

Agrégation externe de Mathématiques
Énoncés

J. E. Rombaldi

29 mai 2009

Table des matières

1	Agrégation externe 1975, épreuve 1	1
2	Agrégation externe 1978, épreuve 1	5
3	Agrégation externe 1979, épreuve 1	9
4	Agrégation externe 1989, épreuve 1	13
5	Agrégation externe 1990, épreuve 1	19
6	Agrégation externe 1991, épreuve 1	25
7	Agrégation externe 1995, épreuve 1	31
8	Agrégation externe 1998. Épreuve 1	41
9	Agrégation externe 1999. Épreuve 1	47
10	Agrégation externe 2000. Épreuve 1	53
11	Agrégation externe 2001. Épreuve 1	59
12	Agrégation externe 2002. Épreuve 1	63
13	Agrégation externe 2003. Épreuve 1	71
14	Agrégation externe 2004. Épreuve 1	75
15	Agrégation externe 2005. Épreuve 1	79
16	Agrégation externe 2006. Épreuve 1	83
17	Agrégation externe 2007. Épreuve 1	89
18	Agrégation externe 2009. Épreuve 1	95

Agrégation externe 1975, épreuve 1

La partie **I** est indépendante des deux suivantes.

— I —

n étant un élément de \mathbb{N}^* (entier naturel non nul), on note $(\pi_1, \pi_2, \dots, \pi_n)$ la base canonique de \mathbb{Q}^n . La matrice d'une forme quadratique \bar{q} relative à cette base est appelée matrice canonique de \bar{q} ; \bar{q} est dite définie positive si $\bar{q}(x) \geq 0$ pour tout x .

$\mathcal{M}_n(\mathbb{Q})$ (resp. $\mathcal{M}_n(\mathbb{Z})$) est l'algèbre des matrices carrées d'ordre n à coefficients dans \mathbb{Q} (resp. \mathbb{Z}). $GL_n(\mathbb{Q})$ (resp. $GL_n(\mathbb{Z})$) est le groupe multiplicatif des matrices inversibles de $\mathcal{M}_n(\mathbb{Q})$ (resp. inversibles de $\mathcal{M}_n(\mathbb{Z})$). I est la matrice unité de $\mathcal{M}_n(\mathbb{Q})$. tM (resp. $\det(M)$) est la transposée (resp. le déterminant) de la matrice M . Dans cette première partie, n ne prend que les valeurs 2 et 3.

1. Soit \bar{q} une forme quadratique de \mathbb{Q}^2 , de matrice canonique $M = \begin{pmatrix} u & v \\ v & w \end{pmatrix} \in GL_2(\mathbb{Z})$.
On pose $\delta = \det(M)$. Montrer que, si \bar{q} est non dégénérée, positive, alors $\delta = 1$.
2. On suppose toujours $M \in GL_2(\mathbb{Z})$ et, pour cette question et la suivante : $\delta = 1$. Montrer que l'une des deux formes \bar{q} ou $-\bar{q}$ est non dégénérée, positive.
3. (a) Admettant ici que \bar{q} est non dégénérée, positive, démontrer, pour $u \neq 1$, l'existence d'une matrice $P = \begin{pmatrix} -s & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{Z})$ telle que, si $M' = {}^tPMP = \begin{pmatrix} u' & v' \\ v' & w' \end{pmatrix}$, alors $0 < u' \leq \frac{u}{2}$.
(b) En déduire l'existence de $N \in GL_2(\mathbb{Z})$ telle que $M = {}^tNN$. Énoncer une propriété relative à la décomposition de \bar{q} en somme de deux carrés.
4. Jusqu'à la fin de cette première partie, \bar{q} désigne une forme quadratique de \mathbb{Q}^3 , non dégénérée, positive, dont la matrice canonique :

$$M = \begin{pmatrix} m & p & q \\ p & m' & r \\ q & r & m'' \end{pmatrix}$$

est un élément de $GL_3(\mathbb{Z})$.

- (a) Que peut-on dire des signes de m, m', m'' et $\det(M)$?

(b) Montrer que, si M n'est pas égale à I , l'une des six inégalités suivantes est vérifiée :

$$|p| > \frac{m}{2}, |p| > \frac{m'}{2}, |q| > \frac{m}{2}, |q| > \frac{m''}{2}, |r| > \frac{m'}{2}, |r| > \frac{m''}{2}$$

(on pourra séparer le cas $m = m' = m''$, puis le cas $m \geq m' \geq m''$, $m > m'$).

5.

(a) Déterminer une matrice triangulaire $P \in GL_3(\mathbb{Z})$ telle que $M_1 = {}^tPMP$ soit de même type que M , avec l'une des trois conditions suivantes réalisée :

$$\begin{cases} m_1 = m, m'_1 \leq m' - 1, m''_1 = m'', \\ m_1 \leq m - 1, m'_1 = m', m''_1 = m'', \\ m_1 = m, m'_1 = m', m''_1 \leq m'' - 1. \end{cases}$$

(b) En déduire l'existence de $N \in GL_3(\mathbb{Z})$ telle que $M = {}^tNN$. Énoncer une propriété relative à la décomposition de \bar{q} en somme de trois carrés.

(c) Application numérique : $M = \begin{pmatrix} 5 & 0 & 3 \\ 0 & 1 & 1 \\ 3 & 1 & 3 \end{pmatrix}$ (on se limitera à exhiber une matrice N).

6. Donner un exemple de matrice $M \in GL_3(\mathbb{Z})$, telle que ${}^tM = M$, que $\det(M) = 1$ et qu'il n'existe aucune matrice $N \in GL_3(\mathbb{Z})$ vérifiant $M = {}^tNN$ (un exemple à coefficients dans \mathbb{N}^* serait apprécié).

7. Retrouver les résultats de la question **3.** à partir de ceux de **5.** Comparer les deux méthodes.

— II —

V est un espace vectoriel de dimension n sur \mathbb{Q} ; H, H', \dots , sont, par convention, des sous-groupes additifs de V (confondus, selon l'usage, avec les ensembles sous-jacents). $\mathcal{H}_0 = \text{Hom}(H, \mathbb{Z})$ est l'ensemble des morphismes de groupes de H vers \mathbb{Z} . \widehat{H} est le sous-espace vectoriel de V engendré par H . La somme $H + H'$ est le sous-groupe de V engendré par $H \cup H'$. Pour $\lambda \in \mathbb{Q}$, λH est l'image de H par l'homothétie de rapport λ .

Une \mathbb{Z} -base de H est une famille libre de vecteurs de V telle qu'un vecteur de V appartient à H si, et seulement si, il est combinaison linéaire à coefficients entiers relatifs des vecteurs de la famille. Un réseau est un sous-groupe de V admettant au moins une \mathbb{Z} -base de cardinal n . L, L', \dots , sont, par convention, des réseaux de V . Un sous-réseau est un réseau d'un sous-espace vectoriel de V .

1. Démontrer que $\widehat{L} = V$.

2. $\mathcal{B} = (e_i)_{1 \leq i \leq p}$ étant une famille finie de vecteurs de V , on note B la matrice des coordonnées des vecteurs e_i , ($1 \leq i \leq p$), dans une base (ω_j) , ($1 \leq j \leq n$), de V considérée comme fixe dans tout le problème : B est appelée matrice canonique de \mathcal{B} . Montrer que B et B' étant les matrices canoniques d'une \mathbb{Z} -base \mathcal{B} de L et d'une famille finie \mathcal{B}' de vecteurs de L , \mathcal{B}' est une \mathbb{Z} -base de L si, et seulement si, il existe $P \in GL_n(\mathbb{Z})$ telle que $B' = BP$. Montrer que le rationnel $\text{vol}(L) = |\det(B)|$ est indépendant du choix d'une \mathbb{Z} -base de L .

3. L' étant un réseau de V , montrer qu'il existe $d \in \mathbb{N}^*$ tel que $dL' \subset L$ et que $d^n \left(\frac{\text{vol}(L')}{\text{vol}(L)} \right)$ est un entier.
4. H étant un sous-groupe de L non réduit à $\{0\}$, montrer que H est un sous-réseau de V (on pourra, par exemple, considérer une \mathbb{Z} -base (e_i) de L , rechercher un élément a de \mathbb{N}^* , une application coordonnée ψ , un vecteur b tel que $\psi(b) = a$ et utiliser l'endomorphisme θ de H défini par :

$$\theta(x) = x - \frac{\psi(x)}{a}b.$$

5. Montrer que l'intersection et la somme de deux réseaux de V sont des réseaux.
6. X et Y étant les matrices canoniques de deux vecteurs x et y de V , on note $(x | y) = {}^tXY$ (produit de x et y), et $\|x\|^2 = {}^tXX$ (carré de x). Une partie A de V est dite bornée s'il existe un rationnel \mathcal{A} tel que $\|x\|^2 \leq \mathcal{A}$ pour tout $x \in A$.
- (a) Montrer que tout sous-groupe H de V dont l'intersection avec toute partie bornée de V est finie est un sous-réseau de V (on pourra considérer une famille libre maximale (h_1, \dots, h_r) de vecteurs de H , la partie Ω de V formée des vecteurs $\sum_{i=1}^r \mu_i h_i$, $\mu_i \in \mathbb{Q} \cap [0, 1]$, et associer au vecteur $\sum_{i=1}^r \lambda_i h_i$, $\lambda_i \in \mathbb{Q}$, le vecteur $\sum_{i=1}^r (\lambda_i - [\lambda_i]) h_i$, où le symbole $[\cdot]$ représente la partie entière).
- (b) Démontrer la réciproque.

— III —

H étant un sous-groupe de V , on note H_0 l'ensemble des $x \in V$ tels que pour tout $y \in H$, on ait $(x | y) \in \mathbb{Z}$. Un réseau L est dit r -modulaire (resp. unimodulaire) si $L_0 = rL$ (resp. $L_0 = L$); il est dit r -modulaire trivial s'il existe une \mathbb{Z} -base (e_i) de L orthogonale (c'est-à-dire vérifiant $(e_i | e_j) = 0$ pour $i \neq j$) et telle que $\|e_i\|^2 = \frac{1}{r}$ pour tout i ($\frac{1}{r}$ s'appelle alors le carré de la \mathbb{Z} -base; cette dernière est dite orthonormale si $r = 1$). \mathbb{F}_2 est le corps à deux éléments.

1. (a) Montrer que, si L est un réseau de V , $\mathcal{L}_0 = \text{Hom}(L, \mathbb{Z})$ est un réseau d'un certain espace vectoriel W de dimension n sur \mathbb{Q} (on pourra utiliser la famille (e_i^0) de \mathcal{L}_0 définie par $e_i^0(e_j) = \delta_{ij}$).
- (b) Définir un isomorphisme α du groupe L_0 sur \mathcal{L}_0 , indépendant de tout choix de \mathbb{Z} -base de L . En déduire que L_0 est un réseau de V , dont on explicitera une \mathbb{Z} -base à partir d'une \mathbb{Z} -base de L .
2. L et L' étant deux réseaux de V , démontrer les égalités :

$$L_{00} = L, (L + L')_0 = L_0 \cap L'_0, (L \cap L')_0 = L_0 + L'_0, \text{vol}(L) \text{vol}(L_0) = 1.$$

Calculer $\text{vol}(L)$ dans le cas où L est r -modulaire.

3. On suppose jusqu'à la fin de cette partie que L est un réseau r -modulaire trivial. Montrer que L est r -modulaire, et qu'il existe une « similitude directe » (notion que l'on définira par analogie avec la structure euclidienne de \mathbb{R}^n) transformant le réseau fondamental Λ , sous-groupe engendré par la base canonique (ω_i) de V , en L .

4. (a) On note $\text{Aut}(L)$ l'ensemble des morphismes de groupe s de L dans lui-même tels que $(s(x) | s(y)) = (x | y)$ pour tout couple (x, y) de L^2 . On considère une \mathbb{Z} -base (e_i) de L , orthogonale et de carré $\frac{1}{r}$. À tout élément s de $\text{Aut}(L)$, on associe la matrice S des coordonnées des vecteurs $e'_i = s(e_i)$ dans la \mathbb{Z} -base (e_i) . Montrer qu'il existe un élément k de S_n (groupe des permutations de $[1, n]$) et une application ε de $[1, n]$ dans $\{-1, 1\}$ tels que l'élément (i, j) de S s'écrive sous la forme $s_{ij} = \varepsilon(j) \delta_{i, k(j)}$. Calculer le cardinal de $\text{Aut}(L)$.
- (b) Étudier l'ensemble U des $s \in \text{Aut}(L)$ auxquels on peut associer une application f de $[1, n]$ dans $\{-1, 1\}$ telle que l'élément (i, j) de S s'écrive $s_{ij} = f(j) \delta_{i, j}$; un tel s sera noté s_f . Comparer U et le groupe $(\mathbb{F}_2^n, +)$.
- (c) Étudier l'ensemble T des $s \in \text{Aut}(L)$ tels que, $k \in S_n$ étant défini comme en a. l'élément (i, j) de S s'écrive $s_{ij} = \delta_{i, k(j)}$; un tel s sera noté s_k . Comparer T et le groupe (S_n, \circ) .
5. (a) Montrer que tout $s \in \text{Aut}(L)$ se décompose, de manière unique, sous la forme $s = s_f \circ s_k$, $(s_f, s_k) \in U \times T$.
- (b) Déterminer un morphisme φ de T dans le groupe $\text{Aut}(U)$ des automorphismes du groupe U tel que $U \times T$, muni de la loi :

$$(s_f, s_k) \perp (s_{f'}, s_{k'}) = (s_f \circ \varphi(s_k)(s_{f'}), s_k \circ s_{k'})$$

soit isomorphe à $\text{Aut}(L)$, muni de la loi \circ .

6. Déterminer un loi \star sur le produit cartésien $\mathbb{F}_2^n \times S_n$ telle qu'il existe un isomorphisme θ de ce produit sur $\text{Aut}(L)$. Caractériser, par analogie avec φ , un morphisme F de S_n dans le groupe linéaire de dimension n sur \mathbb{F}_2 , en calculant la matrice $F(k)$ relative à la base canonique de \mathbb{F}_2^n .

— IV —

On définit dans V les isométries (resp. les rotations), et les groupes matriciels correspondants $O_n(\mathbb{Q})$ (resp. $O_n^+(\mathbb{Q})$) par analogie avec les notions similaires des espaces euclidiens réels. Σ_n est l'ensemble des entiers m de la forme $m = \alpha_1^2 + \dots + \alpha_n^2$, $\alpha_i \in \mathbb{Z}$.

1. Dans toute cette partie, L est un réseau unimodulaire de V . (e_i) étant une \mathbb{Z} -base quelconque de L , de matrice canonique B , on considère l'automorphisme λ de V de matrice canonique B , et la forme quadratique \bar{q} définie par $\bar{q}(x) = \|\lambda(x)\|^2$. Que peut-on dire de la matrice canonique M de \bar{q} ? de l'image $\bar{q}(\Lambda)$ du réseau fondamental Λ par \bar{q} .
2. Dans les questions suivantes (jusqu'à **IV. 5.** incluse), on suppose $n = 3$. Montrer que $\bar{q}(\Lambda) = \Sigma_3$.
3. (a) Démontrer que L est unimodulaire trivial.
(b) Caractériser, à l'aide des ensembles $O_3^+(\mathbb{Q})$ et $GL_3(\mathbb{Z})$, les matrices canoniques des \mathbb{Z} -bases des réseaux unimodulaires de V .
(c) Comment obtient-on ces réseaux à partir de Λ ?
4. Résoudre l'équation matricielle ${}^t K K = {}^t B B$, où $K \in GL_3(\mathbb{Z})$ et B est définie au **IV. 1.** Dénombrer les solutions.
5. Si L' est un réseau de V tel que $L' \subset L'_0$, démontrer l'existence d'un réseau unimodulaire trivial L tel que $L' \subset L \subset L'_0$ (on pourra considérer $(\Lambda + L') \cap L'_0$).
6. Indiquer brièvement ce que deviennent les questions précédentes pour $n = 2$.

Agrégation externe 1978, épreuve 1

Dans tout le problème, on désigne par ω un entier strictement positif pair et par Ω un ensemble de cardinal ω .

Pour tout ensemble finie E , on note $|E|$ son cardinal.

Pour tout entier n , on désigne par \bar{n} son image modulo $2\mathbb{Z}$ et on note \mathbb{F}_2 le corps à deux éléments $\frac{\mathbb{Z}}{2\mathbb{Z}}$.

On note $\mathbb{Z}[X, Y]$ l'ensemble des polynômes à deux indéterminées à coefficients dans \mathbb{Z} .

– I.A – Généralités

1. Vérifier que l'ensemble $\mathcal{P}(\Omega)$ des parties de Ω , muni de l'opération différence symétrique définie par :

$$(x, y) \mapsto x + y = \{t \in \Omega \mid (t \in x \cup y) \text{ et } (t \notin x \cap y)\}$$

est un groupe abélien.

2. Montrer que l'ensemble $\mathcal{P}(\Omega)$ peut être muni d'une structure d'espace vectoriel sur le corps \mathbb{F}_2 dont la loi de groupe additif est celle définie en **I.A.1**.
3. Quelle est la dimension de $\mathcal{P}(\Omega)$? Fournir une base de cet espace vectoriel.
4. Vérifier que l'application α de $\mathcal{P}(\Omega) \times \mathcal{P}(\Omega)$ dans \mathbb{F}_2 définie par :

$$\alpha(x, y) = \overline{|x \cap y|}$$

est une forme bilinéaire symétrique non dégénérée sur $\mathcal{P}(\Omega)$.

Dans ce qui suit, $\mathcal{P}(\Omega)$ est muni de cette forme bilinéaire.

5. On désigne par $\mathcal{D}(\Omega)$ le sous-espace vectoriel de $\mathcal{P}(\Omega)$ engendré par Ω . Décrire l'orthogonal $\mathcal{H}(\Omega)$ de $\mathcal{D}(\Omega)$ et retrouver la formule :

$$\sum_{k=0}^{\frac{\omega}{2}} C_{\omega}^{2k} = 2^{\omega-1}.$$

Quelle le noyau de la restriction de α à $\mathcal{H}(\Omega)$?

– I.B – Codes et polynômes des poids

Les sous-espaces vectoriels de $\mathcal{P}(\Omega)$ sont appelés les codes de $\mathcal{P}(\Omega)$. Si \mathcal{C} est un code de $\mathcal{P}(\Omega)$, on désigne par \mathcal{C}^0 son orthogonal. Pour toute permutation s de Ω , on désigne par \bar{s} l'application linéaire de $\mathcal{P}(\Omega)$ dans $\mathcal{P}(\Omega)$ définie par :

$$x \mapsto \bar{s}(x) = \{s(t) \mid t \in x\}.$$

On dit que deux codes \mathcal{C} et \mathcal{C}' sont isomorphes s'il existe une permutation s de Ω telle que $\bar{s}(\mathcal{C}) = \mathcal{C}'$.

Un code \mathcal{C} de $\mathcal{P}(\Omega)$ est dit auto-orthogonal si $\mathcal{C} = \mathcal{C}^0$.

Si \mathcal{C} est un code de $\mathcal{P}(\Omega)$, on appelle polynôme des poids de \mathcal{C} et on note $P_{\mathcal{C}}(X, Y)$ l'élément de $\mathbb{Z}[X, Y]$ défini par :

$$P_{\mathcal{C}}(X, Y) = \sum_{x \in \mathcal{C}} X^{|x|} Y^{\omega - |x|}.$$

1. Quelle est la dimension d'un code auto-orthogonal ? Démontrer que si \mathcal{C} est auto-orthogonal on a $\mathcal{D}(\Omega) \subset \mathcal{C} \subset \mathcal{H}(\Omega)$.
2. On pose $\omega = 2m$ et $\Omega = \{t_1, t_2, \dots, t_m, u_1, u_2, \dots, u_m\}$. Construire un code auto-orthogonal dont le polynôme des poids est :

$$P_{\omega}(X, Y) = (X^2 + Y^2)^m.$$

3. Soit $\Gamma(\Omega)$ l'ensemble des codes auto-orthogonaux de $\mathcal{P}(\Omega)$ dont le polynôme des poids est $P_{\omega}(X, Y)$. Démontrer que deux éléments quelconques de $\Gamma(\Omega)$ sont isomorphes.
4. Pour $\omega = 2m$ multiple de 4 et $\Omega = \{t_1, t_2, \dots, t_m, u_1, u_2, \dots, u_m\}$, vérifier que le code \mathcal{B}_{ω} engendré par $\{t_1, t_2, \dots, t_m\}$, $\{u_1, u_2, \dots, u_m\}$ et $\{t_h, t_j, u_h, u_j\}$ pour $h \neq j$ et $1 \leq h \leq m$, $1 \leq j \leq m$, est un code auto-orthogonal dont le polynôme des poids est :

$$Q_{\omega}(X, Y) = \frac{1}{2} \left((X^2 + Y^2)^m + (X^2 - Y^2)^m + (2XY)^m \right).$$

5. On dit qu'un code auto-orthogonal est pair si les cardinaux de tous ses éléments sont multiples de 4. Vérifier que si ω est multiple de 8, le code \mathcal{B}_{ω} défini en **I.B.4.** est pair.
6. Soit \mathcal{C} un code de $\mathcal{P}(\Omega)$.

- (a) Soit $f : \mathcal{P}(\Omega) \mapsto M$ une application à valeurs dans un groupe abélien M dont la loi est notée additivement. On pose $(-1)^{\bar{0}} = 1$ et $(-1)^{\bar{1}} = -1$ et on note $\hat{f} : \mathcal{P}(\Omega) \mapsto M$ la fonction définie par :

$$\hat{f}(x) = \sum_{y \in \mathcal{P}(\Omega)} (-1)^{\alpha(x,y)} f(y).$$

Démontrer que pour tout code \mathcal{C} de $\mathcal{P}(\Omega)$, on a :

$$\sum_{x \in \mathcal{C}} \hat{f}(x) = 2^{\dim(\mathcal{C})} \sum_{y \in \mathcal{C}^0} f(y).$$

- (b) En prenant pour M le groupe additif $\mathbb{Z}[X, Y]$ et en choisissant judicieusement la fonction f , démontrer la formule de Mac-Williams :

$$2^{\dim(\mathcal{C})} P_{\mathcal{C}^0}(X, Y) = P_{\mathcal{C}}(Y - X, X + Y).$$

– II.A – Invariants d'un groupe fini

On désigne par V un espace vectoriel complexe de dimension finie, par $\mathcal{E} = (e_1, e_2, \dots, e_n)$ une base de V et par $\text{Aut}(V)$ le groupe des automorphismes de V .

