [\![0, n-1]\!]$, notons :

$$e_p = (1, \xi^p, \xi^{2p}, ..., \xi^{(n-1)p}) \in \mathbb{C}^n.$$

   Montrer que la famille $(e_0, ..., e_{n-1})$ est une base de $\mathbb{C}^n$.

2. Pour tout $p \in [\![0, n-1]\!]$, notons E_p la matrice colonne représentant le vecteur e_p dans la base canonique de $\mathbb{C}^n$:

$$E_p = \begin{pmatrix} 1 \\ \xi^p \\ \xi^{2p} \\ \vdots \\ \xi^{p(n-1)} \end{pmatrix}$$

   Montrer que $C(a_0, ..., a_{n-1})E_p = P(\xi^p)E_p$.

3. Montrer que la matrice $C(a_0, ..., a_{n-1})$ est semblable à une matrice diagonale que l'on explicitera.

4. Montrer que :

$$\det(C(a_0, ..., a_{n-1})) = \prod_{p=0}^{n-1} P(\xi^p).$$

Partie II Combinaisons de racines de l'unité à coefficients aléatoires

Soit $(\Omega, \mathbb{P})$ un espace probabilisé fini, soient $X_1, ..., X_n$ des variables aléatoires définies sur Ω et à valeurs dans $\{-1, 1\}$, mutuellement indépendantes et telles que :

$$\forall k \in [\![1, n]\!],\ \mathbb{P}(X_k = 1) = \mathbb{P}(X_k = -1) = \frac{1}{2}.$$

Notons $Z : \Omega \to \mathbb{C}$ la variable aléatoire définie pour tout $\omega \in \Omega$ par :

$$Z(\omega) = \sum_{k=1}^{n} X_k(\omega) e^{\frac{2ik\pi}{n}}.$$

Pour tout $k \in \mathbb{N}$, on notera $|Z|^k$ la variable aléatoire définie pour tout $\omega \in \Omega$ par :

$$|Z|^k(\omega) = |Z(\omega)|^k.$$

II.1 Espérance et variance

1. a. Soient $1 \leq k < l \leq n$. Donner la valeur de $\mathbb{E}(X_k)$ puis de $\mathbb{E}(X_k X_l)$.

   b. En déduire que $\mathbb{E}(|Z|^2) = n$.

2. a. Soient $i, j, k, l \in [\![1, n]\!]$ tels que $i < j$ et $k < l$. Montrer que $\mathbb{E}(X_i X_j X_k X_l) \neq 0$ si et seulement si $i = k$ et $j = l$.

   b. Calculer $\mathbb{E}(|Z|^4)$ puis $\mathbb{V}(|Z|^2)$.

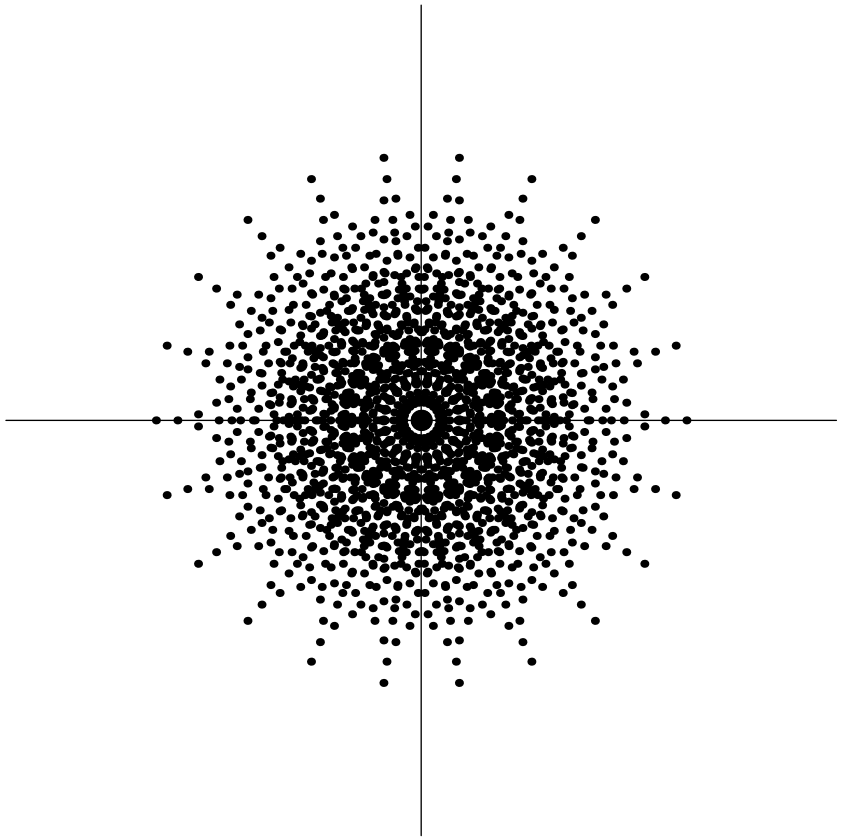

FIG. 1: Valeurs de Z pour $n = 11$

II.2 Inégalités de concentration.

Dans toute cette partie, t désigne un réel strictement positif.

1. Montrer que :
$$\mathbb{P}(|Z|^2 \geq t) \leq \frac{n}{t}.$$

La suite de la partie II.2 est consacrée à la démonstration d'une meilleure majoration.

Notons X et Y les variables aléatoires définies pour tout $\omega \in \Omega$ par :
$$X(\omega) = \sum_{k=1}^{n} X_k \cos\left(\frac{2k\pi}{n}\right), \qquad Y(\omega) = \sum_{k=1}^{n} X_k \sin\left(\frac{2k\pi}{n}\right).$$

2. a. Montrer que pour tout $x \in \mathbb{R}$, $\text{ch}(x) \leq e^{\frac{x^2}{2}}$. On pourra dériver deux fois la fonction $f : x \in \mathbb{R} \mapsto e^{-\frac{x^2}{2}} \text{ch}(x)$.

   b. Calculer la somme :
$$\sum_{k=0}^{n-1} \cos^2\left(\frac{2k\pi}{n}\right).$$

   c. Montrer que pour tout $\theta \in \mathbb{R}$:
$$\mathbb{E}(e^{\theta X}) \leq e^{\frac{n\theta^2}{4}}.$$

3. Montrer que pour tout $\theta \in \mathbb{R}_+$:
$$\mathbb{P}(X \geq t) \leq e^{-\theta t + \frac{n\theta^2}{4}}.$$

4. En déduire que :
$$\mathbb{P}(X \geq t) \leq e^{-\frac{t^2}{n}}.$$

5. Montrer que X et $-X$ ont même loi et en déduire que :
$$\mathbb{P}(|X| \geq t) \leq 2e^{-\frac{t^2}{n}}.$$

On admet que pour tout $t \in \mathbb{R}^+$:
$$\mathbb{P}(|Y| \geq t) \leq 2e^{-\frac{t^2}{n}}.$$

6. Comparer les événements $\{|Z|^2 \geq t\}$ et $\{|X| \geq \sqrt{\frac{t}{2}}\} \cup \{|Y| \geq \sqrt{\frac{t}{2}}\}$. En déduire que :
$$\mathbb{P}(|Z|^2 \geq t) \leq 4e^{-\frac{t}{2n}}.$$

Partie III. Déterminant d'une matrice circulante aléatoire

Dans cette partie, **l'entier n est supposé premier impair**.
On rappelle que $\mathbb{U}_n$ désigne l'ensemble des racines n-èmes de l'unité.
On munit l'ensemble $\mathcal{P}(\mathbb{U}_n)$ des parties de $\mathbb{U}_n$ de l'équiprobabilité $\mathbb{P}$.
Pour tout $u \in \mathbb{U}_n$, on note $X_u : \Omega \to \{-1, 1\}$ la variable aléatoire définie sur Ω par :

$$\forall J \in \Omega,\ X_u(J) = \begin{cases} 1 \text{ si } u \in J \\ -1 \text{ si } u \notin J \end{cases}$$

1. a. Montrer que pour tout $u \in \mathbb{U}_n$:

$$\mathbb{P}(X_u = 1) = \mathbb{P}(X_u = -1) = \frac{1}{2}.$$

   b. Montrer que les variables aléatoires X_u $(u \in \mathbb{U}_n)$ sont mutuellement indépendantes.

Pour tout $k \in [\![0, n-1]\!]$, notons $Z_k : \Omega \to \mathbb{R}_+$ la variable aléatoire définie pour tout $J \in \Omega$ par :

$$Z_k(J) = \sum_{u \in \mathbb{U}_n} X_u(J) u^k.$$

Ainsi, la variable aléatoire Z_1 a la même loi que la variable aléatoire Z définie dans la partie II.

2. On rappelle que n est premier. Soit $k \in [\![1, n-1]\!]$.
   a. Montrer que l'application $\varphi_k : u \in \mathbb{U}_n \mapsto u^k \in \mathbb{U}_n$ est une bijection.
   On note $\overline{\varphi_k} : J \in \Omega \mapsto \varphi_k(J) \in \Omega$ la bijection qui à toute partie J de $\mathcal{P}(\mathbb{U}_n)$ associe son image directe par φ_k.
   b. Montrer que $Z_k = Z_1 \circ \overline{\varphi_k}$.
   c. En déduire que Z_k et Z_1 ont même loi.