On note I l'endomorphisme identité de V .

Si g est un endomorphisme de V , on note $\text{Tr}(g)$ sa trace.

On note A l'algèbre $\mathbb{C}[X_1, X_2, \dots, X_n]$.

Pour tout entier naturel k , on note A_k l'espace vectoriel complexe des polynômes homogènes de degré k en n variables et a_k sa dimension.

À tout élément $g \in \text{Aut}(V)$ on associe l'application $\sigma_g : A \rightarrow A$ définie de la manière suivante :

si pour tout h compris entre 1 et n on a :

$$g(e_h) = \sum_{j=1}^n \gamma_{j,h} e_j,$$

alors pour tout $P \in A$:

$$\sigma_g(P)(X_1, \dots, X_n) = P\left(\sum_{j=1}^n \gamma_{j,1} X_j, \dots, \sum_{j=1}^n \gamma_{j,n} X_j\right).$$

On désigne par G un sous-groupe fini de $\text{Aut}(V)$.

On note V^G le sous-espace vectoriel de V formé des vecteurs v tels que $g(v) = v$ pour tout $g \in G$.

On note A_k^G l'ensemble des $P \in A_k$ tels que $\sigma_g(P) = P$ pour tout $g \in G$, et a_k^G sa dimension.

1. Montrer que :

$$\dim(V^G) = \frac{1}{|G|} \sum_{g \in G} \text{Tr}(g)$$

(on pourra utiliser l'endomorphisme $\rho_G = \frac{1}{|G|} \sum_{g \in G} g$ et démontrer en particulier que $V^G = \rho_G(V)$).

2.

(a) Vérifier que l'application $\sigma : g \mapsto \sigma_g$ est un morphisme de groupes de $\text{Aut}(V)$ dans le groupe $\text{Aut}(A)$ des automorphismes de l'algèbre A .

(b) Vérifier que pour tout $g \in \text{Aut}(V)$ l'application σ_g induit, pour tout entier naturel k , un automorphisme de l'espace vectoriel A_k .

3. Montrer que les séries entières $\sum_{k=0}^{+\infty} a_k z^k$ et $\sum_{k=0}^{+\infty} a_k^G z^k$ ont des rayons de convergence strictement positifs.

On pose :

$$\Phi_G(z) = \sum_{k=0}^{+\infty} a_k^G z^k.$$

4. Pour tout $g \in G$, on désigne par g_k l'automorphisme de A_k défini par g .

(a) Comparer la trace de g_k au coefficient de z^k dans le développement en série entière de $\frac{1}{\det(I - zg)}$.

(b) En déduire que pour $|z| < 1$, on a :

$$\Phi_G(z) = \frac{1}{|G|} \sum_{g \in G} \frac{1}{\det(I - zg)}.$$

– II.B – Algèbre associée aux polynômes des poids

On pose $A = \mathbb{C}[X, Y]$ et on utilise les notations de **II. A.** pour $n = 2$. On note G le groupe des matrices engendré par :

$$\mu = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \text{ et } \rho = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Si $P \in A$ et $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$, on pose alors :

$$\sigma_g(P)(X, Y) = P(aX + cY, bX + dY).$$

Si r est un réel, on note $[r]$ sa partie entière.

1. Soit \mathcal{C} un code auto-orthogonal de $\mathcal{P}(\Omega)$. Montrer que $P_{\mathcal{C}}(X, Y)$ est invariant par les transformations σ_g pour $g \in G$.

2.

(a) Quel est le cardinal de H ?

(b) Montrer que le groupe monogène H engendré par $\rho\mu$ est distingué dans G .

(c) Étudier le groupe quotient G/H , et en déduire que G est de cardinal 16.

3.

(a) Décomposer $\frac{1}{(1 - X^2)(1 - X^8)}$ en éléments simples dans $\mathbb{R}(X)$.

(b) Montrer que pour $|z| < 1$ on a :

$$\Phi_G(z) = \frac{1}{(1 - z^2)(1 - z^8)}.$$

4. Montrer que la dimension de A_k^G est :

$$a_k^G = \begin{cases} \left[\frac{k}{8} \right] + 1 & \text{si } k \text{ est pair,} \\ 0 & \text{si } k \text{ est impair.} \end{cases}$$

5. On désigne par A^G l'algèbre des polynômes à deux variables invariants par G . Montrer que :

$$A^G = \mathbb{C}[P_2(X, Y), Q_8(X, Y)] = \{P(P_2(X, Y), Q_8(X, Y)) \mid P \in A\}$$

où les polynômes P_ω et Q_ω ont été définis en **I. B.**

6. On pose $\Delta(X, Y) = X^2 Y^2 (X^2 - Y^2)^2$.

Montrer que si \mathcal{C} est un code auto-orthogonal de $\mathcal{P}(\Omega)$, alors le polynôme $P_{\mathcal{C}}(X, Y)$ appartient à l'algèbre :

$$\mathbb{Z}[P_2(X, Y), \Delta(X, Y)] = \{P(P_2(X, Y), \Delta(X, Y)) \mid P \in \mathbb{Z}[X, Y]\}.$$

Agrégation externe 1979, épreuve 1

Notations et définitions

Dans tout le problème, on considère un espace vectoriel euclidien E de dimension $n \geq 2$, un entier $k \geq 2$ et un réel $\gamma \in]0, 1[$. Les entiers n et k et le réel γ pourront être assujettis à des conditions supplémentaires qui dépendront de la question traitée.

On se propose d'étudier certaines familles finies de vecteurs de E et certains ensembles de droites vectorielles de E , appelés épis.

Si v, v' appartiennent à E , leur produit scalaire est noté $(v | v')$ et on pose $\|v\| = \sqrt{(v | v)}$.

On note $\mathcal{L}(E)$ l'algèbre des endomorphismes de E , $\mathcal{L}^s(E)$ l'espace des endomorphismes symétriques de E et $\mathcal{O}(E)$ le groupe orthogonal de E .

Pour tout $v \in E$ on désigne par p_v l'endomorphisme de E défini par :

$$\forall v' \in E, \quad p_v(v') = (v | v')v.$$

On définit une opération de $\mathcal{O}(E)$ sur l'ensemble E^k en posant, si $f \in \mathcal{O}(E)$ et si $x = (x_1, x_2, \dots, x_k) \in E^k$:

$$f \cdot x = (f(x_1), f(x_2), \dots, f(x_k)).$$

Si Y est un ensemble, on note $\text{Card}(Y)$ le cardinal de Y et Id_Y l'application identique de Y .

Si P est un polynôme non nul de $\mathbb{C}[x]$ et si $\lambda \in \mathbb{C}$, on note $m(\lambda, P)$ le plus grand entier naturel m tel que $(X - \lambda)^m$ divise P dans $\mathbb{C}[x]$.

On désigne par \mathcal{M}_k l'espace des matrices à k lignes et k colonnes à termes réels.

Si $A \in \mathcal{M}_k$, on note P_A le polynôme caractéristique de A .

L'espace des matrices symétriques de \mathcal{M}_k est noté \mathcal{M}_k^s .

Si $B \in \mathcal{M}_k^s$, $\lambda(B)$ désigne la plus petite valeur propre de B .

On note I_k la matrice identité de \mathcal{M}_k et J_k la matrice de \mathcal{M}_k dont tous les termes sont égaux à 1.

– I – Résultats préliminaires

1.

(a) Déterminer le rang et la trace de J_k . En déduire P_{J_k} .

(b) Si α et β sont des réels quelconques, former le polynôme caractéristique et calculer les valeurs propres de la matrice $A_k = \alpha I_k + \beta J_k$.

2.

- (a) Soit Q un polynôme irréductible dans $\mathbb{Q}[x]$. Montrer que toute racine complexe de Q est simple.
- (b) Soit P un polynôme non nul de $\mathbb{Q}[x]$. Soit λ une racine complexe de P telle que $\deg(P) < 2m(\lambda, P)$. Montrer que λ appartient à \mathbb{Q} .
3. Si $f \in \mathcal{L}(E)$, $\text{Tr}(f)$ désigne la trace de f . Montrer que $\mathcal{L}^s(E)$ muni de la forme bilinéaire symétrique $(f, f') \mapsto \langle f, f' \rangle = \text{Tr}(f \circ f')$ est un espace vectoriel euclidien.
4. À tout $x = (x_1, x_2, \dots, x_k) \in E^k$, on associe la matrice $B_x = ((x_i | x_j))_{1 \leq i, j \leq k}$ dans \mathcal{M}_k^s . L'espace \mathbb{R}^k étant muni du produit scalaire usuel, noté $(\cdot | \cdot)_{\mathbb{R}^k}$, pour lequel la base canonique $\varepsilon = (\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)$ est orthonormée, φ_x désigne l'application linéaire de \mathbb{R}^k dans E définie par :

$$\forall i \in \{1, 2, \dots, k\}, \quad \varphi_x(\varepsilon_i) = x_i.$$

On désigne par φ_x^* l'unique application linéaire de E dans \mathbb{R}^k telle que :

$$\forall v \in E, \forall w \in \mathbb{R}^k, \quad (w | \varphi_x^*(v))_{\mathbb{R}^k} = (\varphi_x(w) | v)$$

- (a) Montrer que B_x est la matrice dans la base ε de $\varphi_x^* \circ \varphi_x$.
- (b) En déduire les égalités :

$$\text{rang}(x) = \text{rang}(B_x) = k - m(0, P_{B_x}).$$

- (c) Montrer que $\lambda(B_x) \geq 0$ et que l'égalité a lieu si, et seulement si, la famille x est liée.
- (d) Pour i compris entre 1 et k on note $p_i = p_{x_i}$. Montrer que :

$$\varphi_x \circ \varphi_x^* = \sum_{i=1}^k p_i.$$

- (e) En déduire que B_x et $\sum_{i=1}^k p_i$ ont les mêmes valeurs propres non nulles.
- 5.
- (a) Soit $B \in \mathcal{M}_k^s$. Montrer qu'il existe $x \in E^k$ tel que $B = B_x$ si, et seulement si, $\lambda(B_x) \geq 0$ et $\text{rang}(B) \leq n$.
- (b) Soient x et y des éléments de E^k . Montrer que $B_x = B_y$ si, et seulement si, x et y ont même orbite sous l'action de $\mathcal{O}(E)$.

– II – Familles équiangulaires de vecteurs de E

On note U l'ensemble des vecteurs unitaires de E .

Une famille $u = (u_1, u_2, \dots, u_k) \in U^k$ est dite équiangulaire d'angle $\arccos(\gamma)$ si :

$$|(u_i | u_j)| = \gamma \quad (1 \leq i < j \leq k)$$

L'ensemble des familles équiangulaires $u \in U^k$ d'angle $\arccos(\gamma)$ est noté U_γ^k .

On désigne par \mathcal{A}_k l'ensemble des matrices $A = (a_{ij})_{1 \leq i, j \leq k}$ de \mathcal{M}_k^s telles que $a_{ii} = 0$ pour $1 \leq i \leq k$ et $a_{ij} \in \{-1, 1\}$ pour $1 \leq i < j \leq k$.

À tout $u \in U_\gamma^k$, on associe la matrice $A_u = \frac{1}{\gamma}(B_u - I_k)$, de sorte que $A_u \in \mathcal{A}_k$.

On dit qu'une famille équiangulaire $u = (u_1, u_2, \dots, u_k)$ est aiguë [resp. obtuse] si $(u_i | u_j) > 0$ [resp. $(u_i | u_j) < 0$] pour $1 \leq i < j \leq k$.

1.

- (a) Montrer que toute famille équiangulaire aiguë est libre.
 (b) Montrer l'existence d'une famille équiangulaire aiguë $u \in U_\gamma^n$.

2.

- (a) Soit $u = (u_1, u_2, \dots, u_k) \in U_\gamma^k$. Montrer que si la famille u est liée alors :

$$\lambda(A_u) = -\frac{1}{\gamma}, \quad m\left(-\frac{1}{\gamma}, P_{A_u}\right) = k - \text{rang}(u).$$

- (b) Montrer l'existence d'une famille équiangulaire obtuse $u \in U_{\frac{1}{n}}^{n+1}$.

3. Jusqu'à la fin de cette partie, on suppose que U_γ^k n'est pas vide et on désigne par $u = (u_1, u_2, \dots, u_k)$ un élément de U_γ^k .

Pour $1 \leq i \leq k$, on pose $p_i = p_{u_i}$.

- (a) Montrer que, pour $1 \leq i \leq k$, p_i appartient à $\mathcal{L}^s(E)$.
 (b) Calculer $\langle p_i, p_j \rangle$ pour $1 \leq i \leq j \leq k$.
 (c) Montrer que $k \leq \frac{n(n+1)}{2}$.

4. On désigne par Π le sous-espace vectoriel de $\mathcal{L}^s(E)$ engendré par (p_1, p_2, \dots, p_k) .

- (a) Montrer que $n \geq \frac{k}{1 + (k-1)\gamma^2}$ et que l'égalité a lieu si, et seulement si, Id_E appartient à Π (on pourra considérer la projection orthogonale de Id_E sur Π).

- (b) Montrer que si Id_E appartient à Π , alors $kId_E = n \sum_{i=1}^k p_i$.

5. Pour $1 \leq i < j \leq k$, on note d_{ij} le nombre d'entiers t tels que $1 \leq t \leq k$, $t \neq i$, $t \neq j$ et $(u_i | u_j)(u_i | u_t)(u_j | u_t) > 0$. On dit que la famille équiangulaire u est régulière si d_{ij} est indépendant du couple (i, j) .

Si $A_u = (\alpha_{ij})_{1 \leq i, j \leq k}$, on pose $A_u^2 = (\alpha'_{ij})_{1 \leq i, j \leq k}$.

- (a) Pour $1 \leq i < j \leq k$, calculer α'_{ij} en fonction de k , α_{ij} et d_{ij} .
 (b) Montrer que la famille u est régulière si, et seulement si, il existe des réels ρ_1, ρ_2 tels que $(A_u - \rho_1 I_k)(A_u - \rho_2 I_k) = 0$.
 (c) Montrer que Id_E appartient à Π si, et seulement si, la famille u est liée, de rang n et régulière. Montrer que, dans ce cas, les valeurs propres de A_u sont $-\frac{1}{\gamma}$ et $\frac{1}{\gamma} \left(\frac{k}{n} - 1\right)$ avec des multiplicités respectives $k - n$ et n .

6. On suppose que la famille $u = (u_1, u_2, \dots, u_k)$ est liée et que k est pair ou $k - \text{rang}(u) \geq 2$. Montrer que si $\frac{1}{\gamma^2}$ est entier, cet entier est impair (on pourra considérer les matrices déduites de A_u et A_u^2 par réduction modulo 2 dans \mathbb{Z}).

7. Montrer que si Id_E appartient à Π et si k est distinct de $n + 1$ et $2n$, alors $\frac{1}{\gamma}$ est un entier impair.

8.

- (a) Montrer que si $k > 2n$ alors $\frac{1}{\gamma}$ est un entier impair.
- (b) Montrer que si $n = 6$ alors $k \leq 16$.
9. On suppose que $k = \frac{n(n+1)}{2}$. Montrer que $n+2 = \frac{1}{\gamma^2}$. En déduire que si $n > 3$ alors $n+2$ est le carré d'un entier impair.

– III – Épis dans E

Si \mathcal{D} est un ensemble fini de droites vectorielles de E ($\text{Card}(\mathcal{D}) \geq 2$), on appelle repère de \mathcal{D} toute famille $(u_D)_{D \in \mathcal{D}}$ telle que pour toute droite $D \in \mathcal{D}$, u_D soit un vecteur unitaire de D . Un tel repère est dit aigu si $(u_D | u_{D'}) > 0$ pour toute couple (D, D') de droites distinctes appartenant à \mathcal{D} .

On dit que \mathcal{D} est un épi d'angle arccos(γ) s'il possède un repère $(u_D)_{D \in \mathcal{D}}$ tel que $|(u_D | u_{D'})| = \gamma$ pour toute couple (D, D') de droites distinctes appartenant à \mathcal{D} .

On appelle base aiguë de E tout épi de cardinal n possédant un repère aigu.

On considère dans toute cette partie une base aiguë \mathcal{B} de E d'angle arccos(γ) et un repère aigu $(u_D)_{D \in \mathcal{B}}$ de \mathcal{B} .

Pour toute partie S de \mathcal{B} , on pose $e_S = \sum_{D \in S} u_D$ et on note v_S l'unique élément de E tel que pour toute droite $D \in \mathcal{B}$ on ait :

$$(v_S | u_D) = \begin{cases} -\gamma & \text{si } D \in S \\ \gamma & \text{si } D \notin S \end{cases}$$

On pose $r = \frac{1-\gamma}{2\gamma}$ et $\Phi(X) = X^2 - nX + r^2(n+2r+1)$.

Soient S, T des parties de \mathcal{B} .

1. Calculer $(e_S | e_T)$, $\|e_S\|^2$, $(e_B | e_S)$, $\|e_B\|^2$ en fonction de $n, r, \text{Card}(S), \text{Card}(T)$ et $\text{Card}(S \cap T)$.
2. Montrer que $v_S = \omega_S e_B - \frac{1}{r} e_S$, où ω_S est un nombre réel que l'on calculera en fonction de n, r et $\text{Card}(S)$.
3. Calculer $\|v_S\|^2$ en fonction de n, r et $\text{Card}(S)$.
4. Montrer que $\|v_S\| = 1$ si, et seulement si, $\text{Card}(S)$ est racine de Φ .
5. On suppose que $\text{Card}(S) = \text{Card}(T)$ et que $\|v_S\| = 1$.
 - (a) Calculer $(v_S | v_T - v_S)$ puis $(v_S | v_T)$ en fonction de $r, \text{Card}(S)$ et $\text{Card}(S \cap T)$.
 - (b) En déduire que :

$$\begin{cases} (v_S | v_T) = \gamma \Leftrightarrow \text{Card}(S \cap T) = \text{Card}(S) - r^2 \\ (v_S | v_T) = -\gamma \Leftrightarrow \text{Card}(S \cap T) = \text{Card}(S) - r(r+1) \end{cases}$$

Agrégation externe 1989, épreuve 1

Pour tout nombre premier p , on note \mathbb{F}_p le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ des classes résiduelles modulo p .

Si S est un sous-anneau de \mathbb{C} , on note $\mathcal{M}_n(S)$ l'anneau des matrices carrées d'ordre n à coefficients dans S et $GL(n, S)$ le groupe des éléments inversibles de $\mathcal{M}_n(S)$. Si M est un élément de $\mathcal{M}_n(S)$, M^* (resp. tM) désigne la matrice adjointe (resp. transposée) de M .

On dit qu'une matrice hermitienne (resp. symétrique réelle) A est définie positive si la forme hermitienne (resp. la forme bilinéaire symétrique) associée à A est définie positive.

On dit que S est un anneau principal, si tout idéal de S peut être engendré par un seul élément, euclidien s'il existe une application N de $S - \{0\}$ dans \mathbb{N} telle que si a, b sont deux éléments non nuls de S , il existe q, r appartenant à S vérifiant $a = bq + r$ et $r = 0$ ou $N(r) < N(b)$.

– I – Préliminaires

A. Dans cette partie, p désigne un nombre premier impair.

1.

(a) Montrer que si u, v, w sont trois éléments non nuls de \mathbb{F}_p , l'équation $ux^2 + vy^2 = w$ a une solution dans \mathbb{F}_p (on pourra considérer le cardinal de l'ensemble des éléments de la forme ux^2 (resp. de la forme $w - vy^2$)).

(b) Soit $n > 1$ un entier tel que p ne divise pas $4n - 1$. Montrer qu'il existe des entiers relatifs a, b et un entier $m \geq 1$ tels que :

$$a^2 + ab + nb^2 + 1 = mp.$$

2. On suppose p de la forme $8k + 1$ ou $8k + 3$, et soit \mathbb{K} une extension de \mathbb{F}_p , corps de rupture du polynôme $t^4 + 1$. Soit b une racine dans \mathbb{K} de ce polynôme, on pose $x = b - b^{-1}$.

(a) Montrer les relations suivantes : $x^2 = -2$ et $x^p = x$. En déduire que x appartient à \mathbb{F}_p .

(b) Montrer qu'il existe des entiers a, m tels que $2a^2 + 1 = (2m - 1)p$ et prouver que la matrice :

$$\begin{pmatrix} p & a & 0 \\ a & m & 1 \\ 0 & 1 & 2 \end{pmatrix}$$

est une matrice symétrique définie positive et de déterminant égal à 1.

Déterminer tous les couples (a, m) lorsque $p = 17$.

B. Soit $D \geq 1$ un entier qui n'est pas divisible par le carré d'un nombre premier. On pose :

$$\omega_D = \begin{cases} i\sqrt{D} & \text{si } D \equiv 1 \text{ ou } 2 \pmod{4} \\ \frac{1+i\sqrt{D}}{2} & \text{si } D \equiv 3 \pmod{4} \end{cases}$$

$\mathbb{Z}[\omega_D]$ désigne le sous-anneau de \mathbb{C} , ensemble des éléments de la forme $\alpha + \beta\omega_D$, α et β éléments de \mathbb{Z} .

1. Montrer que pour tout $\lambda \in \mathbb{Z}[\omega_D]$, $|\lambda|^2$ est un entier.
2. Montrer que λ est inversible dans $\mathbb{Z}[\omega_D]$ si, et seulement si, $|\lambda| = 1$.
3. Soit p un nombre premier impair qui ne divise pas D . Montrer qu'il existe des entiers relatifs a, b, m tels que la matrice :

$$\begin{pmatrix} p & a + b\omega_D \\ a + b\overline{\omega_D} & m \end{pmatrix}$$

soit une matrice hermitienne définie positive et de déterminant égal à 1.

4. Dans le plan euclidien rapporté à un repère orthonormé, on désigne par A, B, C les images respectives des nombres $0, 1, \omega_D$ et par T le triangle, enveloppe convexe des points A, B, C . Le rayon du cercle circonscrit à T est noté R .