On note $D : \Omega \to \mathbb{R}_+$ la variable aléatoire définie par :

$$\forall J \in \Omega,\ D(J) = \left|\det(C(X_{\xi^0}(J), X_{\xi^1} ..., X_{\xi^{n-1}}(J)))\right|.$$

3. Montrer à l'aide de la partie I que pour tout $J \in \Omega$:

$$D(J) = |Z_0(J)| \prod_{k=1}^{\frac{n-1}{2}} |Z_k(J)|^2.$$

4. Posons $M : \Omega \to \mathbb{R}_+$ la variable aléatoire définie pour tout $J \in \Omega$ par :

$$M(J) = \max_{k \in [\![1, \frac{n-1}{2}]\!]} |Z_k(J)|^2.$$

Montrer à l'aide de la partie II que pour tout $t \in \mathbb{R}_+$:

$$\mathbb{P}(M \geq t) \leq 2(n-1)e^{-\frac{t}{2n}}.$$

5. Montrer que pour tout $t \in \mathbb{R}^+$:

$$\mathbb{P}(D \geq nt^{\frac{n-1}{2}}) \leq 2(n-1)e^{-\frac{t}{2n}}.$$

6. Soit $W : \Omega \to \mathbb{R}^+$ une variable aléatoire, soit $p \in \mathbb{N}$ tel que $W(\Omega) \subset [0, p]$.
   a. Montrer que :

$$\mathbb{E}(W) \leq \sum_{k=0}^{p} (k+1)(\mathbb{P}(W \geq k) - \mathbb{P}(W \geq k+1)).$$

   b. Montrer que :

$$\mathbb{E}(W) \leq 1 + \sum_{k=1}^{p} \mathbb{P}(W \geq k).$$

7. a. Montrer que $D(\Omega) \subset [0, n^n]$.
   b. Montrer que :

$$\mathbb{E}(D) \leq 1 + 2(n-1) \sum_{k=1}^{n^n} \exp\left(-\frac{\left(\frac{k}{n}\right)^{\frac{2}{n-1}}}{2n}\right).$$

   c. Montrer que pour tout $k \in \mathbb{N}$:

$$\int_0^{k/2} t^k e^{-t}\, dt \leq k!.$$

   d. Calculer l'intégrale :

$$\int_0^{n^n} \exp\left(-\frac{\left(\frac{x}{n}\right)^{\frac{2}{n-1}}}{2n}\right)\, dx.$$

   e. En déduire que :

$$\mathbb{E}(D) \leq 1 + n\left[\left(\frac{n-1}{2}\right)!\right](2n)^{\frac{n-1}{2}}.$$

Corrigé

Partie I. Calcul d'un déterminant circulant

1. a. On reconnaît un déterminant de Vandermonde. Il faut :

$$\det(V) = \prod_{0\leq i<j\leq n-1} (\xi^j - \xi^i).$$

b. Par propriétés de la dérivation d'un produit :

$$Q' = \sum_{k=1}^{n} \prod_{\substack{j=1\\ j\neq k}}^{n} (X - z_j).$$

Soit $i \in [\![1, n]\!]$. En évaluant cette expression en z_i, on voit que tous les termes de la somme sont nuls sauf celui pour lequel $k = i$, donc :

$$Q'(z_i) = \prod_{\substack{j=1\\ j\neq i}} (z_i - z_j).$$

Ainsi :

$$\prod_{i=1}^{n} Q'(z_i) = \prod_{i=1}^{n} \prod_{\substack{j=1\\ j\neq i}}^{n} Q'(z_j) = \prod_{\substack{(i,j)\in[\![1,n]\!]^2\\ i\neq j}} (z_i - z_j).$$

c. Posons Posons $Q = X^n - 1 = \prod_{i=0}^{n-1}(X - \xi^i)$. D'après les relations coefficients-racines, $-1 = \prod_{k=0}^{n-1} \xi^k = (-1)^n \prod_{k=0}^{n-1}$, d'où le résultat.

d. D'après la b. appliquée au polynôme $Q = X^n - 1$ et à ses racines $1, \xi, ..., \xi^{n-1}$:

$$\prod_{\substack{(i,j)\in[\![1,n]\!]^2\\ i\neq j}} (\xi^i - \xi^j) = \prod_{i=0}^{n-1} P'(\xi^i) = \prod_{i=0}^{n-1} n(\xi^i)^{n-1}.$$

Mais pour tout i, $(\xi^i)^{n-1} = (\xi^{n-1})^i = (\xi^{-1})^i = \xi^{-i}$ car $\xi^{n-1} = \xi^{-1}$ donc :

$$\prod_{\substack{(i,j)\in[\![0,n-1]\!]^2\\ i\neq j}} (\xi^i - \xi^j) = n^n \prod_{i=0}^{n-1} \xi^{-i} = (-1)^{n-1} n^n.$$

Ainsi :

$$\begin{aligned}(-1)^{n-1} n^n &= \prod_{\substack{(i,j)\in[\![0,n-1]\!]^2\\ i\neq j}} (\xi^i - \xi^j)\\ &= \left[\prod_{0\leq i<j\leq n-1} (\xi^i - \xi^j)\right] \left[\underbrace{\prod_{0\leq j<i\leq n-1} (\xi^i - \xi^j)}_{\frac{n(n-1)}{2} \text{ facteurs}}\right]\\ &= (-1)^{\frac{n(n-1)}{2}} \left[\prod_{0\leq i<j\leq n-1} (\xi^i - \xi^j)\right]^2 = (-1)^{\frac{n(n-1)}{2}} \det(V)^2\end{aligned}$$

donc $\det(V)^2 = \pm n^n$. Alors il existe $\varepsilon \in \{1, -1, i, -i\}$ tel que $\det(V) = \varepsilon n^{\frac{n}{2}}$.

e. La matrice de la famille $(e_0, ..., e_{p-1})$ est justement la matrice V. Son déterminant est non nul d'après la question précédente, donc elle est inversible, donc de rang n. Donc la famille $(e_0, ..., e_{n-1})$ est de rang n, donc c'est une base de $\mathbb{C}^n$.