(a) Montrer que pour tout point M de T , on a :

$$\inf(MA, MB, MC) \leq R.$$

(b) On pose :

$$k = \sup_{z \in \mathbb{C}} \left(\inf_{u \in \mathbb{Z}[\omega_D]} |z - u|^2 \right).$$

Prouver l'égalité :

$$k = \sup_{M \in T} (\inf(MA^2, MB^2, MC^2)).$$

(c) En déduire que l'on a :

$$\begin{cases} k = \frac{D+1}{4} & \text{si } D \equiv 1 \text{ ou } 2 \pmod{4} \\ k = \frac{(D+1)^2}{16D} & \text{si } D \equiv 3 \pmod{4}. \end{cases}$$

- (d) Soient α, β deux éléments de $\mathbb{Z}[\omega_D]$, β étant supposé non nul. Montrer qu'il existe γ , élément de $\mathbb{Z}[\omega_D]$, tel que :

$$|\alpha - \beta\gamma|^2 \leq k|\beta|^2.$$

En déduire que $\mathbb{Z}[\omega_D]$ est un anneau euclidien lorsque D est égal à l'une des valeurs suivantes : 1, 2, 3, 7, 11.

Application : déterminer γ lorsque $D = 2$, $\alpha = 5 + 3\omega_2$, $\beta = -1 + 3\omega_2$.

Dans cette partie, S désigne l'anneau \mathbb{Z} ou l'un des anneaux $\mathbb{Z}[\omega_D]$ pour $D = 1, 2, 3, 7$ ou 11. Si $S = \mathbb{Z}$, on pose $k = \frac{1}{4}$, et si $S = \mathbb{Z}[\omega_D]$, k est la constante définie en **I.B.4.b**.

Deux matrices hermitiennes A, B de $\mathcal{M}_n(S)$ sont dites congruentes s'il existe $U \in GL(n, S)$ telle que $A = UBU^*$. Les classes d'équivalence pour cette relation sont appelées classes de congruence.

À un élément $x = (x_1, \dots, x_n)$ de S^n est associé une matrice à une ligne dont les coefficients sont les composantes de x ; on notera également x cette matrice. ${}^t x$ désignera la matrice transposée et x^* la matrice $\overline{{}^t x}$.

1. Montrer que si A, B sont deux matrices congruentes, alors $\det(A) = \det(B)$.
- 2.

- (a) Soit A une matrice hermitienne définie positive appartenant à $\mathcal{M}_n(S)$. Montrer qu'il existe un entier $m(A) > 0$ et un élément z appartenant à S^n dont les composantes sont premières entre elles tels que l'on ait :

$$m(A) = \inf_{x \in S^n \setminus \{0\}} xAx^* = zAz^*.$$

- (b) A-t-on toujours $m(A) = m(B)$ lorsque A et B sont congruentes ?
- (c) Déterminer $m(A)$ lorsque $S = \mathbb{Z}$ et :

$$A = \begin{pmatrix} 2 & 7 \\ 7 & 25 \end{pmatrix}.$$

A. Le cas $n = 2$

Soit A une matrice hermitienne définie positive appartenant à $\mathcal{M}_2(S)$ et soit z un élément de S^2 tel que $m(A) = zAz^*$.

1.

- (a) Montrer que ${}^t z$ est vecteur colonne d'une matrice inversible U_0 de $GL(2, S)$ et en déduire l'existence d'une matrice hermitienne $B = (b_{ij})$, $1 \leq i, j \leq 2$, où $b_{11} = m(A)$, telle que A et B soient congruentes.
- (b) Montrer qu'il existe $s \in S$ tel que :

$$|b_{11}s + b_{12}| \leq k^{\frac{1}{2}} b_{11}$$

et en déduire l'existence d'une matrice

$$C = \begin{pmatrix} a & b \\ \bar{b} & c \end{pmatrix}$$

congruente à A , qui vérifie les deux conditions :

- i. $a = m(A) = m(C)$;
- ii. $k^{-\frac{1}{2}} |b| \leq a \leq c$.

- (c) Montrer que si $A \in \mathcal{M}_2(S)$ est une matrice hermitienne définie positive de déterminant égal à d , alors on a :

$$m(A) \leq (1 - k)^{-\frac{1}{2}} d^{\frac{1}{2}}.$$

- (d) En déduire la finitude de l'ensemble des classes de congruence de matrices hermitiennes d'ordre 2 à coefficients dans S , définies positives, de déterminant donné.

2.

- (a) On suppose que $d = 1$ et que S est l'un des anneaux suivants :

$$S = \mathbb{Z}, \quad S = \mathbb{Z}[\omega_D] \quad \text{pour } D = 1, 3, 7.$$

Montrer alors que $m(A) = 1$ et qu'il existe $B \in GL(2, S)$ telle que $A = B^*B$.

- (b) En déduire les propriétés suivantes :

- i. Tout nombre premier est somme de quatre carrés (théorème de Lagrange).
- ii. Quel que soit le nombre premier p , il existe des entiers relatifs a, b, c, d tels que :

$$p = a^2 + ab + b^2 + c^2 + cd + d^2.$$

- iii. Quel que soit le nombre premier p , il existe des entiers relatifs a, b, c, d tels que :

$$p = a^2 + ab + 2b^2 + c^2 + cd + 2d^2.$$

B. Matrices symétriques à coefficients entiers

1.

- (a) soit $f : \mathbb{Z}^n \rightarrow \mathbb{Z}$ un homomorphisme surjectif de groupes abéliens, et soit $x \in \mathbb{Z}^n$ tel que $f(x) = 1$. Montrer que \mathbb{Z}^n est la somme directe du sous-groupe engendré par x et du noyau de f .

- (b) Soit $x = (x_1, \dots, x_n)$ un élément de \mathbb{Z}^n . Montrer que les conditions suivantes sont équivalentes :

i. x appartient à une base de \mathbb{Z}^n .

ii. Il existe $M \in GL(n, \mathbb{Z})$ admettant ${}^t x$ comme vecteur colonne.

iii. Il existe des entiers relatifs $a_i, 1 \leq i \leq n$, tels que $\sum_{i=1}^n a_i x_i = 1$.

iv. Il existe $f : \mathbb{Z}^n \rightarrow \mathbb{Z}$ homomorphisme surjectif de groupes abéliens tel que $f(x) = 1$.

2. Soit A une matrice symétrique d'ordre $n > 1$ définie positive à coefficients dans \mathbb{Z} . Montrer l'existence d'une matrice $B = (b_{ij}), 1 \leq i, j \leq n$, congruente à A et telle que $b_{11} = m(A)$.

3. Soit $A = (a_{ij}), 1 \leq i, j \leq n$ une matrice symétrique définie positive à coefficients dans \mathbb{Z} telle que $m(A) = a_{11}$. Si $x = (x_1, \dots, x_n)$ est un élément de \mathbb{Z}^n , on définit l'élément $y = (y_1, \dots, y_n)$ par les relations suivantes :

$$\begin{cases} y_1 = x_1 + \sum_{i=2}^n a_{1i} a_{11}^{-1} x_i, \\ y_i = x_i \text{ pour } 2 \leq i \leq n. \end{cases}$$

On pose :

$$z = (x_2, \dots, x_n), \quad {}^t y = U {}^t x.$$

(a) Montrer que l'on a :

$$xA^t x = a_{11}y_1^2 + a_{11}^{-1}zB^t z,$$

où B est une matrice symétrique définie positive appartenant à $\mathcal{M}_{n-1}(\mathbb{Z})$ et qui vérifie les deux relations :

$$\begin{cases} A = {}^tU \begin{pmatrix} a_{11} & 0 \\ 0 & a_{11}^{-1}B \end{pmatrix} U, \\ \det(B) = (a_{11})^{n-2} \det(A). \end{cases}$$

(b) Montrer que l'on a :

$$m(A) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} (\det(A))^{\frac{1}{n}}.$$

On choisira x de telle sorte que l'on ait :

$$|y_1| \leq \frac{1}{2}, \quad zB^t z = m(B).$$

4.

(a) On suppose $n \leq 5$ et soit $A \in \mathcal{M}_n(\mathbb{Z})$ une matrice symétrique définie positive dont le déterminant est égal à 1. Montrer que $m(A) = 1$ et en déduire qu'il existe $B \in \mathcal{M}_n(\mathbb{Z})$ telle que $A = {}^tBB$.

(b) Montrer que tout nombre premier de la forme $8n + 1$ ou $8n + 3$ est somme de trois carrés.

– III – Classes d'idéaux et anneaux principaux

On rappelle que deux éléments A et B de $\mathcal{M}_n(\mathbb{Z})$ sont semblables s'il existe $Q \in GL(n, \mathbb{Z})$ telle que $A = QBQ^{-1}$; les classes d'équivalence pour cette relation sont appelées classes de similitude.

Soit $P(X)$ un polynôme unitaire de degré $n > 1$, à coefficients dans \mathbb{Z} et irréductible sur $\mathbb{Q}[X]$. Si θ est une racine complexe de P , on note $\mathbb{Z}[\theta]$ le sous-anneau de \mathbb{C} , ensemble des éléments de la forme :

$$\sum_{i=0}^{n-1} a_i \theta^i \text{ où } a_i \in \mathbb{Z} \text{ pour } i = 0, 1, \dots, n-1.$$

On dit que deux idéaux I et J de $\mathbb{Z}[\theta]$ appartiennent à la même classe s'il existe deux éléments non nuls a et b de $\mathbb{Z}[\theta]$ tels que $aI = bJ$. A désigne un élément de $\mathcal{M}_n(\mathbb{Z})$ tel que $P(A) = 0$.

1. Montrer que tout idéal non nul de $\mathbb{Z}[\theta]$ est un groupe abélien libre de rang n .

2.

(a) Montrer qu'il existe $x = (x_1, \dots, x_n)$ élément de $\mathbb{Z}[\theta]^n \setminus \{0\}$ tel $A^t x = \theta^t x$.

(b) Montrer que $\mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$ est un idéal de $\mathbb{Z}[\theta]$ dont la classe est indépendante du vecteur propre ${}^t x$ choisi.

On notera I_A la classe de l'idéal $\mathbb{Z}x_1 + \dots + \mathbb{Z}x_n$.

(c) Soit Q un élément de $GL(n, \mathbb{Z})$. Montrer que $I_A = I_{QAQ^{-1}}$.

3. Soit $J = \mathbb{Z}y_1 + \cdots + \mathbb{Z}y_n$ un idéal non nul de $\mathbb{Z}[\theta]$. On pose $y = (y_1, \cdots, y_n)$. Montrer qu'il existe une matrice B à coefficients entiers telle que $B^t y = \theta^t y$, $P(B) = 0$.
4. Montrer qu'il existe une bijection entre l'ensemble des classes de similitude des matrices A , éléments de $\mathcal{M}_n(\mathbb{Z})$ telles que $P(A) = 0$, et l'ensemble des classes d'idéaux non nuls de $\mathbb{Z}[\theta]$.
5. Montrer que les conditions suivantes sont équivalentes :
 - (a) $\mathbb{Z}[\theta]$ est un anneau principal.
 - (b) Il existe une seule classe de similitude dans $\mathcal{M}_n(\mathbb{Z})$ de matrices A d'ordre n à coefficients entiers telles que $P(A) = 0$.

Agrégation externe 1990, épreuve 1

Notations et définitions

Tout espace vectoriel de dimension finie sur \mathbb{R} est muni de la topologie associée à l'une quelconque de ses normes.

Si \mathcal{V} est un espace vectoriel réel euclidien de dimension finie, on note $(x | y)$ le produit scalaire de deux vecteurs x et y de \mathcal{V} et $\|x\| = \sqrt{(x | x)}$ la norme euclidienne de x .

On associe à toute famille (x_1, x_2, \dots, x_k) de \mathcal{V} sa matrice de Gram, $G(x_1, x_2, \dots, x_k)$ définie par :

$$G(x_1, x_2, \dots, x_k) = ((x_i | x_j)).$$

On note Id l'application linéaire identité de \mathcal{V} .

fg désigne la composée $f \circ g$ de deux éléments de $\mathcal{L}(\mathcal{V})$, et on définit f^k , pour tout k de \mathbb{N} , par :

$$f^0 = Id \text{ et } \forall k \in \mathbb{N}, \quad f^{k+1} = f^k \circ f.$$

On munit $\mathcal{L}(\mathcal{V})$ de la norme usuelle d'opérateurs déduite de celle de \mathcal{V} .

Si f appartient à $\mathcal{L}(\mathcal{V})$, χ_f désigne le polynôme caractéristique de f ($\chi_f(T) = \det(TId - f)$).

On note $\rho(f)$ le rayon spectral de f .

On note f^* l'opérateur adjoint de f .

On définit les sous-ensembles suivants de $\mathcal{L}(\mathcal{V})$:

- $\mathcal{B}(\mathcal{V}) = \{f \in \mathcal{L}(\mathcal{V}) \mid \|f\| \leq 1\}$
- $\mathcal{B}_0(\mathcal{V}) = \{f \in \mathcal{B}(\mathcal{V}) \mid \rho(f) < 1\}$
- $\mathcal{C}(\mathcal{V}) = \{f \in \mathcal{B}(\mathcal{V}) \mid \text{rg}(Id - f^*f) \leq 1\}$
- $\mathcal{C}_0(\mathcal{V}) = \{f \in \mathcal{C}(\mathcal{V}) \mid \rho(f) < 1\}$.

On note $\mathcal{O}(\mathcal{V})$ le groupe orthogonal de \mathcal{V} .

On note $\mathcal{S}(\mathcal{V})$ l'espace vectoriel des endomorphismes symétriques de \mathcal{V} . On note $\mathcal{S}^+(\mathcal{V})$ la partie de $\mathcal{S}(\mathcal{V})$ constituée des endomorphismes symétriques positifs.

$\mathcal{M}_k(\mathbb{R})$ désigne l'ensemble des matrices carrées d'ordre k à coefficients réels. On note I_k la matrice identité d'ordre k .

On identifie \mathbb{R}^k avec l'ensemble des matrices colonnes à k lignes, et les éléments de $\mathcal{L}(\mathbb{R}^k)$ avec leur matrice dans la base canonique de \mathbb{R}^k notée (E_1, E_2, \dots, E_k) . \mathbb{R}^k est muni du produit scalaire canonique, de telle sorte que si A appartient à $\mathcal{M}_k(\mathbb{R})$, A^* s'identifie avec la matrice transposée de A .

On notera également X^* la matrice ligne transposée de la matrice colonne X de \mathbb{R}^k .

$\mathbb{R}[T]$ désigne l'algèbre des polynômes à une indéterminée T sur \mathbb{R} .

Si $P(T) = T^k - a_{k-1}T^{k-1} - \dots - a_1T - a_0$ est un polynôme unitaire de $\mathbb{R}[T]$, on appelle matrice compagnon de P la matrice C définie par :

$$C = \begin{pmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 & a_{k-2} \\ 0 & \cdots & 0 & 1 & a_{k-1} \end{pmatrix}.$$

Dans tout le problème, E désigne un espace euclidien de dimension $n \geq 1$.

– I – Préliminaires

A. Décomposition d'un élément de $\mathcal{S}(E)$

1. Soit f_u appartenant à $\mathcal{S}(E)$ défini par $f_u(x) = (u | x)u$ où u est un vecteur donné de E .
 - (a) Vérifier que f_u appartient à $\mathcal{S}^+(E)$.
 - (b) Préciser le rang de f_u .
 - (c) Reconnaitre f_u lorsque $\|u\| = 1$.
 - (d) Si \mathcal{B} est une base orthonormale de E , et si U est la matrice de u dans la base \mathcal{B} , vérifier que la matrice de f_u dans la base \mathcal{B} est UU^* .

Dans toute la suite du problème, on notera uu^* l'application f_u .

2. Soient u et v deux vecteurs de E ; à quelle condition a-t-on $uu^* = vv^*$?
3. Soit f appartenant à $\mathcal{S}(E)$. Montrer l'existence d'une base orthonormale (e_1, e_2, \dots, e_n) et d'un n -uplet $(\lambda_1, \lambda_2, \dots, \lambda_n)$ de réels tels que $f = \sum_{i=1}^n \lambda_i e_i e_i^*$. Que représentent pour f les λ_i et les e_i ? À quelle condition f est-elle dans $\mathcal{S}^+(E)$?
4. Soit f appartenant à $\mathcal{S}(E)$. Montrer que $f = 0$ si, et seulement si, $\forall x \in E, (x | f(x)) = 0$.
5. Soit f appartenant à $\mathcal{S}^+(E)$ et x un vecteur de E . Montrer que $f(x) = 0$ si, et seulement si, $(x | f(x)) = 0$.
6. Soit f appartenant à $\mathcal{L}(E)$. Montrer que f appartient à $\mathcal{S}^+(E)$ si, et seulement si, il existe n vecteurs (u_1, u_2, \dots, u_n) de E tels que $f = \sum_{i=1}^n u_i u_i^*$.

B. Caractérisation des éléments de $\mathcal{B}(E)$ et de $\mathcal{C}(E)$

1. Soit f appartenant à $\mathcal{L}(E)$.

(a) Montrer que :

$$\forall x \in E, \quad \|f(x)\|^2 \leq \|x\| \|f^* f(x)\|.$$

En déduire que :

$$\forall x \in E, \quad \|f(x)\| \leq \|f^*\| \|x\|.$$

(b) Établir que $\|f\| = \|f^*\|$.

2. Soit f appartenant à $\mathcal{L}(E)$.

(a) Vérifier que $f^* f$ appartient à $\mathcal{S}^+(E)$.

(b) Montrer que f appartient à $\mathcal{B}(E)$ si, et seulement si, $Id - f^* f$ appartient à $\mathcal{S}^+(E)$.

3. Soit f appartenant à $\mathcal{B}(E)$. Notons :

$$E_f = \{x \in E \mid \|f(x)\| = \|x\|\},$$

$$E_f^* = \{x \in E \mid \|f^*(x)\| = \|x\|\}.$$

- (a) Montrer que $\|f\| = 1$ si, et seulement si, $E_f \neq \{0\}$.
 (b) Montrer que $E_f = \ker(Id - f^*f)$, $E_f^* = \ker(Id - ff^*)$.
 (c) Établir les égalités suivantes :

$$f(E_f) = E_f^*, \quad f^*(E_f^*) = E_f \quad \text{et} \quad \dim(E_f^*) = \dim(E_f).$$

4. Soit f appartenant à $\mathcal{L}(E)$. Vérifier que f appartient à $\mathcal{C}(E)$ si, et seulement si, f^* appartient à $\mathcal{C}(E)$, et que f appartient à $\mathcal{C}_0(E)$ si, et seulement si, f^* appartient à $\mathcal{C}_0(E)$.
 5. Soit f appartenant à $\mathcal{L}(E)$. Montrer que les propriétés suivantes sont équivalentes :
 i. f appartient à $\mathcal{C}(E)$;
 ii. il existe u appartenant à E tel que $Id - f^*f = uu^*$;
 iii. il existe u appartenant à E tel que $\forall x \in E, \|x\|^2 - \|f(x)\|^2 = (u \mid x)^2$.

C. Propriétés des matrices compagnons

Calculer en fonction de P , polynôme unitaire de $\mathbb{R}[T]$, le polynôme caractéristique et le polynôme minimal de C , matrice compagnon de P .

- II -

Le but de cette partie est de déterminer les matrices triangulaires inférieures qui sont dans $\mathcal{C}(\mathbb{R}^n)$ et, si A est l'une de ces matrices, de trouver U appartenant à \mathbb{R}^n tel que $I_n - A^*A = UU^*$.

1. Soit $A = \begin{pmatrix} \lambda & 0 \\ \nu & \mu \end{pmatrix}$ appartenant à $\mathcal{C}(\mathbb{R}^2)$. Vérifier que $\nu^2 = (1 - \lambda^2)(1 - \mu^2)$. En déduire que les matrices triangulaires inférieures de $\mathcal{C}(\mathbb{R}^2)$ s'écrivent :

$$A = \begin{pmatrix} \cos(\alpha) & 0 \\ -\sin(\alpha)\sin(\beta) & \cos(\beta) \end{pmatrix},$$

avec α et β réels quelconques ; trouver alors U de \mathbb{R}^2 tel que $I_2 - A^*A = UU^*$.

2. On suppose $n \geq 2$. Soit $A = (a_{ij})$ de $\mathcal{M}_n(\mathbb{R})$ telle que $a_{in} = 0$ pour tout i vérifiant $1 \leq i \leq n-1$, et $U = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ de \mathbb{R}^n . On écrit $A = \begin{pmatrix} B & 0 \\ C^* & a_{nn} \end{pmatrix}$ et $U = \begin{pmatrix} W \\ b_n \end{pmatrix}$, avec

B appartenant à $\mathcal{M}_{n-1}(\mathbb{R})$, C et W matrices colonnes de \mathbb{R}^{n-1} .

Montrer que $I_n - A^*A = UU^*$ si, et seulement si, il existe θ_n de \mathbb{R} et V de \mathbb{R}^{n-1} vérifiant les égalités suivantes :

$$a_{nn} = \cos(\theta_n), \quad b_n = \sin(\theta_n), \quad C = -\sin(\theta_n)V, \quad W = \cos(\theta_n)V, \quad I_{n-1} - B^*B = VV^*.$$

3. En déduire la forme générale des matrices triangulaires inférieures de $\mathcal{C}(\mathbb{R}^n)$ et préciser pour chacune d'entre elles un élément U de \mathbb{R}^n tel que $I_n - A^*A = UU^*$.

– III – Étude de $\mathcal{B}(E)$ et de $\mathcal{C}_0(E)$

Dans toute cette partie **III**, f appartient à $\mathcal{B}(E)$, E_f et F sont définis par :

$$\begin{cases} E_f = \{x \in E \mid \|f(x)\| = \|x\|\}, \\ F = \{x \in E \mid \forall k \in \mathbb{N}, f^k(x) \in E_f\}, \end{cases}$$

et on note G l'orthogonal de F dans E .

A. Décomposition d'un élément de $\mathcal{B}(E)$

1. Établir les propriétés suivantes :

- (a) F est un sous-espace vectoriel de E ;
- (b) $f(F) = F$ et $f^*(F) = F$;
- (c) $f(G) \subset G$.

2. On note $\varphi = f|_F$ et $\psi = f|_G$, les endomorphismes de F et G induits par f .

- (a) Montrer que ψ appartient à $\mathcal{B}(G)$.
- (b) Montrer que φ appartient à $\mathcal{O}(F)$.
- (c) Soit x appartenant à E . On suppose que x n'appartient pas à F et on appelle k le plus petit entier naturel tel que $f^k(x)$ n'appartient pas à E_f . Montrer que la famille $(x, f(x), \dots, f^k(x))$ est une famille libre de E . En déduire que $\|f^n(x)\| < \|x\|$.
- (d) Montrer que ψ appartient à $\mathcal{B}_0(G)$.

3. Établir l'équivalence des trois propriétés suivantes :

- i. $F = \{0\}$;
- ii. $\|f^n\| < 1$;
- iii. f appartient à $\mathcal{B}_0(E)$.

B. Caractérisation des éléments de $\mathcal{C}_0(E)$

1. On suppose dans cette question que f appartient à $\mathcal{C}(E)$ et que u est un vecteur de E tel que $Id - f^*f = uu^*$.

(a) Montrer que x appartient à F si, et seulement si :

$$(x \mid u) = (f(x) \mid u) = \dots = (f^{n-1}(x) \mid u) = 0.$$

(b) En déduire que f appartient à $\mathcal{C}_0(E)$ si, et seulement si, $(u, f^*(u), \dots, (f^*)^{n-1}(u))$ est une base de E .

2. On suppose dans cette question que f appartient à $\mathcal{C}_0(E)$. Montrer qu'il existe x appartenant à $E \setminus \{0\}$ tel que $\|x\| = \|f(x)\| = \dots = \|f^{n-1}(x)\|$. En déduire que $\|f^k\| = 1$ pour tout k de $\{0, 1, \dots, n-1\}$ et $\|f^n\| < 1$.

3. Réciproquement, on suppose que f vérifie $\|f^k\| = 1$ pour tout k de $\{0, 1, \dots, n-1\}$ et $\|f^n\| < 1$. Soit x non nul tel que $\|x\| = \|f^{n-1}(x)\|$, montrer que $(x, f(x), \dots, f^{n-1}(x))$ est une base de E et que f appartient à $\mathcal{C}_0(E)$.

C. Étude d'une base adaptée de $\mathcal{C}_0(E)$ et de sa matrice de Gram

On suppose dans toute la fin de cette partie **III** que f est un élément de $\mathcal{C}_0(E)$ et on note C la matrice compagnon de son polynôme caractéristique.

1. Montrer que l'on peut trouver v_1 appartenant à E tel que :

$$\|f^{n-1}(v_1)\| = \|v_1\| \text{ et } \|v_1\|^2 - \|f^n(v_1)\|^2 = 1.$$

On pose alors $v_2 = f(v_1)$, $v_3 = f^2(v_1)$, \dots , $v_n = f^{n-1}(v_1)$. Vérifier que (v_1, v_2, \dots, v_n) est une base de E . Donner la matrice de f dans cette base.

2. On appelle Ω la matrice de Gram $G(v_1, v_2, \dots, v_n)$.
- (a) Montrer que $C^*\Omega C = G(f(v_1), f(v_2), \dots, f(v_n))$.
- (b) En déduire que $\Omega - C^*\Omega C = E_n E_n^*$.

Dans toute la fin du problème, P désigne un polynôme unitaire de $\mathbb{R}[T]$, de degré n dont toutes les racines réelles ou complexes sont de module strictement inférieur à 1, et C est sa matrice compagnon.

– IV – Résolution dans $\mathcal{M}_n(\mathbb{R})$ de l'équation à l'inconnue $G : G - C^*GC = H$

1. Soit A appartenant à $\mathcal{M}_n(\mathbb{R})$ telle que $A = C^*AC$. Montrer que $A = 0$.
2. Soit B appartenant à $\mathcal{M}_n(\mathbb{R})$.
- (a) Montrer qu'il existe une unique matrice A dans $\mathcal{M}_n(\mathbb{R})$ telle que $A - C^*AC = B$.
- (b) Établir que $A = \sum_{p=0}^{+\infty} (C^*)^p B C^p$.
3. Soit H appartenant à $\mathcal{S}^+(\mathbb{R}^n)$, et G de $\mathcal{M}_n(\mathbb{R})$ vérifiant $G - C^*GC = H$.
- (a) Montrer que G appartient à $\mathcal{S}^+(\mathbb{R}^n)$.
- (b) Établir que les propriétés suivantes sont équivalentes :
- X appartient à $\ker(G)$;
 - $\forall k \in \mathbb{N}$, $C^k X \in \ker(H)$;
 - $HX = HCX = \dots = HC^{n-1}X = 0$.
4. Soit U appartenant à \mathbb{R}^n et G de $\mathcal{M}_n(\mathbb{R})$ tels que $G - C^*GC = UU^*$. Montrer que G est définie positive si, et seulement si, l'une des deux conditions suivantes est réalisée :
- $\forall X \in \mathbb{R}^n$, $(X | U) = (CX | U) = \dots = (C^{n-1}X | U) = 0 \Rightarrow X = 0$;
 - $(U, C^*U, \dots, (C^*)^{n-1}U)$ est une base de \mathbb{R}^n .
5. Soit Ω appartenant à $\mathcal{M}_n(\mathbb{R})$ telle que $\Omega - C^*\Omega C = E_n E_n^*$.
- (a) Établir que Ω est définie positive.
- (b) U étant un élément quelconque de \mathbb{R}^n , et G la matrice de $\mathcal{M}_n(\mathbb{R})$ telle que :

$$G - C^*GC = UU^*,$$

montrer qu'il existe un unique polynôme Q de $\mathbb{R}[T]$ vérifiant $\deg(Q) \leq n - 1$ et $U = (Q(C))^* E_n$. En déduire que $G = (Q(C))^* \Omega Q(C)$.

- (c) G étant un élément de $\mathcal{M}_n(\mathbb{R})$, prouver que $G - C^*GC$ appartient à $\mathcal{S}^+(\mathbb{R}^n)$ si, et seulement si, il existe n polynômes Q_1, \dots, Q_n appartenant à $\mathbb{R}[T]$, tels que
- $$G = \sum_{i=1}^n (Q_i(C))^* \Omega Q_i(C).$$

Agrégation externe 1991, épreuve 1

Pour tout a élément de \mathbb{C} et pour tout r élément de $[0, +\infty[$, on note $D(a, r)$ le disque fermé de centre a et de rayon r :

$$D(a, r) = \{z \in \mathbb{C} \mid |z - a| \leq r\}.$$

A. Théorème de Gauss-Lucas, séries lacunaires

– I – Le théorème de Gauss-Lucas

1. *Enveloppe convexe d'une partie d'un espace affine réel E*

- Montrer qu'une intersection de parties convexes de E est convexe, éventuellement vide.
- Si A est une partie de E , montrer l'existence et l'unicité de $C(A)$, partie convexe de E , telle que, pour tout convexe K de E , $A \subset K$ équivaut à $C(A) \subset K$.
 $C(A)$ est appelée l'enveloppe convexe de A .
- Si $A = \{M_1, M_2, \dots, M_n\}$, où les M_i sont des points de E , montrer que $C(A)$ est le barycentre des systèmes (λ_i, M_i) tels que $\sum_{i=1}^n \lambda_i \neq 0$ et, $\lambda_i \geq 0$.

2. *Le théorème de Gauss-Lucas*

Soit $P(X) = c \prod_{i=1}^n (X - \alpha_i)^{n_i}$ un polynôme complexe non constant où les nombres complexes α_i sont deux à deux distincts et c est dans \mathbb{C} .

- Décomposer en éléments simples la fraction rationnelle $\frac{P'}{P}$.
- Soit z un zéro de P' tel que $P(z) \neq 0$. Prouver l'égalité $\sum_{i=1}^n n_i \frac{z - \alpha_i}{|z - \alpha_i|^2} = 0$.
- Montrer que l'ensemble des zéros de P' est inclus dans l'enveloppe convexe de l'ensemble des zéros de P . Ce résultat constitue le théorème de Lucas.

3. *Application à la localisation des zéros dans un disque*

Montrer que si tous les zéros d'un polynôme P sont de module inférieur ou égal au réel strictement positif R , il en est de même pour les zéros de P' .

– II – Surjectivité des fonctions définies par une série lacunaire

Dans tout le problème si $(n_k)_{k \in \mathbb{N}}$ est une suite strictement croissante de \mathbb{N} telle que la série $\sum_{k=1}^{+\infty} \frac{1}{n_k}$ converge et $(a_k)_{k \in \mathbb{N}}$ une suite de nombres complexes non nuls, on dira que la série entière $\sum_{k=0}^{+\infty} a_k z^{n_k}$ est lacunaire.

On suppose dans les questions **1.** et **2.** de cette partie **A. II.** que $n_0 = 0$, $n_1 = 1$, $a_0 = 1$, $a_1 = -1$, et que la série entière lacunaire $1 - z + \sum_{k=2}^{+\infty} a_k z^{n_k}$ converge pour tout z élément de \mathbb{C} .

On note $f(z)$ la somme de cette série. Pour tout d entier supérieur ou égal à 1, on note P_d , Q_d , R_d les trois polynômes suivants :

$$P_d(X) = \sum_{k=0}^d a_k X^{n_k}, \quad Q_d(X) = X^{n_d} P_d\left(\frac{1}{X}\right), \quad R_d(X) = X^{n_d-1} Q'_d\left(\frac{1}{X}\right).$$

1. *Borne du module d'un zéro du polynôme P*

- Calculer les coefficients du polynôme R_d .
- Soit ρ un réel strictement positif, montrer que si P_d n'a pas de zéros dans $D(0, \rho)$, R_d n'en a pas non plus.
- Montrer, par récurrence sur d , que P_d a au moins un zéro de module inférieur ou égal à ρ_d où $\rho_1 = 1$ et $\rho_d = \prod_{k=2}^d \frac{n_k}{n_k - 1}$ si $d \geq 2$.

Indication – On pourra considérer le polynôme S tel que $R_d(X) = n_d S\left(\frac{n_d - 1}{n_d} X\right)$.

2. *Existence d'un zéro de f*

- Montrer l'existence d'un réel M vérifiant :

$$\forall d \in \mathbb{N}^*, \quad \exists z \in \mathbb{C}, \quad (P_d(z) = 0 \text{ et } |z| \leq M).$$

- Montrer que l'application f s'annule au moins une fois dans \mathbb{C} .

3. *Surjectivité de certaines sommes de séries lacunaires*

Montrer que si g est la somme d'une série entière lacunaire de rayon de convergence infini et si $g'(0) \neq 0$ alors l'application $g : \mathbb{C} \rightarrow \mathbb{C}$ est surjective.

B. Localisation des zéros d'un polynôme

Dans cette partie **B**, on considère n un entier supérieur ou égal à 1.

Pour A élément de l'algèbre $\mathcal{M}_n(\mathbb{C})$ des matrices carrées complexes d'ordre n , dont le coefficient de ligne i et colonne j est noté A_{ij} , on pose :

$$L_i = |A_{ii}| - \sum_{\substack{j \neq i \\ j=1}}^n |A_{ij}|, \quad \alpha = \min \{L_i \mid i = 1, \dots, n\}.$$

$\mathcal{M}_{n,1}(\mathbb{C})$ l'espace des matrices colonnes à n éléments, est muni de la norme $\|\cdot\|$ définie par :

$$\|X\| = \max \{|x_i| \mid i = 1, \dots, n\},$$

les nombres x_i étant les éléments de la matrice colonne X .

1. Localisation des valeurs propres d'une matrice

(a) Dans cette question (a) uniquement, on suppose que α est strictement positif.

Montrer que :

$$\forall X \in \mathcal{M}_{n,1}(\mathbb{C}), \quad \|AX\| \geq \alpha \|X\|.$$

En déduire que A est inversible.(b) On ne fait plus d'hypothèse sur α . Montrer que toute valeur propre de A est incluse dans :

$$\bigcup_{i=1}^n D \left(A_{ii}, \sum_{\substack{j \neq i \\ j=1}}^n |A_{ij}| \right).$$

2. Application aux polynômes

Soit $P(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$. En étudiant la matrice :

$$A = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & 0 \\ 0 & \dots & \dots & 0 & 0 & 1 \\ -a_0 & -a_1 & \dots & \dots & -a_{n-2} & -a_{n-1} \end{pmatrix},$$

montrer que tout zéro de P est dans l'ensemble :

$$D(0, 1) \cup D \left(-a_{n-1}, \sum_{j=0}^{n-2} |a_j| \right).$$

3. Nombre de zéros d'un polynôme situés dans un disque donné

Soit D un disque de rayon non nul et de frontière le cercle Γ , orienté dans le sens direct, et P un polynôme ne s'annulant pas sur Γ .Montrer que le nombre de zéros de P , comptés avec leur multiplicité, qui sont situés dans D est égal à l'intégrale :

$$\frac{1}{2i\pi} \int_{\Gamma} \frac{P'(z)}{P(z)} dz.$$

C. Le théorème de Grace

Dans cette partie **C**, p étant un élément de \mathbb{N}^* , on note $\mathbb{C}_p[X]$ l'espace des polynômes à coefficients complexes de degré au plus p , et on définit la forme bilinéaire d'apolarité, G_p , sur $\mathbb{C}_p[X]$ par :

$$\forall (P, Q) \in (\mathbb{C}_p[X])^2, \quad G_p(P, Q) = \sum_{k=0}^p (-1)^k P^{(k)}(0) Q^{(p-k)}(0).$$

$GL_2(\mathbb{C})$ désigne le groupe multiplicatif des matrices inversibles d'ordre 2 à coefficients complexes.

Dans cette partie **C**, n est un élément fixe de \mathbb{N}^* .

On appelle sphère de Riemann l'ensemble, noté S , obtenu en adjoignant au plan complexe \mathbb{C} un point noté ∞ .

S est donc l'ensemble $\mathbb{C} \cup \{\infty\}$.

Les opérations de \mathbb{C} sont, en partie, prolongées à S par :

- pour $a \in \mathbb{C}$, $a + \infty = \infty + a = \infty$ et $\frac{a}{\infty} = 0$; $\infty \times \infty = \infty$;
- pour $a \in \mathbb{C}^*$, $a \times \infty = \infty \times a = \infty$ et $\frac{\infty}{a} = \infty$.

N. B. $\infty + \infty$, $0 \times \infty$, $\frac{\infty}{\infty}$, $\frac{0}{0}$ n'ont pas de sens dans S .

1. Action de $GL_2(\mathbb{C})$ sur la sphère de Riemann

Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, matrice complexe inversible, on définit l'homographie associée :

$$H_A : S \rightarrow S, \text{ par } H_A(z) = \frac{az + b}{cz + d} \text{ pour } z \text{ dans } \mathbb{C} \text{ et } H_A(\infty) = \frac{a}{c}.$$

On rappelle que l'ensemble \mathbb{H} des homographies de S est un sous-groupe du groupe des bijections de S sur elle-même et que l'application $A \mapsto H_A$ est un morphisme surjectif du groupe $GL_2(\mathbb{C})$ sur le groupe \mathbb{H} .

- (a) Déterminer le noyau de ce morphisme.
- (b) Montrer que $GL_2(\mathbb{C})$ est engendré par l'ensemble des matrices :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} k & 0 \\ 0 & 1 \end{pmatrix} \text{ où } k \text{ décrit } \mathbb{C}^*.$$

Indication – On pourra utiliser des opérations élémentaires sur les lignes ou les colonnes.

- (c) En déduire une partie génératrice de \mathbb{H} .

2. Géométrie de la sphère de Riemann

\mathbb{C} est muni de sa structure affine euclidienne usuelle. On appellera :

- S -droite toute droite de \mathbb{C} complétée par ∞ ;
- S -cercle tout cercle de \mathbb{C} et toute droite de S ;
- S -disque fermé :
 - tout disque fermé de \mathbb{C} (de rayon strictement positif),
 - tout complémentaire d'un disque ouvert non vide de \mathbb{C} complété par ∞ ,
 - tout demi-plan fermé de \mathbb{C} complété par ∞ .

- (a) Montrer que l'image d'un S -cercle (respectivement d'un S -disque fermé) par une homographie est un S -cercle (respectivement un S -disque fermé).
- (b) Montrer que tout S -cercle est l'image du cercle unité de \mathbb{C} , $\Gamma_0 = \{z \in \mathbb{C} \mid |z| = 1\}$, par au moins une homographie et que tout S -disque fermé est l'image du disque unité de \mathbb{C} , $D_0 = \{z \in \mathbb{C} \mid |z| \leq 1\}$, par au moins une homographie.

3. Action de $GL_2(\mathbb{C})$ sur les polynômes et sur la forme d'apolarité

Pour P élément de $\mathbb{C}_n[X]$ et $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ élément de $GL_2(\mathbb{C})$, on définit l'élément $A(P)$ de $\mathbb{C}_n[X]$ par :

$$A(P)(X) = (-cX + a)^n P\left(\frac{dX - b}{-cX + a}\right).$$

- (a) Pour A et B dans $GL_2(\mathbb{C})$ et P dans $\mathbb{C}_n[X]$, montrer que $(AB)(P) = A(B(P))$.
- (b) Pour t nombre complexe, on considère la matrice $A_t = \begin{pmatrix} 1 & -t \\ 0 & 1 \end{pmatrix}$. Montrer que pour P et Q dans $\mathbb{C}_n[X]$ et t dans \mathbb{C} , on a :

$$G_n(P, Q) = G_n(A_t(P), A_t(Q)).$$

- (c) Montrer que pour tous P et Q dans $\mathbb{C}_n[X]$ et tout A dans $GL_2(\mathbb{C})$, $G_n(P, Q) = 0$ si, et seulement si, $G_n(A(P), A(Q)) = 0$.
Si P et Q appartiennent à $\mathbb{C}_n[X]$, on dira que P et Q sont apolaires lorsque $G_n(P, Q) = 0$.

4. Effet de l'action de $GL_2(\mathbb{C})$ sur les zéros des polynômes

Rappel – Les fonctions symétriques élémentaires sont définies par :

$$\sigma_p : \mathbb{C}^n \rightarrow \mathbb{C}, \quad \sigma_p(x_1, x_2, \dots, x_n) = \sum_{\substack{I \subset \{1, 2, \dots, n\} \\ \text{card}(I)=p}} \prod_{i \in I} x_i, \quad \text{pour } 1 \leq p \leq n,$$

$$\sigma_0(x_1, x_2, \dots, x_n) = 1.$$

Elles sont invariantes par permutations des x_i .

Notations – Si le degré de P , polynôme non nul, est $m \leq n$, on dira que ∞ est zéro de multiplicité $n - m$ de P .

Pour P élément de $\mathbb{C}_n[X]$ on appellera zéro dans S de P les nombres complexes z , tels que $P(z) = 0$ et ∞ si P est de degré strictement inférieur à n .

On prolonge à S les fonctions symétriques élémentaires en gardant l'invariance par permutation et en posant, pour $(x_1, x_2, \dots, x_{n-k})$ élément de \mathbb{C}^{n-k} :

$$\sigma_p(x_1, x_2, \dots, x_{n-k}, \infty, \dots, \infty) = \begin{cases} 0 & \text{si } p \leq k - 1, \\ \sigma_{p-k}(x_1, x_2, \dots, x_{n-k}) & \text{si } n \geq p \geq k. \end{cases}$$

- (a) Montrer que pour P élément non nul de $\mathbb{C}_n[X]$, (x_1, x_2, \dots, x_n) est la famille des zéros dans S de P , comptés avec leur multiplicité si, et seulement si, il existe un nombre complexe K non nul tel que :

$$P(X) = K \sum_{j=0}^n (-1)^j \sigma_j(x_1, x_2, \dots, x_n) X^{n-j}.$$

- (b) Soit P élément non nul de $\mathbb{C}_n[X]$ et A élément de $GL_2(\mathbb{C})$, montrer que la famille des zéros dans S de $A(P)$ est l'image par l'homographie H_A de celle des zéros dans S de P .

5. Le théorème de Grace

On considère P et Q , deux éléments apolaires de $\mathbb{C}_n[X]$, et on veut prouver que tout S -disque fermé contenant tous les zéros dans S de P contient au moins un zéro dans S de Q : ceci constitue le théorème de Grace. Pour cela, nous raisonnerons par l'absurde en supposant que $G_n(P, Q) = 0$ et qu'il existe un S -disque fermé contenant tous les zéros dans S de P et aucun des zéros dans S de Q .

- (a) Montrer que, quitte à modifier P et Q , on peut supposer que :
- Q est de degré strictement inférieur à n ;
 - il existe un disque fermé D , de \mathbb{C} , contenant tous les zéros dans S de P ;

- aucun des zéros dans S de Q n'appartient à D .
- (b) Sous les hypothèses du (a), montrer que $G_{n-1}(P', Q) = 0$.
- (c) Prouver la propriété annoncée pour tout $n \geq 1$ et tout couple (P, Q) de polynômes non nuls de $\mathbb{C}_n[X]$.

Agrégation externe 1995, épreuve 1

Notations et définitions

On désigne respectivement par $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ et \mathbb{C} , l'ensemble des entiers naturels, l'anneau des entiers relatifs, le corps des nombres rationnels, le corps des nombres réels et le corps des nombres complexes.

On désigne par $|z|$ le module du nombre complexe z . Si k et ℓ sont des entiers positifs ou nuls, avec $k \leq \ell$, on désigne par $\binom{\ell}{k}$ le coefficient binomial $\frac{\ell!}{k!(\ell-k)!}$. Par convention $0! = 1$. Soit A un anneau. Si p et q sont des entiers strictement positifs, $\mathcal{M}_{p,q}(A)$ désigne l'ensemble des matrices à p lignes et à q colonnes à coefficients dans A . Lorsque $p = q$, on allège la notation en $\mathcal{M}_p(A)$.

Soit $B \in \mathcal{M}_{p,q}(A)$. On désigne par tB la matrice transposée de B . Pour $p \geq 1$, on munit \mathbb{R}^p de sa structure euclidienne canonique, et on désigne par $\|\cdot\|$ la norme euclidienne :

$$\forall x = \begin{pmatrix} x_1 \\ \vdots \\ x_p \end{pmatrix} \in \mathbb{R}^p, \|x\| = \left(\sum_{i=1}^p x_i^2 \right)^{\frac{1}{2}}.$$

Soit $B \in \mathcal{M}_{p,q}(\mathbb{R})$. On munit \mathbb{R}^p et \mathbb{R}^q de leurs bases canoniques ; B détermine alors une application linéaire de \mathbb{R}^p vers \mathbb{R}^q , et on désigne par $\|B\|$ la norme de cette application linéaire pour la norme euclidienne sur \mathbb{R}^p et \mathbb{R}^q . Autrement dit :

$$\|B\| = \max_{\|x\|=1} \|Bx\|.$$

– I – Spectre des matrices positives

Définitions Soient m et n des entiers strictement positifs.

- (1) On dit qu'une matrice rectangulaire $A \in \mathcal{M}_{m,n}(\mathbb{C})$ est positive (resp. strictement positive) si tous ses coefficients sont des réels positifs ou nuls (resp. strictement positifs). En particulier, pour $n = 1$, on dit qu'un vecteur de \mathbb{C}^m est positif (resp. strictement positif) si toutes ses coordonnées sont des réels positifs ou nuls (resp. strictement positifs).