2. La première ligne du vecteur colonne $C(a_0, ..., a_{n-1})E_p$ vaut :

$$a_0 + a_1\xi^p + ... + a_{n-1}\xi^{p(n-1)} = P(\xi^p).$$

Soit $i \in [\![2, n]\!]$. La i-ème ligne du vecteur colonne $C(a_0, ..., a_{n-1})E_p$ vaut :

$$\begin{aligned}a_{n-i+1} + a_{n-i+2}\xi^p + ... + a_{n-1}\xi^{p(i-2)} + a_0\xi^{p(i-1)} + ... + a_{n-i}\xi^{p(n-1)}\\ = \xi^{p(i-1)}[a_{n-i+1}\xi^{-p(i-1)} + a_{n-i+2}\xi^{-p(i-2)}\\ + ... + a_{n-1}\xi^{-p} + a_0 + a_1\xi^p + ... + a_{n-i}\xi^{p(n-i)}].\end{aligned}$$

Comme $\xi^{np} = 1$, alors :

$$\xi^{-p(n-i)} = \xi^{p(n-i+1)}, ..., \xi^{-p} = \xi^{p(n-1)}.$$

Donc la ième ligne du vecteur colonne $C(a_0, ..., a_{n-1})E_p$ vaut :

$$\xi^{p(i-1)}[a_0 + a_1\xi^p + ... + a_{n-1}\xi^{p(n-1)}] = \xi^{p(i-1)}P(\xi^p).$$

Donc $C(a_0, ..., a_{n-1})E_p = P(\xi^p)E_p$.

3. Notons $u \in \mathcal{L}(\mathbb{C}^n)$ l'endomorphisme canoniquement associé à $C(a_0, ..., a_{n-1})$. D'après la question précédente, pour tout $p \in [\![0, n-1]\!]$, $u(e_p) = P(\xi^p)e_p$. Donc la matrice de u dans la base $(e_0, ..., e_{p-1})$ est diagonale de coefficients diagonaux $P(1), (\xi), ..., P(\xi^{n-1})$. Ainsi, $C(a_0, ..., a_{n-1})$ est semblable à la matrice :

$$\begin{pmatrix} P(1) & & & \\ & P(\xi) & & \\ & & \ddots & \\ & & & P(\xi^{n-1}) \end{pmatrix}$$

4. Le déterminant de $C(a_0, ..., a_{n-1})$ est égal au déterminant de la matrice diagonale ci-dessus, qui vaut :

$$\prod_{k=0}^{n-1} P(\xi^k).$$

Partie II. Module de combinaisons linéaires de racines de l'unité à coefficients aléatoires

II.1 Espérance et variance

1. a. Par définition, $\mathbb{E}(X_k) = \mathbb{P}(X_k = 1) - \mathbb{P}(X_k = -1) = 0$. Comme les variables sont mutuellement indépendantes :

$$X_k \neq X_l \Rightarrow \mathbb{E}(X_k X_l) = \mathbb{E}(X_k)\mathbb{E}(X_l) = 0.$$

b. Introduisons le conjugué pour exprimer le carré du module puis utilisons la linéarité de l'espérance et la question précédente :

$$|Z|^2 = \sum_{(k,l)\in[\![1,n]\!]^2} X_k X_l\, \xi^{k-l} = n + 2 \sum_{\substack{(k,l)\in[\![1,n]\!]^2 \\ k<l}} X_k X_l\, \xi^{k-l}$$

$$\Rightarrow \mathbb{E}(|Z|^2) = n + 2 \sum_{\substack{(k,l)\in[\![1,n]\!]^2 \\ k<l}} \underbrace{\mathbb{E}(X_k X_l)}_{=0} \xi^{k-l} = n$$

car X_k^2 est la variable constante (certaine) de valeur 1.

2. a. Comme les variables sont mutuellement indépendantes et centrées,

$$\mathbb{E}(X_i X_j X_k X_l) \neq 0 \Rightarrow \text{Card}\,\{X_i, X_j, X_k, X_l\} < 4.$$

On sait que $X_i \neq X_j$ car $i < j$ et $X_k \neq X_l$ car $k < l$. Les deux paires $\{X_i, X_j\}$ et $\{X_k, X_l\}$ ne peuvent pas être disjointes.
Si $X_k = X_j$ alors $k = j$ donc $j < l$ donc

$$\mathbb{E}(X_i X_j X_k X_l) = \mathbb{E}(X_i X_j X_l) = 0.$$

On en déduit $X_k = X_i$ et $\mathbb{E}(X_i X_j X_k X_l) = \mathbb{E}(X_j X_l)$ serait nul si $X_j \neq X_l$. On doit donc avoir $i = k$ et $j = l$.