Mise en garde. On prendra garde à ne pas confondre cette notion avec celle de matrice d'un endomorphisme symétrique réel à valeurs propres positives.

- (2) On dit qu'une matrice carrée $A \in \mathcal{M}_n(\mathbb{C})$ est réductible s'il existe une matrice de permutation (c'est-à-dire une matrice possédant un seul coefficient non nul dans

chaque ligne et chaque colonne, ce coefficient valant 1) $P \in \mathcal{M}_n(\mathbb{C})$ telle que $P^{-1}AP$ soit de la forme :

$$\begin{pmatrix} B & 0 \\ C & D \end{pmatrix}$$

où B et D sont des matrices carrées, et 0 la matrice nulle de format correspondant. Autrement dit, A peut être mise sous cette forme en effectuant une permutation sur ses lignes et la même permutation sur ses colonnes.

(3) On dit qu'une matrice carrée est irréductible si elle n'est pas réductible.

1. Soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice carrée positive irréductible et soit $y \in \mathbb{C}^n$ un vecteur positif non nul.

(a) Soit $z = (I + A)y$. Montrer que z est un vecteur positif et que le nombre de coordonnées nulles de z , est strictement inférieur au nombre de coordonnées nulles de y .

(b) Montrer que toutes les coordonnées de $(I + A)^{n-1}y$ sont strictement positives.

(c) Montrer que la matrice $(I + A)^{n-1}$ est strictement positive.

2. Soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice carrée positive irréductible. On appelle $a_{i,j}$, $1 \leq i, j \leq n$ ses coefficients. Pour :

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n$$

on appelle $(Ax)_1, \dots, (Ax)_n$ les composantes du vecteur Ax .

(a) Soit :

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

un vecteur positif non nul. Soit $I \subset \{1, \dots, n\}$ l'ensemble des indices i tels que $x_i \neq 0$. On pose :

$$r(x) = \min_{i \in I} \frac{(Ax)_i}{x_i}.$$

Montrer que $r(x)$ est le plus grand réel ρ tel que :

$$\forall i = 1, \dots, n, \quad \rho x_i \leq (Ax)_i.$$

(b) Montrer que la restriction de la fonction r à l'ensemble Q^+ des vecteurs dont toutes les coordonnées sont strictement positives est continue.

(c) Soit :

$$E = \left\{ x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n \mid \forall i = 1, \dots, n, x_i \geq 0, \sum_{i=1}^n x_i^2 = 1 \right\}.$$

i. Montrer que l'image de E par $(I + A)^{n-1}$ est une partie compacte non vide de Q^+ . On note F cette image.

ii. Soit $x \in E$ et $y = (I + A)^{n-1}x$. Montrer que $r(x) \leq r(y)$.

- iii. Montrer que la fonction $x \mapsto r(x)$ définie sur E (resp. sur F) y atteint sa borne supérieure et que :

$$\max_{x \in E} r(x) = \max_{y \in F} r(y).$$

- iv. On appelle r la borne supérieure introduite en *iii*. Montrer que r est strictement positif.

On garde la notation introduite dans (c) *iv*. dans les questions (d), (e), (f) et (g).

- (d) Soit $z \in E$ tel que $r(z) = r$. Montrer que z est un vecteur propre de A , de valeur propre r .

Indication : On pourra considérer le vecteur $t = (I + A)^{n-1} z$ et montrer que si $Az - rz$ n'est pas nul, alors $At - rt$ est un vecteur strictement positif.

- (e) Montrer que si $z \in E$ satisfait à $r(z) = r$, alors toutes ses coordonnées sont strictement positives.

- (f) Soit α une valeur propre de A et :

$$y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbb{C}^n$$

un vecteur propre de valeur propre α . Soit :

$$y_+ = \begin{pmatrix} |y_1| \\ \vdots \\ |y_n| \end{pmatrix}.$$

Montrer que le vecteur $Ay_+ - |\alpha|y_+$ est positif, puis que $|\alpha| \leq r$.

- (g) Montrer que la dimension du sous-espace propre associé à la valeur propre r est 1.

Indication. On pourra commencer par montrer que pour tout vecteur propre y de valeur propre r , le vecteur y_+ défini comme ci-dessus est encore un vecteur propre de valeur propre r .

3. Soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice carrée positive irréductible. Montrer que A ne peut pas posséder deux vecteurs propres positifs linéairement indépendants.
4. Soit $A = (a_{i,j}) \in \mathcal{M}_n(\mathbb{C})$ une matrice carrée irréductible et $B = (b_{i,j}) \in \mathcal{M}_n(\mathbb{C})$ telle que :

$$\forall i, j \in \{1, \dots, n\} \quad |b_{i,j}| \leq a_{i,j}.$$

On appelle r la valeur propre positive de module maximal de A (cf. 2.).

- (a) Montrer que si γ est une valeur propre de B , alors $|\gamma| \leq r$.

- (b) On suppose de plus que B est positive et que $B \neq A$. Montrer que si γ est une valeur propre de B , alors $|\gamma| < r$.

5. Soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice carrée strictement positive (on notera que A est irréductible), et soit r la valeur propre positive de module maximal de A . Montrer que si α une autre valeur propre de A , on a alors $|\alpha| < r$.
6. Soit $A \in \mathcal{M}_n(\mathbb{C})$ une matrice positive telle qu'il existe un entier $p \geq 1$ tel que A^p soit strictement positive.

- (a) Montrer que A est irréductible.
Soit r sa valeur propre de module maximal.
- (b) Montrer que pour toute autre valeur propre α de A , on a $|\alpha| < r$.
7. On dit qu'une matrice rectangulaire $B \in \mathcal{M}_{m,n}(\mathbb{C})$ est non redondante si aucune de ses lignes ni aucune de ses colonnes n'est nulle.
Une matrice non redondante $B \in \mathcal{M}_{m,n}(\mathbb{C})$ est dite décomposable s'il existe des matrices de permutation $P \in \mathcal{M}_n(\mathbb{C})$ et $Q \in \mathcal{M}_m(\mathbb{C})$ telles que $P \cdot B \cdot Q$ soit de la forme :

$$\begin{pmatrix} B' & 0 \\ 0 & B'' \end{pmatrix}$$

où B' et B'' sont des matrices rectangulaires.

Une matrice rectangulaire B est dite indécomposable si elle est non redondante et n'est pas décomposable.

- (a) Soit $B \in \mathcal{M}_{m,n}(\mathbb{C})$ et posons :

$$C = \begin{pmatrix} 0 & B \\ {}^t B & 0 \end{pmatrix} \in \mathcal{M}_\ell(\mathbb{C}), \quad \text{avec } \ell = m + n.$$

Montrer que B est indécomposable si et seulement si C est irréductible.

- (b) Soit $B \in \mathcal{M}_{m,n}(\mathbb{R})$ une matrice à coefficients réels positifs ou nuls. Montrer que si B est indécomposable, alors $B^t B$ et ${}^t B B$ sont irréductibles et satisfont à la conclusion de 6. (b).

– II – Algèbre des matrices

Définitions, notations, rappels Soit \mathbb{K} un corps. On rappelle qu'une \mathbb{K} -algèbre associative avec unité est un \mathbb{K} -espace vectoriel $(A, +, \cdot)$ muni d'une structure d'anneau avec unité $(A, +, \times)$, tel que les lois de groupe abélien $(A, +)$ soient les mêmes pour les deux structures et que la loi de multiplication \times de la structure d'anneau soit une application \mathbb{K} -bilinéaire de $A \times A$ vers A . Soient A et B des algèbres associatives avec unité. Un morphisme d'algèbres de A vers B est une application \mathbb{K} -linéaire de A vers B qui est de plus un homomorphisme d'anneaux avec unité. Soit A une algèbre associative avec unité; une sous-algèbre de A est un sous-espace-vectoriel qui est aussi un sous-anneau qui possède le même élément unité que A . Dans la suite du problème, \mathbb{K} est \mathbb{R} ou \mathbb{C} , et, lorsque le contexte est clair, on parle simplement d'algèbre associative avec unité, ou même d'algèbre associative.

Soit A une algèbre associative, N une partie de A , a et b des éléments de A . On désigne par aNb l'ensemble des éléments de A de la forme anb , où n décrit N .

Soit A une algèbre associative. On dit qu'un élément p de A est idempotent s'il satisfait $p^2 = p$. Un idempotent central est un idempotent qui appartient au centre de A , c'est-à-dire qui commute avec tout élément de A . Soit n un entier supérieur ou égal à 2; on dit que les idempotents p_1, \dots, p_n sont orthogonaux s'ils vérifient : pour $i \neq j$, $p_i p_j = p_j p_i = 0$.

Soit M une algèbre de matrices (i.e. $M = \mathcal{M}_n(\mathbb{K})$, où \mathbb{K} est un corps) et S une partie de M . On appelle commutant de S dans M , et on note S' ou $C(S)$ l'ensemble $\{m \in M \mid ms = sm \quad \forall s \in S\}$.

On désigne par M l'algèbre $\mathcal{M}_n(\mathbb{C})$. Pour $1 \leq i, j \leq n$, on désigne par $E_{i,j}$ la matrice dont le seul coefficient non nul est celui situé à l'intersection de la i -ème ligne et de la j -ème colonne et vaut 1.

1. (a) Soit J un idéal bilatère non nul de M . Montrer que $J = M$.
Indication. Si $x \neq 0$ est dans J , on pourra considérer les éléments $E_{\ell,i}x E_{j,\ell}$, $1 \leq i, j, \ell \leq n$.
- (b) Quel est le centre de M ?
2. Soit V un espace vectoriel complexe de dimension finie m . On désigne par $\text{End}(V)$ l'algèbre des endomorphismes de V . Soit $\rho : M \rightarrow \text{End}(V)$ un morphisme d'algèbres avec unité.

- (a) Soit, pour $i = 1, \dots, n$, V_i l'image de $\rho(E_{i,i})$. Montrer que $V = \bigoplus_{i=1}^n V_i$.
- (b) Montrer que si $k \neq j$, la restriction de $\rho(E_{i,j})$ à V_k est nulle, et que la restriction de $\rho(E_{i,j})$ à V_j définit un isomorphisme de V_j sur V_i .
- (c) On pose $d = \dim(V_1)$, et on fixe une base (e_1, \dots, e_d) de V_1 . Pour tout $k = 1, \dots, d$, soit W_k le sous-espace vectoriel de V engendré par les éléments :

$$\rho(E_{1,1})e_k, \rho(E_{2,1})e_k, \dots, \rho(E_{n,1})e_k.$$

- i. Montrer que pour tout $k = 1, \dots, n$, W_k est un sous-espace vectoriel de dimension n , dont les éléments ci-dessus forment une base.
- ii. Montrer que $\forall x \in M$, $\rho(x)$ envoie W_k dans W_k . On notera alors $\rho_k(x)$ l'endomorphisme de W_k donné par la restriction de $\rho(x)$ à W_k .
- iii. Montrer que dans la base décrite au *i*. la matrice de $\rho_k(x)$ est x .
- iv. Montrer que $V = \bigoplus_{k=1}^d W_k$.
- v. Montrer que dans la base de V obtenue en écrivant à la suite les unes des autres les bases respectives de W_1, \dots, W_d évoquées au *i*. la matrice de $\rho(x)$ est la matrice diagonale par blocs :

$$\begin{pmatrix} x & 0 & \cdots & 0 \\ 0 & x & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & x \end{pmatrix}.$$

- (d) Soit $\rho : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_m(\mathbb{C})$ un morphisme d'algèbres avec unité. Montrer que ρ est injectif et que m est un multiple de n .
3. On conserve les notations du 2.
- (a) Soit A un endomorphisme de V qui commute avec tous les $\rho(x)$, $x \in M$. On considère sa matrice dans la base du 2. (c) v. que l'on décrit comme une matrice par blocs :

$$\begin{pmatrix} A_{11} & \cdots & A_{1d} \\ \vdots & \ddots & \vdots \\ A_{d1} & \cdots & A_{dd} \end{pmatrix}$$

où les $A_{i,j}$ sont des matrices carrées dans $\mathcal{M}_n(\mathbb{C})$. Montrer que chaque matrice $A_{i,j}$ est une matrice scalaire.

- (b) Montrer que l'ensemble des endomorphismes de V qui commutent avec tous les $\rho(x)$, $x \in M$, que l'on note $\rho(M)'$, est une sous-algèbre de $\text{End}(V)$ isomorphe à l'algèbre des matrices $\mathcal{M}_d(\mathbb{C})$, et que l'ensemble des endomorphismes de V qui commutent avec tous les éléments de $\rho(M)'$ est exactement $\rho(M)$.
4. Soient A_1, A_2, \dots, A_m des algèbres de matrices (i.e. chaque $A_j = \mathcal{M}_{n_j}(\mathbb{C})$ pour un entier $n_j \geq 1$). On rappelle que la formule suivante permet de munir le produit $N = A_1 \times A_2 \times \dots \times A_m$ d'une structure d'algèbre associative avec unité :

$$(a_1, \dots, a_m)(b_1, \dots, b_m) = (a_1 b_1, \dots, a_m b_m).$$

Pour $j = 1, \dots, m$, on note $i_j : A_j \rightarrow N$, $\pi_j : A_j \rightarrow N$ les applications données par :

$$\begin{aligned} i_j(a) &= (0, \dots, 0, a, 0, \dots, 0) \quad (a \text{ figure en position } j) \\ \pi_j(a_1, \dots, a_m) &= a_j. \end{aligned}$$

Ce sont des morphismes d'algèbres avec unité, respectivement injectif et surjectif. On identifiera A_j avec son image $i_j(A_j)$ dans N , si bien que $N = \bigoplus_{j=1}^m A_j$ et que π_j s'identifie à la j -ème projection de cette décomposition en somme directe. On dit que N est une somme directe d'algèbres de matrices.

Dans la suite, lorsque l'on considèrera une somme directe d'algèbres de matrices $\bigoplus_{j=1}^m A_j$, on la considèrera toujours munie de la structure d'algèbre associative avec unité provenant de l'identification de $\bigoplus_{j=1}^m A_j$ avec $A_1 \times A_2 \times \dots \times A_m$.

On note I_j l'élément unité de A_j , et p_j son image dans N par i_j .

- (a) Montrer que p_1, \dots, p_m sont des idempotents deux à deux orthogonaux, de somme égale à l'élément identité de N .
- (b) Déterminer le centre de N .
- (c) Déterminer les idempotents centraux de N .
- (d) On dit qu'un idempotent central p de N est minimal si pour tout autre idempotent central q de N tel que $pq \neq 0$, on a : $pq = qp = p$. Déterminer les idempotents centraux minimaux de N .
5. Soit $N = \bigoplus_{j=1}^m A_j$ comme au 4. et W un espace vectoriel complexe de dimension finie. Soit $\rho : N \rightarrow \text{End}(W)$ un morphisme d'algèbres avec unité supposé injectif.

- (a) Pour tout $j = 1, \dots, m$, on appelle W_j l'image de $\rho(p_j)$. Montrer que $W = \bigoplus_{j=1}^m W_j$.
- (b) Soit y un élément de $\rho(A_j)$. Montrer que pour $k \neq j$, y agit par 0 dans W_k , et que y envoie W_j dans lui-même.
Ceci permet, pour chaque $j = 1, \dots, m$, de considérer la restriction de ρ à A_j comme un morphisme de A_j dans $\text{End}(W_j)$, encore noté ρ .
- (c) Montrer que ce morphisme $A_j \rightarrow \text{End}(W_j)$ est injectif, et qu'il existe une base de W_j telle que, pour tout x dans A_j , la matrice de $\rho(x)$ dans cette base est une matrice diagonale par blocs :

$$\begin{pmatrix} x & 0 & \dots & 0 \\ 0 & x & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & x \end{pmatrix}.$$

On appelle d_j le nombre de blocs.

- (d) On note $C(N)$ l'ensemble des endomorphismes de W qui commutent à tous les $\rho(x)$, $x \in N$. Montrer que $C(N) = \bigoplus_{j=1}^m \rho(p_j) C(N) \rho(p_j)$.
- (e) Montrer que $C(N)$ est isomorphe à la somme directe d'algèbres de matrices $\bigoplus_{j=1}^m \mathcal{M}_{d_j}(\mathbb{C})$.
- (f) Montrer que l'ensemble des endomorphismes de W qui commutent à tout élément de $C(N)$ est $\rho(N)$.
6. Soit $A = \mathcal{M}_n(\mathbb{C})$, $B = \mathcal{M}_m(\mathbb{C})$ et $\rho : A \rightarrow B$ un morphisme d'algèbres avec unité ; ρ est donc injectif (cf. 2. (d)). Pour tout élément x de A , on note encore x son image $\rho(x)$ dans B .
- (a) Soit q un idempotent non nul de A .
- Montrer que qAq et qBq sont isomorphes à des algèbres de matrices.
 - Soit $C(A)$ le commutant de A dans B . Montrer que le commutant de qAq dans qBq est $qC(A)q$.
- (b) Soit q un idempotent non nul de A .
- Montrer que l'application de A dans qAq envoyant x sur qxq est un isomorphisme d'algèbres avec unité.
 - Montrer que le commutant de qAq dans qBq est $qC(A)q$.

– **III – Normes des matrices à coefficients entiers** Dans l'anneau $\mathbb{Z}[X_1, \dots, X_n]$ des polynômes à n indéterminées et à coefficients entiers, on désigne par $\sigma_1, \dots, \sigma_n$ les polynômes symétriques élémentaires, c'est-à-dire :

$$\sigma_1 = \sum_{i=1}^n X_i, \quad \sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j, \dots, \sigma_n = X_1 X_2 \cdots X_n.$$

On rappelle que si $P \in \mathbb{Z}[X_1, \dots, X_n]$ est un polynôme symétrique à coefficients entiers, alors il existe un polynôme Q à coefficients entiers tel que :

$$P(X_1, \dots, X_n) = Q(\sigma_1, \dots, \sigma_n).$$

Soit n un entier strictement supérieur à 1, et soient $\omega_1, \dots, \omega_\ell \in \mathbb{C}$ les racines primitives n -ème de l'unité. On pose :

$$Q_n(X) = \prod_{i=1}^{\ell} (X - \omega_i).$$

On rappelle que Q_n est un polynôme à coefficients entiers, qui est irréductible sur \mathbb{Z} .

On désigne par U l'ensemble des polynômes à coefficients entiers et de coefficient dominant égal à 1, c'est-à-dire l'ensemble des polynômes de la forme :

$$P(X) = X^\ell - a_1 X^{\ell-1} + \dots + (-1)^\ell a_\ell, \text{ avec } \forall i = 1, \dots, \ell, \quad a_i \in \mathbb{Z}.$$

1. (a) Soit $P \in U$. On suppose que toutes les racines complexes de P sont dans le disque fermé unité centré en 0. On pose $P(X) = X^\ell - a_1 X^{\ell-1} + \dots + (-1)^\ell a_\ell$. Montrer que :

$$\forall k = 1, \dots, \ell \quad |a_k| \leq \binom{\ell}{k}.$$

- (b) Soit ℓ un entier positif ou nul fixé. Montrer que l'ensemble des polynômes appartenant à U , de degré ℓ et dont toutes les racines complexes sont dans le disque fermé unité centré en 0 est un ensemble fini.
- (c) Soit P dans l'ensemble fini décrit au (b). On appelle μ_1, \dots, μ_ℓ ses racines complexes. Pour tout entier positif ou nul k , on définit un polynôme P_k par :

$$P_k(X) = \prod_{i=1}^{\ell} (X - \mu_i^k).$$

- i. Montrer que $\forall k \in \mathbb{N}$, P_k est un polynôme à coefficients entiers.
 - ii. Montrer qu'il existe deux entiers strictement positifs distincts j et k tels que $P_j = P_k$.
 - iii. En déduire que toutes les racines de P sont des racines de l'unité.
- (d) Soit P un élément de U . On suppose que toutes les racines complexes de P sont en fait réelles et contenues dans l'intervalle $[-2, 2]$. Montrer que ces racines sont de la forme $2 \cos(2\pi r)$, où r est rationnel.

Indication. On pourra considérer $Q(X) = X^\ell P\left(X + \frac{1}{X}\right)$ (où ℓ est le degré de P), montrer que Q est un élément de U et qu'on peut appliquer (c).

- (e) i. Soit n un entier strictement positif et $\omega \in \mathbb{C}$ une racine primitive n -ième de l'unité. Soit $\mathbb{L} \subset \mathbb{C}$ l'extension de \mathbb{Q} engendrée par ω . Soit $\rho \in \mathbb{C}$ une autre racine primitive n -ième de l'unité. Rappeler pourquoi il existe un automorphisme \mathbb{Q} -linéaire du corps \mathbb{L} qui envoie ω sur ρ .
- ii. Soit P un polynôme à coefficients entiers. On suppose que P possède une racine de la forme $\lambda = 2 \cos\left(2\pi \frac{p}{q}\right)$, où p et q sont deux entiers premiers entre eux. Montrer que $2 \cos\left(\frac{2\pi}{q}\right)$ est aussi une racine de P .
- iii. Soit P un élément de U , de degré ℓ , et différent de X^ℓ . On suppose que toutes ses racines $\lambda_1, \dots, \lambda_\ell$ sont réelles et dans l'intervalle ouvert $] -2, 2[$. Montrer qu'il existe un entier $q \geq 3$ tel que :

$$\max\{|\lambda_j|, j = 1, \dots, \ell\} = 2 \cos\left(\frac{\pi}{q}\right).$$

2. (a) Soient m et n des entiers strictement positifs. On pose $\ell = m+n$. Soit $B \in \mathcal{M}_{m,n}(\mathbb{R})$. On pose :

$$C = \begin{pmatrix} 0 & B \\ {}^t B & 0 \end{pmatrix} \in \mathcal{M}_\ell(\mathbb{R}).$$

Montrer que :

$$\|B\| = \|{}^t B\| = \|C\| = \|B {}^t B\|^{\frac{1}{2}} = \|{}^t B B\|^{\frac{1}{2}}$$

- (b) Soit $B \in \mathcal{M}_{m,n}(\mathbb{Z})$. Montrer que soit $\|B\|$ est de la forme $2 \cos\left(\frac{\pi}{q}\right)$, où q est un entier supérieur ou égal à 2, soit $\|B\| \geq 2$.

– IV – Indices d'inclusion On conserve les notations de la partie II.

Définition. Soit $\rho : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_m(\mathbb{C})$ un morphisme d'algèbres avec unité. On rappelle (cf. partie II. 2. (d)) que ρ est injectif et que m est un multiple de n . On pose $m = nd$. On appelle indice d'inclusion de $\mathcal{M}_n(\mathbb{C})$ dans $\mathcal{M}_m(\mathbb{C})$, et on le note $[\mathcal{M}_m(\mathbb{C}) : \mathcal{M}_n(\mathbb{C})]$, l'entier $d^2 = \frac{\dim \mathcal{M}_m(\mathbb{C})}{\dim \mathcal{M}_n(\mathbb{C})}$.

1. Soient $A = \mathcal{M}_n(\mathbb{C})$, $B = \mathcal{M}_m(\mathbb{C})$, $C = \mathcal{M}_f(\mathbb{C})$ des algèbres de matrices et $\rho : A \rightarrow B$, $\tau : B \rightarrow C$ des morphismes d'algèbres avec unité. Montrer que le commutant $\tau(B)'$ de $\tau(B)$ dans C est une sous-algèbre du commutant $(\tau \circ \rho(A))'$ de $(\tau \circ \rho(A))$ dans C , et que l'on a : $[(\tau \circ \rho(A))' : \tau(B)'] = [B : A]$.
2. Soient $R = \bigoplus_{j=1}^r A_j$ et $S = \bigoplus_{i=1}^s B_i$ des sommes directes d'algèbres de matrices (cf. partie II, 4.), et $\Phi : R \rightarrow S$ un morphisme injectif d'algèbres avec unité. Ceci permet de considérer R comme une sous-algèbre de S et, pour tout $x \in R$, d'appeler encore x son image $\Phi(x)$ dans S . Pour tout $j = 1, \dots, r$ soit $q_j \in R$ l'image de l'identité de A_j dans R , et pour $i = 1, \dots, s$ soit $p_i \in S$ l'image de l'identité de B_i dans S .
 - (a) Montrer que $\forall j = 1, \dots, r$ et $\forall i = 1, \dots, s$, $p_i q_j$ est un idempotent de B_i .
 - (b) Si $p_i q_j \neq 0$, on pose $S_{ij} = p_i q_j S p_i q_j$ et $R_{ij} = p_i q_j R p_i q_j$. Montrer que S_{ij} est isomorphe à une algèbre de matrices et que l'application de A_j vers R_{ij} , qui envoie x sur $p_i x p_i$ est un isomorphisme d'algèbres avec unité.
 - (c) On pose pour $j = 1, \dots, r$ et $i = 1, \dots, s$,

$$\begin{aligned} \lambda_{ij} &= 0 \text{ si } p_i q_j = 0 \\ \lambda_{ij} &= [S_{ij} : R_{ij}]^{\frac{1}{2}} \text{ si } p_i q_j \neq 0. \end{aligned}$$

On forme alors la matrice à coefficients entiers positifs $\Lambda_R^S = (\lambda_{ij}) \in \mathcal{M}_{s,r}(\mathbb{N})$. Cette matrice est appelée matrice d'indice pour l'inclusion de R dans S .

Montrer qu'aucune ligne ni aucune colonne de Λ_R^S n'est identiquement nulle.

- (d) On appelle $Z(R)$ (resp. $Z(S)$) le centre de R (resp. de S). Montrer que la matrice Λ_R^S est indécomposable (cf. partie I, 7.) si et seulement si l'intersection $Z(R) \cap Z(S)$ est réduite aux multiples de l'élément unité.
- (e) Soient R, S, T des sommes directes d'algèbres de matrices telles que R soit une sous-algèbre de S et S une sous-algèbre de T . Montrer que :

$$\Lambda_R^T = \Lambda_S^T \cdot \Lambda_R^S.$$

- (f) Soient R et S des sommes directes d'algèbres de matrices telles que R soit une sous-algèbre de S et on suppose de plus que S est une sous-algèbre d'une algèbre de matrices F . On appelle $C(R)$ et $C(S)$ les commutants respectifs de R et S dans F . Montrer que $C(S)$ est une sous-algèbre de $C(R)$ et que la matrice d'indice pour l'inclusion de $C(S)$ dans $C(R)$ est la transposée de celle de l'inclusion de R dans S .
3. Soit S une somme directe d'algèbres de matrices et $F = \text{End}(S)$ l'algèbre des applications \mathbb{C} -linéaires de S dans S . Pour tout x dans S , on définit les éléments $\lambda(x)$ et $\rho(x)$ dans F par :

$$\forall y \in S, \quad \lambda(x)y = xy, \quad \rho(x)y = yx.$$

- (a) Montrer que λ est un morphisme injectif d'algèbres avec unité, que ρ est un anti-homomorphisme d'algèbres avec unité (c'est-à-dire que ρ est une application linéaire envoyant l'unité sur l'unité et telle que, pour tout u et v dans S : $\rho(uv) = \rho(v)\rho(u)$) et que :

$$\forall x, z \in S, \quad \lambda(x)\rho(z) = \rho(z)\lambda(x).$$

- (b) Soit R une somme directe d'algèbres de matrices qui est une sous-algèbre de S . On note $\text{End}_R(S)$ la sous-algèbre de F formée des applications linéaires f vérifiant :

$$\forall x \in R, \quad f \circ \rho(x) = \rho(x) \circ f.$$

Montrer que $\lambda(S)$ est contenu dans $\text{End}_R(S)$ et que $\text{End}_R(S)$ est isomorphe à une somme directe d'algèbres de matrices.

- (c) Montrer que la matrice d'indice pour l'inclusion de $\lambda(S)$ dans $\text{End}_R(S)$ est la transposée de Λ_R^S .
4. Soient R et S des sommes directes d'algèbres de matrices (cf. partie II), R étant une sous-algèbre de S . On pose $S_1 = S$, $S_2 = \text{End}_R(S)$, puis $S_3 = \text{End}_{S_1}(S_2)$ et par récurrence $S_{k+2} = \text{End}_{S_k}(S_{k+1})$. On construit donc ainsi une suite croissante d'algèbres avec unité :

$$R = S_0 \subset S = S_1 \subset S_2 \subset S_3 \subset \dots$$

On pose $\Lambda = \Lambda_R^S$. On suppose que $Z(R) \cap Z(S)$ est réduit aux multiples de l'identité.

- (a) Déterminer, en fonction de Λ , la matrice de l'inclusion $S_0 \subset S_{2k}$ et celle de l'inclusion $S_0 \subset S_{2k+1}$.
- (b) Montrer que $\Lambda^t \Lambda$ et ${}^t \Lambda \Lambda$ sont des matrices positives irréductibles et diagonalisables à valeurs propres positives ou nulles.
- (c) Soit $A = \Lambda^t \Lambda$ ou ${}^t \Lambda \Lambda$. Soit P_0 le projecteur orthogonal sur le sous-espace propre associé à la valeur propre positive maximale (cf. partie I). Soit $y \in \mathbb{R}^n$ un vecteur non nul à coordonnées positives ou nulles. Montrer que $\frac{A^k}{\|A\|^k} y$ converge, quand k tend vers l'infini, vers $P_0 y$.
- (d) Sous les mêmes hypothèses qu'en (c), montrer que :

$$\lim_{k \rightarrow +\infty} \left\| (\Lambda^t \Lambda)^k y \right\|^{\frac{1}{k}} = \lim_{k \rightarrow +\infty} \left\| ({}^t \Lambda \Lambda)^k y \right\|^{\frac{1}{k}} = \|\Lambda\|^2.$$

- (e) Montrer que :

$$\lim_{k \rightarrow +\infty} (\dim S_k)^{\frac{1}{k}} = \|\Lambda\|^2.$$

Quelles sont les valeurs possibles de cette limite ?

Agrégation externe 1998. Épreuve 1

Avertissement.

Les parties I et II sont indépendantes du reste du problème. Le candidat est libre de traiter le problème dans l'ordre qu'il souhaite en admettant clairement des résultats énoncés dans les questions précédentes du problème. Il sera tenu le plus grand compte de la clarté et de la précision de la rédaction.

Notations.

Si A est une partie d'un ensemble B , on notera $B - A$ le complémentaire de A dans B . Soit \mathcal{E} un espace affine euclidien. On note $\|\cdot\|$ la norme de l'espace vectoriel euclidien dirigeant \mathcal{E} . Par sous-espace de \mathcal{E} , on entend sous-espace affine de \mathcal{E} muni de la structure euclidienne induite. Pour tout point c de \mathcal{E} et tout réel $r > 0$, on note $B(c, r)$ (resp. $S(c, r)$) la boule ouverte (resp. sphère) de centre c et de rayon r , c'est-à-dire :

$$B(c, r) = \{p \in \mathcal{E} \mid \|p - c\| < r\} \text{ et } S(c, r) = \{p \in \mathcal{E} \mid \|p - c\| = r\}.$$

Toutes les boules ou sphères considérées dans le problème sont de rayon strictement positif. On appelle *cercle* une partie C de \mathcal{E} telle qu'il existe un sous-espace \mathcal{P} de \mathcal{E} de dimension 2, un point c de \mathcal{P} et un réel $r > 0$ tel que $C = \mathcal{P} \cap S(c, r)$. On appelle alors *disque de bord C* l'ensemble $D = \{p \in \mathcal{P} \mid \|p - c\| \leq r\}$.

Partie I

Soit \mathcal{E} un espace affine euclidien de dimension 2. On veut montrer que l'on ne peut pas recouvrir \mathcal{E} par une famille de cercles disjoints. Soit $(C_i)_{i \in I}$ une partition de \mathcal{E} en cercles C_i de rayon $r_i > 0$; on note D_i le disque de bord C_i .

1. Construire une suite $(i_n)_{n \in \mathbb{N}}$ d'éléments de I telle que :

$$D_{i_{n+1}} \subset D_{i_n} \text{ et } r_{i_{n+1}} \leq \frac{1}{2}r_{i_n}$$

pour tout n .

2. Que dire de $\bigcap_{n \in \mathbb{N}} D_{i_n}$?
3. Conclure.

Partie II

Soit \mathcal{E} un espace affine euclidien de dimension 3.

1. Soient p et q des points distincts d'un cercle C et soit D le disque de bord C . Montrer que $D - \{p, q\}$ est réunion disjointe de segments de droites de longueur non nulle (on dessinera *d'abord* soigneusement la famille choisie et on démontrera *ensuite* qu'elle convient).
2. Soient p et q des points distincts d'une sphère S . Montrer que l'on peut recouvrir $S - \{p, q\}$ par une famille de cercles disjoints (on pourra utiliser la question précédente).
Soient Δ une droite de \mathcal{E} et O un point de Δ .
3. Montrer que l'on peut trouver une famille de cercles $(C_m)_{m \in \mathbb{Z}}$ telle que :
 - les centres des cercles C_m soient sur Δ ;
 - toute sphère de \mathcal{E} de centre O coupe $\bigcup_{m \in \mathbb{Z}} C_m$ en exactement deux points (on dessinera *d'abord* soigneusement la famille choisie et on démontrera *ensuite* qu'elle convient).
4. Montrer que \mathcal{E} est réunion disjointe de cercles.

Partie III

Dans toute la suite du problème, on munit l'espace vectoriel \mathbb{R}^n , $n \geq 1$, du produit scalaire usuel, noté $\langle \cdot, \cdot \rangle$. On identifiera souvent une matrice réelle M carrée d'ordre n et l'endomorphisme de \mathbb{R}^n de matrice M dans la base canonique. En particulier, si P est une partie de \mathbb{R}^n , on note $M(P)$ l'ensemble des $M(x)$, pour x parcourant P . On notera $\|M\|$ la norme d'endomorphisme de M , c'est-à-dire :

$$\|M\| = \sup_{x \in \mathbb{R}^n, \|x\|=1} \|M(x)\|.$$

On rappelle le théorème d'orthonormalisation : étant donné une base (x_1, \dots, x_n) de \mathbb{R}^n , il existe une unique base *orthonormée* (y_1, \dots, y_n) de \mathbb{R}^n telle que y_i soit dans l'espace vectoriel engendré par x_1, \dots, x_i et que $\langle x_i, y_i \rangle$ soit strictement positif pour tout $i \in \{1, \dots, n\}$. On note $GL_n(\mathbb{Z})$ le sous-groupe de $GL_n(\mathbb{R})$ formé des matrices M telles que M et M^{-1} soient à coefficients entiers.

1. Montrer que toute matrice M de $GL_n(\mathbb{R})$ s'écrit de manière unique sous la forme $M = KDT$, où K est une matrice orthogonale, D une matrice diagonale à coefficients diagonaux strictement positifs, et T une matrice triangulaire supérieure à coefficients diagonaux égaux à 1 (on pourra appliquer le théorème d'orthonormalisation aux colonnes de M).
On dira que (K, D, T) est la décomposition d'Iwasawa de M ; on notera $t_{ij}(M)$ les coefficients de T , et $d_i(M)$ les coefficients diagonaux de D .
2. Montrer que $GL_n(\mathbb{Z})$ est l'ensemble des matrices à coefficients entiers de déterminant ± 1 .
On note \mathcal{H}_n l'ensemble $GL_n(\mathbb{R})/GL_n(\mathbb{Z})$ et π_n la surjection canonique $GL_n(\mathbb{R}) \rightarrow \mathcal{H}_n$.
Pour tout élément M de $GL_n(\mathbb{R})$, on notera $[M]$ sa classe $\pi_n(M)$, c'est-à-dire le sous-ensemble $M \cdot GL_n(\mathbb{Z})$ de $GL_n(\mathbb{R})$.
3. Existe-t-il une structure de groupe sur \mathcal{H}_n telle que π_n soit un morphisme de groupes ?
On rappelle qu'un sous-groupe Γ de \mathbb{R}^n est un *réseau* s'il existe une base $\mathcal{C} = (f_1, \dots, f_n)$ de \mathbb{R}^n telle que :

$$\Gamma = \{a_1 f_1 + \dots + a_n f_n \mid a_1, \dots, a_n \in \mathbb{Z}\}.$$

On dit que \mathcal{C} est une *base* du réseau Γ . On note \mathcal{R}_n l'ensemble des réseaux de \mathbb{R}^n .

4. Montrer que l'application :

$$\begin{array}{ccc} GL_n(\mathbb{R}) & \rightarrow & \mathcal{R}_n \\ M & \mapsto & M(\mathbb{Z}^n) \end{array}$$

se factorise à travers π_n pour définir une bijection $\mathcal{H}_n \rightarrow \mathcal{R}_n$.

5. Montrer que l'application $M \mapsto |\det(M)|$ définit par passage au quotient une application $\nu : \mathcal{R}_n \rightarrow \mathbb{R}$.

Donner une interprétation géométrique de $\nu(\Gamma)$ pour un réseau Γ .

On pose $e = (1, 0, \dots, 0)$. Soit $\varphi : GL_n(\mathbb{R}) \rightarrow \mathbb{R}$ l'application $M \mapsto \|M(e)\|$, et soit \mathcal{M} une classe dans \mathcal{H}_n .

6. Montrer que toute boule de \mathbb{R}^n ne contient qu'un nombre fini d'éléments de Γ .

7. Montrer que φ atteint son minimum sur \mathcal{M} .

Une matrice M dans $GL_n(\mathbb{R})$ telle que $\varphi(M) = \min \varphi([M])$, c'est-à-dire telle que $\varphi(M) \leq \varphi(MA)$ pour tout A dans $GL_n(\mathbb{Z})$, sera dite *minimale*.

8. Soient M une matrice dans $GL_n(\mathbb{R})$ et (K, D, T) sa décomposition d'Iwasawa. Exprimer $\varphi(M)$ en fonction des coefficients de D .

9. Si M est minimale, montrer l'inégalité $d_1(M) \leq \frac{2}{\sqrt{3}} d_2(M)$.

On note \mathcal{F}_n l'ensemble des matrices $M \in GL_n(\mathbb{R})$ qui satisfont aux inégalités :

$$d_i(M) \leq \frac{2}{\sqrt{3}} d_{i+1}(M) \text{ pour } 1 \leq i \leq n.$$

Le but des deux questions suivantes est de montrer par récurrence sur n l'égalité $\pi_n(\mathcal{F}_n) = \mathcal{H}_n$.

10. On suppose dans cette question $\pi_{n-1}(\mathcal{F}_{n-1}) = \mathcal{H}_{n-1}$. Soient M une matrice dans $GL_n(\mathbb{R})$ et (K, D, T) sa décomposition d'Iwasawa.

(a) Montrer qu'il existe une matrice A dans $GL_n(\mathbb{Z})$ telle que :

$$DTA = \begin{pmatrix} d_1 & b_2 & \cdots & b_n \\ 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{pmatrix},$$

où b_2, \dots, b_n sont des réels, et où M' est dans \mathcal{F}_{n-1} .

(b) Exprimer la décomposition d'Iwasawa de MA à l'aide de celle de M' .

11. Montrer l'égalité $\pi_n(\mathcal{F}_n) = \mathcal{H}_n$.

12. On définit des applications $m : \mathcal{R}_n \rightarrow \mathbb{R}$ et $\gamma : \mathcal{R}_n \rightarrow \mathbb{R}$ en posant, pour tout réseau Γ dans \mathbb{R}^n ,

$$m(\Gamma) = \inf_{a \in \Gamma, a \neq 0} \|a\| \text{ et } \gamma(\Gamma) = \frac{m(\Gamma)^2}{\nu(\Gamma)^{2/n}}.$$

Montrer les inégalités :

$$0 < \gamma(\Gamma) \leq \left(\frac{2}{\sqrt{3}} \right)^{n-1}.$$

13. Calculer $m(\Gamma)$ et $\gamma(\Gamma)$ pour les réseaux suivants :

$$\mathbb{Z}^n \text{ dans } \mathbb{R}^n; \quad \mathbb{Z}(1, 0) \oplus \mathbb{Z} \left(\frac{1}{2}, \frac{\sqrt{3}}{2} \right) \text{ dans } \mathbb{R}^2.$$

14. On note \mathcal{S}_n l'ensemble des matrices M de \mathcal{F}_n qui satisfont aux inégalités $|t_{ij}(M)| \leq \frac{1}{2}$ pour $1 \leq i < j \leq n$. Montrer l'égalité $\pi_n(\mathcal{S}_n) = \mathcal{H}_n$.

Partie IV

On identifie \mathcal{R}_n et \mathcal{H}_n à l'aide de la bijection construite en **III. 4**. On munit \mathcal{R}_n de la topologie dont les ouverts sont les $\pi_n(U)$ où U est un ouvert de $GL_n(\mathbb{R})$.

1. Montrer que l'application π_n est continue et que \mathcal{R}_n est séparé.
2. Montrer que l'application ν définie en **III. 5**. est continue.
3. Soit U une partie compacte de $GL_n(\mathbb{R})$. Montrer qu'il existe une constante $c > 0$ telle que :

$$\|M(x)\| \geq c\|x\|,$$

pour tout M dans U et tout x dans \mathbb{R}^n .

4. Montrer que les applications m et γ définies en **III. 12**. sont continues.
5. Soit \mathcal{Y} une partie fermée de l'ensemble \mathcal{S}_n défini en **III. 14**. Montrer que \mathcal{Y} est compacte si et seulement s'il existe des réels strictement positifs α et β tels que $d_1(M) \geq \alpha$ et $d_n(M) \leq \beta$, pour tout élément M de \mathcal{Y} .
6. Soit \mathcal{P} une partie fermée de \mathcal{R}_n . Montrer que \mathcal{P} est compacte si et seulement si les deux conditions suivantes sont réalisées :

(i) $\nu(\mathcal{P})$ est une partie majorée de \mathbb{R} ;

(ii) il existe un voisinage U de 0 dans \mathbb{R}^n tel que pour tout réseau Γ de \mathcal{P} , on ait $\Gamma \cap U = \{0\}$.

On note \mathcal{R}'_n la partie fermée de \mathcal{R}_n formée des réseaux Γ tels que $\nu(\Gamma) = 1$, et on note $\gamma' : \mathcal{R}'_n \rightarrow]0, +\infty[$ l'application induite par γ par restriction.

7. Montrer que γ et γ' ont même image.
8. Montrer que l'image réciproque par γ' d'un compact de $]0, +\infty[$ est compacte.
9. Montrer qu'il existe un réseau Γ dans \mathbb{R}^n tel que $\gamma(\Gamma) = \sup_{\Gamma' \in \mathcal{R}_n} \gamma(\Gamma')$.

Partie V

Soit Γ un réseau ; on note $S(\Gamma)$ l'ensemble des $a \in \Gamma$ tels que $\|a\| = m(\Gamma)$ et B_Γ l'ensemble des formes bilinéaires symétriques B sur \mathbb{R}^n telles que $B(a, a) = 1$ pour tout $a \in S(\Gamma)$.

1. Exhiber un élément de B_Γ .
2. Montrer qu'il existe un réel $c(\Gamma) > 1$ ne dépendant que de Γ tel que :

$$\|M(\gamma)\| \geq c(\Gamma) \frac{m(\Gamma)}{\|M^{-1}\|},$$

pour tout M dans $GL_n(\mathbb{R})$ et tout γ non nul dans $\Gamma - S(\Gamma)$.

3. Montrer l'existence d'un voisinage U de la matrice identité I_n dans $GL_n(\mathbb{R})$ tel que :

$$S(M(\Gamma)) \subset M(S(\Gamma))$$

pour tout $M \in U$.

Soient B et B' des éléments de B_Γ et soit M la matrice $B - B'$ dans la base canonique de \mathbb{R}^n . Soit α un réel ; on rappelle (et on admettra) que pour $|\alpha|$ assez petit, il existe une unique matrice définie positive M_α de carré $I_n + \alpha M$. De plus, $\lim_{\alpha \rightarrow 0} M_\alpha = I_n$.

4. Montrer que pour $|\alpha|$ assez petit, on a $m(M_\alpha(\Gamma)) = m(\Gamma)$.
5. Donner un développement limité d'ordre 2 de la fonction $\alpha \rightarrow \det(M_\alpha)$ au voisinage de 0. On suppose dans cette question seulement $\gamma(\Gamma) = \sup_{\Gamma' \in \mathcal{R}_n} \gamma(\Gamma')$. Montrer que B_Γ a un seul élément.
6. On suppose dans cette question que B_Γ a un seul élément. Soit \mathcal{B} une base de Γ .
- (a) Soit B une forme bilinéaire symétrique sur \mathbb{R}^n . Montrer qu'il existe un système linéaire Σ dont le nombre d'équations est $\frac{1}{2} \text{Card}(S(\Gamma))$ tel que :
 B est dans B_Γ si et seulement si les $B(b, b')$, pour b, b' dans \mathcal{B} , sont solutions de Σ .
- (b) Montrer que $S(\Gamma)$ a au moins $n(n+1)$ éléments.
- (c) Exprimer le déterminant de la matrice $(\langle b, b' \rangle)_{b, b' \in \mathcal{B}}$ en fonction de Γ .
- (d) En déduire que $\gamma(\Gamma)^n$ est rationnel.