b. Comme en 1.b.

$$|Z|^4 = \left(n + 2 \sum_{\substack{(i,j)\in[\![1,n]\!]^2 \\ i<j}} X_i X_j\, \xi^{i-j} \right) \left(n + 2 \sum_{\substack{(k,l)\in[\![1,n]\!]^2 \\ k<l}} X_k X_l\, \xi^{k-l} \right)$$

$$= n^2 + 4n \sum_{\substack{(i,j)\in[\![1,n]\!]^2 \\ i<j}} X_i X_j\, \xi^{i-j} + 4 \sum_{\substack{(i,j,k,l)\in[\![1,n]\!]^4 \\ i<j,\ k<l}} X_i X_j X_k X_l\, \xi^{i-j+k-l}$$

$$\Rightarrow \mathbb{E}\left(|Z|^4\right) = n^2 + 4\,\frac{n(n-1)}{2} = 3n^2 - 2n$$

car dans la dernière somme, seuls les quadruplets (i, j, i, j) contribuent vraiment et chacun pour la valeur 1.
Avec $\mathbb{E}(|Z|^2) = n$, on obtient

$$\mathbb{V}(|Z|^2) = \mathbb{V}(|Z|^4) - \mathbb{E}(|Z|^2) = 2n(n-1).$$

II.2. Inégalités de concentration.

1. Comme Z est une variable aléatoire à valeurs positives, on peut lui appliquer l'inégalité de Markov :

$$\mathbb{P}(|Z|^2 \geq t) \leq \frac{\mathbb{E}(|Z|^2)}{t} = \frac{n}{t}.$$

2. a. Introduisons une fonction f définie dans $\mathbb{R}$ et calculons sa dérivée

$$f(x) = \text{ch}(x)e^{-\frac{x^2}{2}} \Rightarrow f'(x) = (\text{sh}(x) - x\,\text{ch}(x))\,e^{-\frac{x^2}{2}}.$$

Le signe de $f'(x)$ est celui de $g(x)$ avec $g(x) = \text{sh}(x) - x\,\text{ch}(x)$. Alors

$$g'(x) = -x\,\text{sh}(x) \leq 0.$$

La fonction g est décroissante dans $\mathbb{R}$, nulle en 0 donc positive pour les négatifs et négative pour les positifs. La fonction f admet en minimum absolu en 0 de valeur 1. On en déduit

$$\forall x \in \mathbb{R},\ \text{ch}(x) \leq e^{-\frac{x^2}{2}}.$$

b. On linéarise :

$$\sum_{k=0}^{n-1}\cos^2\left(\frac{2k\pi}{n}\right)=\sum_{k=0}^{n-1}\left(\frac{1}{2}+\frac{1}{2}\cos\left(\frac{4k\pi}{n}\right)\right)=\frac{n}{2}.$$

c. Comme les variables aléatoires X_k sont mutuellement indépendantes, les variables $e^{\theta\cos\left(\frac{2k\pi}{n}\right)X_k}$ le sont aussi. Remarquons que

$$\mathbb{E}\left(e^{\theta\cos\left(\frac{2k\pi}{n}\right)X_k}\right)=\frac{1}{2}\left(e^{\theta\cos\left(\frac{2k\pi}{n}\right)}+e^{-\theta\cos\left(\frac{2k\pi}{n}\right)}\right)=\mathrm{ch}\left(\theta\cos\left(\frac{2k\pi}{n}\right)\right).$$

On en déduit

$$\mathbb{E}(e^{\theta X})=\prod_{k=1}^{n}E\left(e^{\theta X_k\cos\left(\frac{2k\pi}{n}\right)}\right)=\prod_{k=1}^{n}\mathrm{ch}\left(\theta\cos\left(\frac{2k\pi}{n}\right)\right)$$
$$\leq\prod_{k=1}^{n}e^{\frac{\left(\theta\cos\left(\frac{2k\pi}{n}\right)\right)^2}{2}}=e^{\frac{\theta^2}{2}\sum_{k=1}^{n}\cos^2\left(\frac{2k\pi}{n}\right)}=e^{\frac{n\theta^2}{4}}.$$

3. Soit $\theta\in\mathbb{R}_+$, d'après l'inégalité de Markov appliquée à $e^{\theta X}$:

$$\mathbb{P}(X\geq t)=\mathbb{P}(e^{\theta X}\geq e^{\theta t})\leq e^{-\theta t}\mathbb{E}(e^{\theta X})\leq e^{-\theta t+\frac{n\theta^2}{4}}$$

4. Posons $\theta=\frac{2t}{n}$, de manière à minimiser l'expression $-\theta t+\frac{n\theta^2}{4}$. Alors :

$$\mathbb{P}(X\geq t)\leq e^{-\frac{t^2}{n}}.$$

5. Soit $x\in C$. Alors :

$$\{X=x\}=\bigcup_{\substack{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n\\ \sum_{i=1}^{n}\varepsilon_i\xi^i}}\{(X_1=\varepsilon_1,\dots,X_n=\varepsilon_n\}.$$