Agrégation externe 1999. Épreuve 1

Notations et définitions Si A et B sont deux ensembles, on note $A - B$ l'ensemble des éléments de A qui ne sont pas dans B .

Dans tout le problème, \mathbb{K} désigne le corps \mathbb{R} ou \mathbb{C} . On fixe un entier n strictement positif et un \mathbb{K} -espace vectoriel V de dimension $n + 1$. On munit V de sa topologie d'espace vectoriel normé. On note $\mathbb{P}V$ l'espace projectif associé à V , c'est à dire l'ensemble des droites vectorielles de V , ou encore le quotient de $V - \{0\}$ par la relation d'équivalence de colinéarité. On note $\pi : V - \{0\} \rightarrow \mathbb{P}V$ l'application quotient, qui à un vecteur non nul x associe la droite engendrée par x . Soit d un entier ; on appelle *sous-espace projectif de $\mathbb{P}V$ de dimension d* un sous-ensemble P de $\mathbb{P}V$ tel que $\pi^{-1}(P) \cup \{0\}$ soit un sous-espace vectoriel de V de dimension $d + 1$, que l'on notera alors toujours \widehat{P} . Les sous-espaces projectifs de $\mathbb{P}V$ de dimension 0 sont donc les points de $\mathbb{P}V$, ceux de dimension 1 sont appelés *droites projectives* ou simplement droites, et ceux de dimension 2 *plans projectifs* ou simplement plans.

Si q est une forme quadratique sur V , on appelle *quadrique projective* associée à q le sous-ensemble $Q = \pi(\{x \in V - \{0\} \mid q(x) = 0\})$ de $\mathbb{P}V$.

Soit m un entier vérifiant $0 \leq 2m \leq n + 1$; on dit que q est de *type m* s'il existe une base \mathcal{B} de V telle que, pour tout vecteur x de V de coordonnées (x_0, \dots, x_n) dans \mathcal{B} , on ait :

$$q(x) = x_0x_m + x_1x_{m+1} + \dots + x_{m-1}x_{2m-1}.$$

On dit qu'une telle base est *adaptée* à q . Si q est de type m , on dira aussi que Q est une quadrique de type m .

Préliminaire

Dans toute cette partie, q désigne une forme quadratique sur V et Q la quadrique projective associée.

1. Soient P un sous-espace projectif de $\mathbb{P}V$ de dimension d et P' un sous-espace projectif de $\mathbb{P}V$ de dimension d' .
 - (a) Si $d + d' \geq n$, montrer que P rencontre P' .
 - (b) Si P est disjoint de P' , montrer qu'il existe un unique sous-espace projectif de dimension $d + d' + 1$ de $\mathbb{P}V$ qui contient P et P' .
2. (a) On suppose $n = 1$; si Q contient trois points distincts, montrer que $Q = \mathbb{P}V$.

- (b) On suppose $n = 2$; si Q contient une droite projective D , montrer que soit $Q = \mathbb{P}V$, soit il existe une droite projective D' telle que $Q = D \cup D'$.
3. Soit D une droite de $\mathbb{P}V$.
- (a) Si D rencontre Q en au moins trois points, montrer que D est contenue dans Q .
- (b) Si $\mathbb{K} = \mathbb{C}$, montrer que D rencontre Q .
4. Soit m un entier positif.
- (a) Lorsque $\mathbb{K} = \mathbb{R}$, caractériser les formes quadratiques de type m à l'aide de leur signature.
- (b) Lorsque $\mathbb{K} = \mathbb{C}$, caractériser les formes quadratiques de type m à l'aide de leur rang.
5. On suppose $n + 1 = 2m$ et q de type m .
- (a) Déterminer la dimension maximale d'un sous-espace projectif de $\mathbb{P}V$ contenu dans Q .
- (b) Soit q' une forme quadratique sur V dont la quadrique associée contient Q . Montrer que q' est proportionnelle à q (on pourra montrer que la matrice de q' dans une base de V adaptée à q est $\begin{pmatrix} 0 & A \\ {}^tA & 0 \end{pmatrix}$, où A est une matrice carrée d'ordre m , puis que A est diagonale, puis que A est multiple de l'identité).

Première Partie

Droites projectives contenues dans une quadrique de type 2

On suppose dans cette partie $n = 3$. Soient D_1, D_2 et D_3 des droites de $\mathbb{P}V$ deux à deux disjointes.

- Montrer que par chaque point x de D_1 , il passe une unique droite qui rencontre D_2 et D_3 . On la notera D_x .
- Soient x et y des points distincts sur D_1 . Montrer que D_x ne rencontre pas D_y .
- Montrer qu'il existe une base $\mathcal{B} = (e_0, e_1, e_2, e_3)$ de V telle que $\widehat{D_2}$ soit le sous-espace vectoriel de V engendré par e_0 et e_1 , que $\widehat{D_3}$ soit le sous-espace vectoriel de V engendré par e_2 et e_3 , et que $\widehat{D_1}$ soit le sous-espace vectoriel de V engendré par $e_0 - e_3$ et $e_1 + e_2$.
 - On définit une forme quadratique q sur V en posant $q(x) = x_0x_2 + x_1x_3$ pour tout vecteur x de coordonnées (x_0, \dots, x_3) dans la base \mathcal{B} . On note Q la quadrique projective associée. Montrer que pour tout x dans D_1 , la droite D_x est contenue dans Q .
 - Montrer l'égalité $Q = \bigcup_{x \in D_1} D_x$ (si $y \in Q - D_1$, on pourra considérer l'intersection de Q avec le plan contenant y et D_1).
- Soient x un point de Q et \widehat{x} la droite vectorielle de V associée. On note \widehat{x}^\perp l'orthogonal de \widehat{x} pour q , et x^\perp le plan projectif associé $\pi(\widehat{x}^\perp - \{0\})$.
 - Montrer que toute droite projective passant par x et contenue dans Q est contenue dans x^\perp .
 - Quel est le rang de la restriction de q à \widehat{x}^\perp ?

- (c) Montrer qu'exactement deux droites contenues dans Q passent par x .
5. On note \mathcal{P}^+ l'ensemble des droites contenues dans Q qui sont du type D_x , pour $x \in D_1$, et \mathcal{P}^- l'ensemble des droites contenues dans Q qui ne sont pas de ce type.
- (a) Montrer que par chaque point de Q , il passe exactement une droite de \mathcal{P}^+ et une droite de \mathcal{P}^- . En déduire que deux droites distinctes de \mathcal{P}^+ (respectivement de \mathcal{P}^-) sont disjointes.
- (b) Montrer que chaque droite de \mathcal{P}^+ rencontre chaque droite de \mathcal{P}^- .
6. Soient D_1, D_2, D_3 et D_4 des droites de $\mathbb{P}V$ deux à deux disjointes. Montrer que l'on est dans l'un des quatre cas suivants, et que chacun de ces cas peut se produire, à l'exception du premier lorsque $\mathbb{K} = \mathbb{C}$:
- aucune droite ne rencontre D_1, D_2, D_3 et D_4 ;
 - exactement une droite rencontre D_1, D_2, D_3 et D_4 ;
 - exactement deux droites rencontrent D_1, D_2, D_3 et D_4 ;
 - une infinité de droites rencontrent D_1, D_2, D_3 et D_4 .

Deuxième Partie

Plans projectifs contenus dans une quadrique de type 3

Soit d un entier vérifiant $0 \leq d \leq n$. On note \mathcal{G}_d l'ensemble des sous-espaces projectifs de $\mathbb{P}V$ de dimension d (c'est-à-dire aussi l'ensemble des sous-espaces vectoriels de V de dimension $d + 1$). En particulier, $\mathcal{G}_0 = \mathbb{P}V$. On note $GL(V)$ le groupe des automorphismes linéaires de V ; c'est un sous-ensemble de l'espace vectoriel des endomorphismes de V , que l'on munit de la topologie induite

1. Soit W un sous-espace vectoriel de V de dimension $d + 1$.
 - (a) On définit une application $\rho_W : GL(V) \mapsto \mathcal{G}_d$ en associant à un élément g de $GL(V)$ le sous-espace projectif de $\mathbb{P}V$ associé au sous-espace vectoriel $g(W)$ de V . Montrer que ρ_W est surjective.
 - (b) On munit \mathcal{G}_d de la topologie dont les ouverts sont les sous-ensembles \mathcal{U} de \mathcal{G}_d tels que $\rho_W^{-1}(\mathcal{U})$ soit ouvert dans $GL(V)$. Montrer que cette topologie est indépendante du choix de W et que ρ_W est continue pour cette topologie.
2. Soit M un sous-espace vectoriel de V de dimension $n - d$. Montrer que

$$\mathcal{U}_M = \{P \in \mathcal{G}_d \mid \widehat{P} \cap M = \{0\}\}$$

est un ouvert de \mathcal{G}_d homéomorphe à $\mathbb{K}^{(d+1)(n-d)}$ (on pourra introduire un supplémentaire W de M dans V , et considérer l'application ρ_W associée).

3. On fixe une base (e_0, \dots, e_n) de V . Notons \mathcal{I} l'ensemble des parties à $n - d$ éléments de $\{0, \dots, n\}$. Pour tout I dans \mathcal{I} , on note M_I le sous-espace vectoriel de V engendré par $\{e_i \mid i \in I\}$. Montrer l'égalité $\mathcal{G}_d = \bigcup_{I \in \mathcal{I}} \mathcal{U}_{M_I}$.
4. Montrer qu'une partie A de \mathcal{G}_d est ouverte (respectivement fermée) si et seulement si, pour tout I dans \mathcal{I} , l'ensemble $A \cap \mathcal{U}_{M_I}$ est ouvert (respectivement fermé) dans \mathcal{U}_{M_I} .
5. On note V^* l'espace vectoriel dual de l'espace vectoriel V et $A(V^*)$ l'espace vectoriel des formes bilinéaires alternées sur V^* . On note enfin $\mathbb{P}A(V^*)$ l'espace projectif associé à $A(V^*)$.

- (a) Quelle est la dimension de $A(V^*)$?
 (b) Montrer que le déterminant d'une matrice carrée antisymétrique d'ordre impair est nul.
 (c) Montrer que toute forme bilinéaire alternée sur V^* est de rang pair.
 (d) Soient D un élément de \mathcal{G}_1 et (d_1, d_2) une base de \widehat{D} . On associe à D la forme bilinéaire

$$\begin{aligned} V^* \times V^* &\rightarrow \mathbb{K} \\ (l_1, l_2) &\mapsto l_1(d_1)l_2(d_2) - l_1(d_2)l_2(d_1) \end{aligned}$$

Montrer que l'on définit ainsi une application $\kappa : \mathcal{G}_1 \mapsto \mathbb{P}A(V^*)$, puis que κ est injective.

- (e) Caractériser les points de l'image de κ . Décrire l'application réciproque :

$$\kappa^{-1} : \kappa(\mathcal{G}_1) \mapsto \mathcal{G}_1.$$

Dans toute la suite de cette partie, on suppose $n = 3$.

6. Soit $A = (a_{ij})_{1 \leq i, j \leq 4}$ une matrice antisymétrique à coefficients dans \mathbb{K} . Déterminer un polynôme homogène en les coefficients $a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{34}$ dont le carré soit le déterminant de A . En déduire que l'image de κ , est une quadrique Q de type 3 dans $\mathbb{P}A(V^*)$.
7. Soient x un point de $\mathbb{P}V$ et P un plan dans $\mathbb{P}V$. On note $\Pi_x = \kappa(\{D \in \mathcal{G}_1 \mid x \in D\})$ et $\Pi_P = \kappa(\{D \in \mathcal{G}_1 \mid D \subset P\})$.
- (a) Montrer que Π_x est un plan dans $\mathbb{P}A(V^*)$.
 (b) Montrer que Π_P est un plan dans $\mathbb{P}A(V^*)$.
 (c) Montrer que $\Pi_x \cap \Pi_P$ est vide si $x \notin P$, et que c'est une droite projective sinon.
8. Soient ω_1 et ω_2 des formes bilinéaires alternées dégénérées sur V^* . Montrer que les propriétés suivantes sont équivalentes :
- (i) la forme bilinéaire alternée $\omega_1 + \omega_2$ est non dégénérée ;
 (ii) $V^* = \ker(\omega_1) \oplus \ker(\omega_2)$.
9. En déduire que toute droite contenue dans Q est une intersection $\Pi_x \cap \Pi_P$, où P est un plan dans $\mathbb{P}V$ et x un point de P .
10. Montrer que tout plan contenu dans Q est soit du type Π_x , avec $x \in \mathbb{P}V$, soit du type Π_P , où P est un plan dans $\mathbb{P}V$.
11. On obtient ainsi une partition de l'ensemble des plans contenus dans Q en deux sous-ensembles. Montrer que l'intersection de deux de ces plans est de dimension paire si et seulement s'ils sont dans le même sous-ensemble (on rappelle que conformément à nos conventions, l'ensemble vide est un sous-espace projectif de $\mathbb{P}V$ de dimension -1).

Troisième Partie

Espaces projectifs contenus dans une quadrique de type m

Dans toute cette partie, on suppose qu'il existe un entier m tel que $n = 2m - 1$ et l'on fixe une forme quadratique q de type m sur V ainsi qu'une base $\mathcal{B} = (e_0, \dots, e_{2m-1})$ de V adaptée à q (cf. Notations et définitions). On note Q la quadrique projective associée à q et \mathcal{P} l'ensemble des sous-espaces projectifs de $\mathbb{P}V$ de dimension $m - 1$ contenus dans Q ; c'est un sous-ensemble de l'espace topologique \mathcal{G}_{m-1} défini dans la première question de la partie précédente.

1. Montrer que \mathcal{P} est fermé dans \mathcal{G}_{m-1} .
2. Soit I une partie de $\{0, \dots, m-1\}$. On pose $I^C = \{0, \dots, m-1\} - I$. Soit N_I le sous-espace vectoriel de V engendré par les vecteurs $(e_i)_{i \in I}$ et $(e_{m+i})_{i \in I^C}$. On note u_I l'automorphisme de V défini par $u_I(e_i) = e_{m+i}$ et $u_I(e_{m+i}) = e_i$ si $i \in I$, et $u_I(e_i) = e_i$ et $u_I(e_{m+i}) = e_{m+i}$ si $i \in I^C$ de sorte que $N_I = u_I(N_\emptyset)$. En particulier, u_\emptyset est l'identité de V .
 - (a) Montrer que $\mathcal{P} \cap \mathcal{U}_{N_\emptyset}$ est homéomorphe à $\mathbb{K}^{m(m-1)/2}$.
 - (b) Montrer que l'application $v_I : \mathcal{G}_{m-1} \mapsto \mathcal{G}_{m-1}$ qui à un sous-espace projectif P de $\mathbb{P}V$ de dimension $m-1$ associe le sous-espace projectif $u_I(P)$, est un homéomorphisme. Déterminer $v_I(\mathcal{P} \cap \mathcal{U}_{N_\emptyset})$.
 - (c) Montrer que \mathcal{P} est contenu dans la réunion des \mathcal{U}_{N_I} , lorsque I parcourt l'ensemble des parties de $\{0, \dots, m-1\}$.
 - (d) Montrer que $\mathcal{P} \cap \mathcal{U}_{N_\emptyset} \cap \mathcal{U}_{N_I}$ est vide si et seulement si le cardinal de I est impair.
 - (e) Soient I et J des parties de $\{0, \dots, m-1\}$; déterminer $u_I(N_J)$. En déduire une condition nécessaire et suffisante sur I et J pour que $\mathcal{P} \cap \mathcal{U}_{N_I} \cap \mathcal{U}_{N_J}$ soit vide.
3. En déduire que \mathcal{P} est réunion disjointe de deux sous-ensembles fermés connexes homéomorphes notés \mathcal{P}^+ et \mathcal{P}^- , et que deux sous-espaces projectifs de dimension $m-1$ contenus dans Q sont dans le même sous-ensemble \mathcal{P}^+ ou \mathcal{P}^- si et seulement si la dimension de leur intersection a même parité que $m-1$.
4. Soit P_1 un sous-espace projectif de $\mathbb{P}V$ de dimension $m-2$ contenu dans Q . Montrer qu'il existe un unique élément de \mathcal{P}^+ contenant P_1 et un unique élément de \mathcal{P}^- contenant P_1 .

Agrégation externe 2000. Épreuve 1

Pour deux entiers $t, u \geq 1$, on notera $\mathcal{M}_{t,u}(\mathbb{C})$ (resp. $\mathcal{M}_t(\mathbb{C})$) l'espace des matrices à t lignes et u colonnes (resp. carrées à t lignes) à coefficients dans \mathbb{C} , munis de leurs topologies habituelles. Pour q entier, on notera I_q la matrice identité $q \times q$. Pour un entier $n \geq 1$ et un sous-groupe S de $GL(2n, \mathbb{C})$, on notera $\text{Ad}_g(X)$ le conjugué gXg^{-1} de $X \in \mathcal{M}_{2n}(\mathbb{C})$ par $g \in S$, et $\text{Ad}(S)X = \{\text{Ad}_g(X), g \in S\}$.

Dans tout le problème on notera M le sous-groupe de $GL(2n, \mathbb{C})$ formé des matrices blocs $\begin{bmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{bmatrix}$ où $A \in GL(n, \mathbb{C})$; on remarquera qu'il est isomorphe à $GL(n, \mathbb{C})$. On désigne par \mathcal{S} l'espace vectoriel des matrices $n \times n$ symétriques complexes et \mathcal{A} l'espace vectoriel des matrices $n \times n$ alternées (ou antisymétriques) complexes.

I

- Montrez que le groupe M opère sur \mathcal{S} (resp. \mathcal{A}) par l'action $(g, X) \mapsto {}^tA^{-1}XA^{-1}$ où $g = \begin{bmatrix} A & 0 \\ 0 & {}^tA^{-1} \end{bmatrix} \in M$ et $X \in \mathcal{S}$ (resp. \mathcal{A}).
Deux matrices, dans la même orbite pour l'action précédente, sont dites congrues.
- Déterminez les orbites X_i pour cette action.
- Si Ω est l'une de ces orbites, déterminez l'adhérence $\overline{\Omega}$ de Ω dans \mathcal{S} au moyen des orbites X_i .

On n'utilisera pas dans la suite du problème les propriétés topologiques de cette adhérence ni de celle définie en **II 3**.

II

On posera $J_r = \begin{bmatrix} 0 & I_r \\ -I_r & 0 \end{bmatrix}$, r entier positif, avec la convention, si $r = 0$, que $I_0 = 0$ et donc $J_0 = 0$.

- Montrez que toute matrice alternée complexe $n \times n$ de rang $2r$ est congrue à une matrice bloc $\begin{bmatrix} J_r & 0 \\ 0 & 0 \end{bmatrix}$.

On pourra montrer d'abord que la matrice d'une forme bilinéaire alternée non dégénérée est, dans une certaine base, une diagonale de blocs 2×2 : $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

2. Déterminez les orbites Y_j de M dans l'action sur \mathcal{A} pour la congruence.
3. Si Ω est l'une des orbites précédentes, déterminez l'adhérence $\overline{\Omega}$ de Ω dans \mathcal{A} .

III

Soient E un \mathbb{C} -espace vectoriel de dimension $2n$ et L, L' deux sous-espaces supplémentaires de dimension n , $E = L \oplus L'$. On choisit des bases (e_1, e_2, \dots, e_n) de L et $(e_{-1}, e_{-2}, \dots, e_{-n})$ de L' et l'on définit sur E une forme bilinéaire symétrique, notée $(,)$, pour laquelle L et L' sont des sous-espaces totalement isotropes tels que $(e_i, e_j) = \delta_{-i,j}$ pour $i = 1, 2, \dots, n$, $j = -1, -2, \dots, -n$ où δ est le symbole de Kronecker.

1. Ecrire la matrice P de la forme bilinéaire $(,)$ dans la base (e_1, \dots, e_{-n}) de E .
On note G^s le groupe des matrices q complexes $2n \times 2n$, telles que ${}^t q P q = P$, et \mathcal{G}^σ l'espace des matrices z complexes $2n \times 2n$, qui vérifient $P {}^t z + z P = 0$.
2. Montrez que \mathcal{G}^σ est stable pour la conjugaison par les matrices de G^s .
3. Décrire la forme des matrices blocs 2×2 qui appartiennent à l'espace \mathcal{G}^σ .

IV

Soient F un \mathbb{C} -espace vectoriel de dimension $2n$ et U, U' deux sous-espaces supplémentaires de dimension n , $F = U \oplus U'$. On choisit des bases (e_1, e_2, \dots, e_n) de U et $(e_{-1}, e_{-2}, \dots, e_{-n})$ de U' et l'on définit sur F une forme bilinéaire alternée, notée $\langle | \rangle$, dont la matrice dans la base $(e_1, \dots, e_n, e_{-1}, \dots, e_{-n})$ est J_n .

On notera G^a le groupe des matrices q inversibles $2n \times 2n$ telles que ${}^t q J_n q = J_n$.

1. Quelles relations nécessaires et suffisantes doivent vérifier $A, B, C, D \in \mathcal{M}_n(\mathbb{C})$ pour que la matrice bloc

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

appartienne à G^a ?

2. Montrez que G^a laisse stable pour la conjugaison l'espace \mathcal{G}^A des matrices blocs

$$\begin{bmatrix} A & B \\ C & -{}^t A \end{bmatrix}$$

où $A, B, C \in \mathcal{M}_n(\mathbb{C})$ et $B, C \in \mathcal{S}$.