La réunion est disjointe et pour tout $(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n$, $\mathbb{P}(X_1=\varepsilon_1,\dots,X_n=\varepsilon_n)=\frac{1}{2^n}$. Donc :

$$\mathbb{P}(X=x)=\frac{\mathrm{card}(A(x))}{2^n}$$

avec

$$A(x)=\{(\varepsilon_1,\dots,\varepsilon_n)\in\{-1,1\}^n\mid\sum_{i=1}^{n}\varepsilon_i\xi^i=x\}$$

Or L'application $f:(\varepsilon_1,\dots,\varepsilon_n)\in A(x)\mapsto(-\varepsilon_1,\dots,-\varepsilon_n)\in A(-x)$ est une bijection donc $\mathrm{card}(A(x))=\mathrm{card}(A(-x))$. Donc $\mathbb{P}(X=x)=\mathbb{P}(X=-x)=\mathbb{P}(-X=x)$. Ainsi, X et $-X$ ont même loi.
Ainsi, comme $\{|X|\geq t\}=\{X\geq t\}\cup\{-X\geq t\}$, alors :

$$\mathbb{P}(|X|\geq t)\leq\mathbb{P}(X\geq t)+\mathbb{P}(-X\geq t)=2\mathbb{P}(X\geq t)\leq 2e^{-\frac{t^2}{n}}.$$

6. Comme $|Z|^2=X^2+Y^2$, alors :

$$\{|Z|^2\geq t\}\subset\{X^2\geq\frac{t}{2}\}\cup\{Y^2\geq\frac{t}{2}\}$$

(si $x^2+y^2\geq t$, alors l'un au-moins des réels x^2 et y^2 et supérieur ou égal à $\frac{t}{2}$). Donc :

$$\{|Z|^2\geq t\}\subset\{|X|\geq\sqrt{\frac{t}{2}}\}\cup\{|Y|\geq\sqrt{\frac{t}{2}}\}.$$

Donc :

$$\mathbb{P}(|Z|^2\geq t)\leq\mathbb{P}(|X|\geq\sqrt{\frac{t}{2}})+\mathbb{P}(|Y|\geq\sqrt{\frac{t}{2}})\leq 4e^{-\frac{t}{2n}}.$$

Partie III. Déterminant d'une matrice circulaire aléatoire

1. a. Soit $u\in\mathbb{U}_n$. Notons $\mathcal{A}=\{J\in\Omega\mid u\in J\}$. Alors :

$$\mathbb{P}(X_u=1)=\frac{\mathrm{card}(\mathcal{A})}{\mathrm{card}(\Omega)}=\frac{\mathrm{card}(\mathcal{A})}{2^n}.$$

Comme l'application $J\in\mathcal{A}\mapsto J^c\in\mathcal{A}^c$ est une bijection, alors $\mathcal{A}$ et son complémentaire ont même cardinal. Mais comme $\mathcal{A}$ et $\mathcal{A}^c$ partitionnent Ω, alors $2^n=\mathrm{card}(\mathcal{A})+\mathrm{card}(\mathcal{A}^c)$ donc $\mathrm{card}(\mathcal{A})=2^{n-1}$. Donc :

$$\mathbb{P}(X_u=1)=\mathbb{P}(X_u=-1)=\frac{1}{2}.$$

b. Soit $(\varepsilon_u)_{u\in\mathbb{U}_n} \in \{-1,1\}^n$. Alors

$$\bigcap_{u\in\mathbb{U}_n} \{X_u = \varepsilon_u\} = \{J \in \Omega \mid \forall u \in \mathbb{U}_n,\ \varepsilon_u = 1 \iff u \in J\} = \{J\}.$$

Donc :

$$\mathbb{P}\left(\bigcap_{u\in\mathbb{U}_n} \{X_u = \varepsilon_u\}\right) = \frac{1}{2^n} = \prod_{u\in\mathbb{U}_n} \mathbb{P}(X_u = \varepsilon_u).$$

Ainsi, les variables aléatoires X_u sont mutuellement indépendantes.

2. a. Comme $\mathbb{U}_n$ est fini, il suffit de montrer que φ_k est injective. Soient $u, v \in \mathbb{U}_n$ tels que $\varphi_k(u) = \varphi_k(v)$. Il existe $p, q \in [\![0, n-1]\!]$ tels que $u = e^{\frac{2ip\pi}{n}}$ et $v = e^{\frac{2iq\pi}{n}}$, donc $e^{\frac{2ik(p-q)\pi}{n}} = 1$. Donc n divise $k(p-q)$. Comme n est premier et $1 \leq k < n$, alors n est premier avec k donc d'après le théorème de Gauss, n divise $(p-q)$. Mais comme $-n < p-q < n$, alors $p = q$ et $u = v$; L'application φ_k est bien injective donc bijective.

b. Soit $J \in \Omega$. Alors pour tout $u \in \mathbb{U}_n$, $X_{\varphi_k^{-1}(u)}(J) = X_u(\overline{\varphi_k}(J))$. Donc le changement d'indice $v = \varphi_k(u)$ donne :

$$Z_k(J) = \sum_{u\in\mathbb{U}_n} X_u(J)\varphi_k(u) = \sum_{v\in\mathbb{U}_n} X_{\varphi_k^{-1}(v)}(J)v$$
$$= \sum_{v\in\mathbb{U}_n} X_v(\overline{\varphi_k}(J))v = Z_1 \circ \overline{\varphi_k}(J).$$

c. Ainsi, comme $\overline{\varphi_k}$ est bijective, alors $Z_k(\Omega) = Z_1(\Omega)$ et pour tout $z \in Z_k(\Omega)$:

$$\{Z_k = z\} = \{Z_1 \circ \overline{\varphi_k} = z\} = \overline{\varphi_k}(\{Z_1 = z\}).$$

Comme $\overline{\varphi_k}$ est bijective, alors les ensembles $\{Z_1 = z\}$ et $\overline{\varphi_k}(\{Z_1 = z\})$ ont même cardinal, donc même probabilité :

$$\mathbb{P}(Z_k = z) = \mathbb{P}(Z_1 = z).$$

Donc Z_k et Z_1 ont même loi.

3. Soit $J \in \Omega$. Notons P_J le polynôme :

$$P_J = \sum_{k=0}^{n-1} X_{\xi^k}\xi^k = \sum_{u\in\mathbb{U}_n} X_u(J)u^k = Z_k(J).$$

D'après la partie I : :

$$D(J) = \prod_{p=0}^{n-1} |P_J(\xi^p)| = \prod_{k=0}^{n-1} |Z_k(J)|.$$

Mais pour tout $k \in [\![1, \frac{n-1}{2}]\!]$:

$$Z_{n-k}(J) = \sum_{u\in\mathbb{U}_n} X_u(J)u^{n-k} = \sum_{u\in\mathbb{U}_n} X_u(J)u^{-k} = \sum_{u\in\mathbb{U}_n} X_u(J)\overline{u^k} = \overline{Z_k(J)}.$$

Donc en particulier : $|Z_k(J)| = |Z_{n-k}(J)|$. Ainsi :

$$|Z_1(J)| = |Z_{n-1}(J)|, |Z_2(J)| = |Z_{n-2}(J)|, ..., \left|Z_{\frac{n-1}{2}}(J)\right| = \left|Z_{\frac{n+1}{2}}(J)\right|.$$

Donc :

$$D(J) = |Z_0(J)| \prod_{k=1}^{\frac{n-1}{2}} |Z_k(J)|^2.$$

4. Soit $t > 0$. Alors :

$$\{M \geq t\} = \bigcup_{k=1}^{\frac{n-1}{2}} \{|Z_k|^2 \geq t\}$$

donc :

$$\mathbb{P}(M \geq t) \leq \sum_{k=1}^{\frac{n-1}{2}} \mathbb{P}(|Z_k|^2 \geq t) = \frac{n-1}{2}\mathbb{P}(|Z_1|^2 \geq t)$$

puisque les Z_k ont la même loi que Z_1. Mais comme Z_1 a la même loi que la variable aléatoire Z introduite dans la partie II, alors :

$$\mathbb{P}(|Z_1|^2 \geq t) \leq 4e^{-\frac{t}{2n}}$$

donc :

$$\mathbb{P}(M \geq t) \leq 2(n-1)e^{-\frac{t}{2n}}.$$

5. Il suffit de remarquer que pour tout $J \in \Omega$:

$$|D(J)| \leq |Z_0(J)|\,|M(J)|^{\frac{n-1}{2}}.$$

Comme $|Z_0(J)| \leq n$, alors $|D(J)| \leq nM(J)^{\frac{n-1}{2}}$. Donc :

$$\{D \geq nt^{\frac{n-1}{2}}\} \subset \{nM^{\frac{n-1}{2}} \geq nt^{\frac{n-1}{2}}\} = \{M \geq t\}$$

donc :

$$\mathbb{P}(D \geq nt^{\frac{n-1}{2}}\} \leq 2(n-1)e^{-\frac{t}{2n}}.$$

6. a. Par définition de l'espérance :

$$\mathbb{E}(W) = \sum_{w \in W(\Omega)} w\mathbb{P}(W = w) = \sum_{k=0}^{p} \sum_{w \in W(\Omega) \cap [p, p+1[} w\mathbb{P}(W = w).$$

Mais pour tout $k \in [\![0, p]\!]$:

$$\begin{aligned}\sum_{w \in W(\Omega) \cap [k, k+1[} w\mathbb{P}(W = w) &\leq (k+1) \sum_{w \in W(\Omega) \cap [k, k+1[} \mathbb{P}(W = w) \\ &= (k+1)\mathbb{P}(k \leq W < k+1) \\ &= (k+1)[\mathbb{P}(W \geq k) - \mathbb{P}(W \geq k+1)]\end{aligned}$$

Cela donne le résultat souhaité.

b. Coupons la somme en deux, effectuons un changement d'indice dans la deuxième somme puis regroupons les termes :

$$\begin{aligned}\mathbb{E}(W) &\leq \sum_{k=0}^{p}(k+1)[\mathbb{P}(W \geq k) - \mathbb{P}(W \geq k+1)] \\ &= \sum_{k=0}^{p}(k+1)\mathbb{P}(W \geq k) - \sum_{k=0}^{p}(k+1)\mathbb{P}(W \geq k+1) \\ &= \sum_{k=0}^{p}(k+1)\mathbb{P}(W \geq k) - \sum_{l=1}^{p+1} l\mathbb{P}(W \geq l) \quad (l = k+1) \\ &= \sum_{k=0}^{p}(k+1)\mathbb{P}(W \geq k) - \sum_{k=1}^{p} k\mathbb{P}(W \geq k) \quad (\mathbb{P}(W \geq p+1) = 0) \\ &= \mathbb{P}(W \geq 0) + \sum_{k=1}^{p}[(k+1) - k]\mathbb{P}(W \geq k) \\ &= 1 + \sum_{k=1}^{p}\mathbb{P}(W \geq k) \quad (\mathbb{P}(W \geq 0) = 1)\end{aligned}$$

7. a. Pour tout $k \in [\![0, n-1]\!]$, pour tout $J \in \Omega$, $|Z_k(J)| \leq n$ (inégalité triangulaire) donc $0 \leq D(J) \leq n^n$.

b. D'après la question précédente :

$$\mathbb{E}(D) \leq 1 + \sum_{k=1}^{n^n} \mathbb{P}(D \geq k).$$

Mais d'après la question 5, en posant $t = \left(\frac{k}{n}\right)^{\frac{2}{n-1}}$:

$$\mathbb{P}(D \geq k) = \mathbb{P}(D \geq nt^{\frac{n-1}{2}}) \leq 2(n-1)e^{-\frac{t}{2n}} = e^{-\frac{\left(\frac{k}{n}\right)^{\frac{2}{n-1}}}{2n}}$$

donc :

$$\mathbb{E}(D) \leq 1 + 2(n-1)\sum_{k=1}^{n^n} e^{-\frac{\left(\frac{k}{n}\right)^{\frac{2}{n-1}}}{2n}}$$

c. Un intégration par parties donne pour $k \geq 1$:

$$\int_0^{k/2} t^n e^{-t}\, dt = [-kt^{k-1}e^{-t}]_0^{k/2} + k\int_0^{k/2} t^{k-1}e^{-t}\, dt.$$

Comme :

$$[-kt^{k-1}e^{-t}]_0^{k/2} = -k\left(\frac{k}{2}\right)^{k-1} e^{-k/2} \leq 0$$

donc :

$$\int_0^{k/2} t^k e^{-t}\, dt \leq k\int_0^{k/2} t^{k-1}e^{-t}\, dt.$$

Une simple récurrence montre alors que :

$$\int_0^{k/2} t^k e^{-t}\, dt \leq k! \underbrace{\int_0^{k/2} e^{-t}\, dt}_{=1-e^{-k/2} \leq 1} \leq k!.$$

d. Notons i l'intégrale à calculer. Effectuons d'abord le changement de variables $ny = x$, $ndy = dx$. Alors :

$$I = n\int_0^{n^{n-1}} e^{-\frac{y^{\frac{2}{n-1}}}{2n}}\, dy.$$

Effectuons ensuite le changement de variables $t^{\frac{n-1}{2}} = y$, $\frac{n-1}{2}t^{\frac{n-3}{2}}dt = dy$:

$$I = \frac{n(n-1)}{2}\int_0^{n^2} e^{-\frac{t}{2n}}t^{\frac{n-3}{2}}\ dt.$$

Effectuons enfin le changement de variables $2nu = t$, $2ndu = dt$:

$$I = \frac{n(n-1)}{2}\int_0^{n/2} e^{-u}(2nu)^{\frac{n-3}{2}}(2n)\ du = \frac{n(n-1)(2n)^{\frac{n-1}{2}}}{2}\int_0^{n/2} e^{-u}u^{\frac{n-3}{2}}\ du$$

donc d'après la question précédente :

$$I \leq \frac{n(n-1)}{2}(2n)^{\frac{n-1}{2}}\left(\frac{n-3}{2}\right)! = n\left(\frac{n-1}{2}\right)!(2n)^{\frac{n-1}{2}}.$$

e. Notons $f : x \in \mathbb{R} \mapsto e^{-\frac{(\frac{x}{n})^{\frac{2}{n-1}}}{2n}}$. Cette fonction est décroissante donc pour tout $k \in [\![1, n^n]\!]$:

$$f(k) = \int_{k-1}^{k} f(k)\ dx \leq \int_{k-1}^{k} f(x)\ dx.$$

Donc en sommant, la relation de Chasles donne :

$$\sum_{k=1}^{n^n} f(k) \leq \int_0^{n^n} f(x)\ dx.$$

La question 7 appliquée à $W = D$ et le calcul précédent donnent la majoration souhaitée.