V

On définit les sous-espaces suivants de $\mathcal{M}_{2n}(\mathbb{C})$:

$$\underline{\mathcal{M}} = \left\{ \begin{bmatrix} A & 0 \\ 0 & -{}^t A \end{bmatrix}, \quad A \in \mathcal{M}_n(\mathbb{C}) \right\}$$

$$\underline{\mathcal{L}}_a^+ = \left\{ \begin{bmatrix} 0 & 0 \\ C & 0 \end{bmatrix}, \quad C = -{}^t C \in \mathcal{M}_n(\mathbb{C}) \right\} \quad \underline{\mathcal{L}}_s^+ = \left\{ \begin{bmatrix} 0 & 0 \\ C & 0 \end{bmatrix}, \quad C = {}^t C \in \mathcal{M}_n(\mathbb{C}) \right\}$$

$$\underline{r}_a^- = \left\{ \begin{bmatrix} 0 & B \\ 0 & 0 \end{bmatrix}, B = -{}^t B \in \mathcal{M}_n(\mathbb{C}) \right\} \quad \underline{r}_s^- = \left\{ \begin{bmatrix} 0 & B \\ 0 & 0 \end{bmatrix}, B = {}^t B \in \mathcal{M}_n(\mathbb{C}) \right\}$$

$$\underline{p}_\lambda^+ = \underline{\mathcal{M}} \oplus \underline{r}_\lambda^+ \text{ où } \lambda = s \text{ ou } a,$$

$$\underline{p}_\lambda^- = \underline{\mathcal{M}} \oplus \underline{r}_\lambda^- \text{ où } \lambda = s \text{ ou } a.$$

On notera $\pi_{+,a}$ la projection de \mathcal{G}^σ sur \underline{r}_a^+ parallèlement à \underline{p}_a^- et $\pi_{+,s}$ la projection de \mathcal{G}^A sur \underline{r}_s^+ parallèlement à \underline{p}_s^- .

1. (a) Montrez que le groupe M opère par la conjugaison sur chacun des espaces \underline{r}_λ^+ , $\lambda = s$ ou a .

- (b) Dédurre de (a) que l'application η_a (resp. η_s) $\begin{bmatrix} 0 & 0 \\ C & 0 \end{bmatrix} \mapsto C$ est une bijection linéaire de \underline{r}_a^+ (resp. \underline{r}_s^+) sur \mathcal{A} (resp. \mathcal{S}) qui transforme l'opération de conjugaison de M en l'action de M définie en **I 1**.

On identifiera les orbites X_i (resp. Y_j) aux sous-ensembles correspondant par η_a^{-1} (resp. η_s^{-1}) de \underline{r}_a^+ (resp. \underline{r}_s^+).

2. On note \mathbb{O}_k^a (resp. \mathbb{O}_k^s) l'ensemble des éléments z de \mathcal{G}^σ (resp. \mathcal{G}^A) de rang $2k$ (resp. de rang k) tels que $z^2 = 0$. Vérifiez que \mathbb{O}_k^a (resp. \mathbb{O}_k^s) est stable sous l'action de conjugaison de G^s (resp. G^a).

On note, pour k entier ≥ 1 , V_k^a (resp. V_k^s) l'ensemble des $z = \begin{bmatrix} A & B \\ C & -{}^t A \end{bmatrix} \in \mathbb{O}_k^a$ (resp. \mathbb{O}_k^s) vérifiant l'inégalité $\text{rang } C \leq 2(k-1)$ (resp. $\leq k-1$).

3. On pose $R^{-,s} = \left\{ \begin{bmatrix} I_n & T \\ 0 & I_n \end{bmatrix}, T \in \mathcal{S} \right\}$, $R^{-,a} = \left\{ \begin{bmatrix} I_n & T \\ 0 & I_n \end{bmatrix}, T \in \mathcal{A} \right\}$.

- (a) Vérifiez que $R^{-,s}$ (resp. $R^{-,a}$) est un sous-groupe de G^a (resp. G^s) et qu'il en est ainsi de

$$P^s = MR^{-,s} = \{ZY, \text{ où } Z \in M \text{ et } Y \in R^{-,s}\}$$

(resp. $P^a = MR^{-,a}$).

- (b) Démontrez que V_k^a est stable par l'action de P^a et que V_k^s est stable par l'action de P^s .

VI

1. (a) Soit $z = \begin{bmatrix} A & B \\ C & -{}^t A \end{bmatrix} \in \mathcal{G}^A$, $1 \leq r = \text{rang } B$, $1 \leq u = \text{rang } C$. Montrez qu'il existe

$$\gamma_1, \gamma_2 \in M \text{ tels que } \text{Ad } \gamma_1(z) = \begin{bmatrix} A' & B' \\ C' & -{}^t A' \end{bmatrix} \text{ avec } B' = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix},$$

$$\text{Ad } \gamma_2(z) = \begin{bmatrix} A'' & B'' \\ C'' & -{}^t A'' \end{bmatrix} \text{ avec } C'' = \begin{bmatrix} I_u & 0 \\ 0 & 0 \end{bmatrix}.$$

- (b) On introduit pour un entier $r \geq 1$, la matrice $K_r = \sqrt{-1}J_r$; vérifiez que $K_r^{-1} = K_r$. Démontrez un résultat parallèle à celui de **VI 1.(a)** faisant intervenir K_r , où $z \in \mathcal{G}^\sigma$ et $2r = \text{rang } B$, $2u = \text{rang } C$.

2. (a) Soit $w = \begin{bmatrix} A' & B' \\ C' & D' \end{bmatrix} \in V_k^s$ où $D' = -{}^t A'$. On suppose dans cette question que B' est de la forme $\begin{bmatrix} I_c & 0 \\ 0 & 0 \end{bmatrix}$ où $c \geq 0$. Montrez que A', C' et D' sont des matrices blocs de la forme suivante :

$$A' = \begin{bmatrix} A_1 & A_2 \\ 0 & A_4 \end{bmatrix}, \text{ où } A_1 \text{ est une matrice } c \times c, \text{ } {}^t A_1 = A_1 \text{ et } A_4^2 = 0;$$

$$C' = \begin{bmatrix} C_1 & C_2 \\ C_3 & C_4 \end{bmatrix}, \text{ où } C_1 = -A_1^2, C_2 = -(A_1 A_2 + A_2 A_4), C_3 = D_3 A_1 - D_4 D_3;$$

$$D' = -{}^t A' = \begin{bmatrix} -A_1 & 0 \\ D_3 & D_4 \end{bmatrix}.$$

- (b) Démontrez le résultat parallèle à **VI 2. (a)** pour $w \in V_k^a$ et $B' = \begin{bmatrix} K_c & 0 \\ 0 & 0 \end{bmatrix}$, où A_1 est une matrice $2c \times 2c$, ${}^t A_1 = -J_c A_1 J_c$, $A_4^2 = 0$;

$$C' = \begin{bmatrix} C_1 & C_2 \\ C_3 & C_4 \end{bmatrix}, \text{ où } C_1 = -K_c A_1^2, C_2 = -K_c (A_1 A_2 + A_2 A_4),$$

$$C_3 = D_3 K_c A_1 - D_4 D_3 K_c; D' = \begin{bmatrix} -K_c A_1 K_c & 0 \\ D_3 & D_4 \end{bmatrix}.$$

3. (a) Soient $z = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in V_k^s$ et $\gamma \in M$; on pose $\text{Ad } \gamma(z) = w = \begin{bmatrix} A' & B' \\ C' & D' \end{bmatrix}$ et l'on suppose que $B' = \begin{bmatrix} I_c & 0 \\ 0 & 0 \end{bmatrix}$ où $c = \text{rang } B \geq 1$.

En écrivant w comme dans la question **VI 2. (a)** sous la forme de blocs 4×4 on a

$$\begin{bmatrix} A_1 & A_2 & I_c & 0 \\ 0 & A_4 & 0 & 0 \\ C_1 & C_2 & -A_1 & 0 \\ C_3 & C_4 & D_3 & D_4 \end{bmatrix}.$$

Démontrez que $c = k$ si et seulement si $A_4 = D_4 = C_4 - D_3 A_2 = 0$.

- (b) Démontrez le résultat parallèle à celui de **VI 3. (a)** pour $z = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \in V_k^a$, $B' = \begin{bmatrix} K_c & 0 \\ 0 & 0 \end{bmatrix}$ où $2c = \text{rang } B$.

VII

On pose, pour $k \geq 1$

$$W_k^s = \left\{ z \in V_k^s, \quad z = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \text{ où } \text{rang } B = k \right\},$$

$$W_k^a = \left\{ z \in V_k^a, \quad z = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \text{ où } \text{rang } B = 2k \right\}.$$

On se propose, dans cette question, de démontrer que pour tout $z \in V_k^s$, il existe $\gamma \in P^s$ tel que $w = \text{Ad } \gamma(z)$ appartient à W_k^s . Pour cela, l'on choisit parmi les éléments de $\text{Ad}(P^s)z$ un élément $z = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ de \mathcal{G}^A tel que le rang c de B soit maximum ; on va raisonner ensuite par l'absurde en supposant $c < k$ et aboutir à une contradiction.

1. Montrez que l'on peut supposer que

$$B = \begin{bmatrix} I_c & 0 \\ 0 & 0 \end{bmatrix}, \quad c \geq 0.$$

On va utiliser dans la suite des matrices $\gamma \in R^{-,s}$ de la forme $\gamma = \begin{bmatrix} I_n & T \\ 0 & I_n \end{bmatrix}$,

$T = \begin{bmatrix} 0 & 0 \\ 0 & T' \end{bmatrix}$ où T' est une matrice symétrique $(n-c) \times (n-c)$ telle que $n-c$ soit supérieur ou égal à 1.

2. En conjuguant z par une telle matrice γ et utilisant les notations de **VI 3. (a)** montrez que

$$\text{Ad}(\gamma)z = \begin{bmatrix} A+TC & E \\ C & D-CT \end{bmatrix}, \quad \text{où } E = \begin{bmatrix} I_c & -A_2T' \\ T'D_3 & T'D_4 - A_4T' - T'C_4T' \end{bmatrix}$$

et montrez que la maximalité du rang de B implique que

$$F = T'D_4 - A_4T' - T'(C_4 - D_3A_2)T'$$

est nulle.

3. (a) En supposant que $A_4 \neq 0$, montrez l'existence d'une matrice inversible g et d'une matrice (éventuellement vide) H telles que

$$gA_4g^{-1} = \begin{bmatrix} E_{12} & 0 \\ 0 & H \end{bmatrix}, \quad \text{où } E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

et vérifiez que $n-c \geq 2$.

- (b) En déduire, en prenant $T' = g^{-1} \begin{bmatrix} E_{22} & 0 \\ 0 & 0 \end{bmatrix} {}^t g^{-1}$ et en posant $Y = \begin{bmatrix} E_{11} & 0 \\ 0 & 0 \end{bmatrix} g$ où

$$E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \text{ et } E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \text{ que } YT' = 0, YF = -YA_4T'.$$

- (c) En déduire une contradiction avec le fait que $A_4 \neq 0$.

- (d) Montrez qu'il en résulte que $A_4 = 0$ et $D_4 = 0$.

4. En choisissant convenablement la matrice T' montrez que $X = C_4 - D_3A_2$ est nulle et conclure.

VIII

Si $2 \leq 2k \leq n-1$, adaptez la preuve de **VII** de façon à prouver que pour tout $z \in V_k^a$ il existe $\gamma \in P^a$ tel que $w = \text{Ad } \gamma(z)$ appartient à W_k^a .

IX

Soit $k \geq 1$. On notera V_k pour V_k^a ou V_k^s et l'on désignera par \tilde{k} le nombre k si $V_k = V_k^s$ et le nombre $2k$ si $V_k = V_k^a$. Démontrez que si

$$z = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$$

appartient à V_k , alors $\text{rang } A < \tilde{k}$.

*Les résultats des parties **VII**, **VIII**, **IX** interviennent dans la classification de certaines représentations d'algèbres de Lie.*

Agrégation externe 2001. Épreuve 1

Dans tout le problème n désigne un entier naturel strictement positif, \mathbb{R} le corps des nombres réels et \mathbb{R}^n l'espace vectoriel euclidien canonique de dimension n . \mathbb{R}^n est également canoniquement muni d'une structure d'espace affine. On choisit pour origine, notée O , le vecteur nul de l'espace vectoriel.

On note $\langle x, y \rangle$ le produit scalaire de deux vecteurs x et y de \mathbb{R}^n et $\|x\|$ la norme euclidienne de x .

On note $GL_n(\mathbb{R})$ le groupe des matrices carrées de dimension n inversibles et on note $\det(A)$ le déterminant de la matrice carrée A . Si E est une partie de \mathbb{R}^n et A une matrice dans $GL_n(\mathbb{R})$, on note $A(E)$ l'image de E par l'endomorphisme de \mathbb{R}^n canoniquement associé à A .

Si E est une partie de \mathbb{R}^n , on appelle figure polaire de E , notée E^* , la partie de \mathbb{R}^n formée des points y tels que $\langle x, y \rangle \leq 1$ pour tout x dans E :

$$E^* = \{y \in \mathbb{R}^n \mid \forall x \in E, \langle x, y \rangle \leq 1\}.$$

On rappelle qu'une partie de \mathbb{R}^n est convexe si, pour tout couple (A, B) de ses points, elle contient le segment $[A, B]$. Une fonction f d'une partie E de \mathbb{R}^n à valeurs dans \mathbb{R} est dite convexe si E est convexe et si

$$\forall (x, y) \in E^2, \quad \forall \lambda \in [0, 1], \quad f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y)$$

(i.e. le graphe est sous ses cordes). On dit que f est strictement convexe si elle est convexe et si l'inégalité précédente n'est une égalité que si $x = y$ ou $\lambda \in \{0, 1\}$. Enfin f est dite (strictement) concave si $-f$ est (strictement) convexe.

Une partie E de \mathbb{R}^n est dite O -symétrique si elle est globalement invariante par la symétrie centrale (affine) de centre O . Si λ est un scalaire, on note λE l'image de E par l'homothétie de centre O et de rapport λ .

On dit qu'une partie E de \mathbb{R}^n est un corps convexe si elle convexe et d'intérieur non vide. On remarquera qu'un corps convexe O -symétrique contient toujours O dans son intérieur (car si x est intérieur, il en est de même de $-x$ par symétrie et aussi de $\frac{x + (-x)}{2}$ par convexité).

Enfin si E est une partie Lebesgue-mesurable de \mathbb{R}^n on note $\text{vol}(E)$ son volume.

Les deuxième et troisième parties sont indépendantes l'une de l'autre. Il est rappelé que la présentation, la rédaction et la précision sont des éléments importants d'appréciation des copies.

Partie I – Généralités

Soit K un corps convexe et compact de \mathbb{R}^n contenant O dans son intérieur.

1. Soient K_0 et K_1 des parties convexes de \mathbb{R}^n et θ un réel dans $[0, 1]$; montrer que K_θ est convexe, où on a noté :

$$K_\theta = (1 - \theta) K_0 + \theta K_1 = \{x \in \mathbb{R}^n \mid \exists (x_0, x_1) \in K_0 \times K_1, \quad x = (1 - \theta) x_0 + \theta x_1\}.$$

2. Soit A une matrice dans $GL_n(\mathbb{R})$. Montrer $(A(K))^* = {}^t A^{-1}(K^*)$.
3. Soit x dans \mathbb{R}^n , on pose $I_x = \{\lambda \in \mathbb{R}_+ \mid x \in \lambda K\}$.
 - (a) Montrer que I_x est un intervalle fermé non majoré de \mathbb{R}_+ .
 - (b) On peut donc poser $j_K(x) = \inf(I_x)$; c'est un réel positif. Soit ∂K la frontière de K . Montrer que :

$$x \in K \Leftrightarrow j_K(x) \leq 1 \text{ et } x \in \partial K \Leftrightarrow j_K(x) = 1.$$

4. Étude d'exemples

- (a) Expliciter K^* , j_K et j_{K^*} dans les trois cas suivants :
 - i. K est le disque unité (euclidien) de \mathbb{R}^2 .
 - ii. K est le carré $K = \{(x_1, x_2) \in \mathbb{R}^2 \mid -1 \leq x_1, x_2 \leq 1\}$.
 - iii. K est un parallélogramme, dans \mathbb{R}^2 , de centre O .
- (b) Montrer que K^* est un corps convexe, compact, contenant O dans son intérieur et :

$$\forall y \in \mathbb{R}^n, \quad j_{K^*}(y) = \max \{\langle x, y \rangle \mid x \in K\}.$$

- (c) On suppose que K est O -symétrique. Montrer que j_K et j_{K^*} sont des normes. Que dire de (\mathbb{R}^n, j_K) et (\mathbb{R}^n, j_{K^*}) ?

5. Un résultat de dualité

On note p_K la projection sur le convexe compact K .

- (a) Soit a n'appartenant pas à K et H l'hyperplan passant par $p_K(a)$ et orthogonal à la droite passant par a et $p_K(a)$. Montrer qu'il existe une équation de la forme :

$$H = \{x \in \mathbb{R}^n \mid \langle x, u \rangle = 1\}$$

pour un certain vecteur u de \mathbb{R}^n , telle que $\langle a, u \rangle > 1$ et, pour tout point x de K , $\langle x, u \rangle \leq 1$.

- (b) Montrer que $(K^*)^* = K$.

6. Projection d'un convexe

Soit pr_H une projection (affine) de \mathbb{R}^n d'image un hyperplan affine H et de direction quelconque D (une droite affine) non parallèle à H . On munit l'espace affine d'un repère (non nécessairement orthogonal) tel que H soit l'hyperplan d'équation $x_n = 0$ et D la droite d'équation $x_1 = \dots = x_{n-1} = 0$.

Montrer qu'il existe ϕ_K et ϕ^K des applications de $pr_H(K)$ dans \mathbb{R} respectivement convexe et concave telles que K soit l'ensemble des $x = (x_1, \dots, x_n)$ tels que (x_1, \dots, x_{n-1}) appartient à $pr_H(K)$ et

$$\phi_K(x_1, \dots, x_{n-1}) \leq x_n \leq \phi^K(x_1, \dots, x_{n-1}).$$

Partie II – Géométrie des formes quadratiques

On appelle ellipsoïde (sous-entendu centré en O) la boule unité pour une forme quadratique définie positive sur \mathbb{R}^n . Il revient au même de se donner une matrice symétrique définie positive A et de considérer le sous-ensemble $E(A)$ de \mathbb{R}^n des x tels que $\langle x, Ax \rangle \leq 1$. On note \mathcal{E} l'ensemble des ellipsoïdes. En identifiant l'ellipsoïde $E(A)$ aux coefficients $a_{i,j}$ de A avec $i \leq j$, on considère \mathcal{E} comme une partie de $\mathbb{R}^{n(n+1)/2}$ et on le munit de la topologie induite.

1. Ellipsoïdes et boules unités

Soit A une matrice symétrique définie positive. Montrer qu'il existe une matrice symétrique définie positive telle que $B^2 = A^{-1}$. En déduire qu'un ellipsoïde est l'image de la boule unité (euclidienne) par une application linéaire.

2. Ellipsoïdes et convexité

Montrer que l'application $A \mapsto (\det A)^{-1/2}$ de l'ensemble des matrices $n \times n$ symétriques définies positives dans \mathbb{R}_+^* est strictement convexe. (On pourra songer à considérer le logarithme.)

3. Ellipsoïde maximal

Soit K un corps convexe compact O -symétrique de \mathbb{R}^n .

- Soit v un réel strictement positif. Montrer que l'ensemble $\mathcal{E}_{K,v}$ des ellipsoïdes de \mathbb{R}^n ayant un volume supérieur à v et inclus dans K est une partie compacte de \mathcal{E} .
- En déduire qu'il existe un unique ellipsoïde E_K de \mathbb{R}^n inclus dans K et de volume maximal pour cette propriété.

4. Formes quadratiques et corps convexes

- Soit K un corps convexe compact O -symétrique de \mathbb{R}^n . On note Is_K le groupe des automorphismes linéaires u de \mathbb{R}^n tels que $u(K) = K$. Montrer qu'il existe une forme quadratique q_K définie positive invariante par Is_K , i.e. :

$$\forall u \in Is_K, \quad \forall x \in \mathbb{R}^n, \quad q_K(u(x)) = q_K(x).$$

- Donner E_K et une forme q_K possible dans chacun des exemples de **I.4.a**.

Partie III – Théorème de Brunn-Minkowski

Soient K_0 et K_1 deux parties compactes de \mathbb{R}^n **non nécessairement convexes**. On note :

$$K_0 + K_1 = \{x \in \mathbb{R}^n \mid \exists (k_0, k_1) \in K_0 \times K_1, \quad x = k_0 + k_1\}.$$

Le but de cette partie est de démontrer l'inégalité suivante (théorème de Brunn-Minkowski) :

$$\text{vol}(K_0)^{1/n} + \text{vol}(K_1)^{1/n} \leq \text{vol}(K_0 + K_1)^{1/n}. \quad (11.1)$$

On **admettra** pour la suite la précision suivante. L'égalité ne se produit que dans les cas suivants : soit $\text{vol}(K_0) = \text{vol}(K_1) = 0$, soit l'un des compacts est réduit à un point, soit K_0 et K_1 sont images l'un de l'autre par une homothétie affine ou une translation.

1. Si (a_1, \dots, a_n) et (b_1, \dots, b_n) sont deux n -uplets de réels, on note $P(a, b)$ le parallélépipède rectangle donné par :

$$P(a, b) = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \forall i \in [1, n], \quad a_i \leq x_i \leq b_i\}.$$

On appelle standard un parallélépipède qui est de cette forme et d'intérieur non vide.

On suppose que K_0 et K_1 sont chacun réunions finies de parallélépipèdes standard d'intérieurs disjoints :

$$K_0 = \bigcup_{i=1}^{n_0} P(a^{(i)}, b^{(i)}), \quad K_1 = \bigcup_{i=1}^{n_1} P(c^{(i)}, d^{(i)}).$$

On va montrer par récurrence sur $n_0 + n_1$ que l'inégalité (11.1) est valable pour K_0 et K_1 .

- (a) Etablir l'inégalité (11.1) dans le cas où K_0 et K_1 sont des parallélépipèdes standard (i.e. $n_0 = n_1 = 1$) en précisant le cas d'égalité (on pourra commencer par diviser par $\text{vol}(K_0 + K_1)^{1/n}$).
- (b) Pour n_0 et n_1 quelconques avec n_0 supérieur ou égal à 2, trouver un entier k entre 1 et n ainsi que deux réels t et u de sorte que chacun des demi-espaces $x_k \geq t$ et $x_k \leq t$ contienne l'un des parallélépipèdes constituant K_0 et que l'hyperplan $x_k = u$ partage K_1 suivant les mêmes proportions que ne le fait $x_k = t$ avec K_0 :

$$\frac{\text{vol}(K_0 \cap \{x_k \leq t\})}{\text{vol}(K_0 \cap \{x_k \geq t\})} = \frac{\text{vol}(K_1 \cap \{x_k \leq u\})}{\text{vol}(K_1 \cap \{x_k \geq u\})}.$$

- (c) Etablir l'inégalité (11.1) dans le cas où K_0 et K_1 sont des réunions finies de parallélépipèdes standard d'intérieurs disjoints.

2. En déduire le théorème de Brunn-Minkowski.

Agrégation externe 2002. Épreuve 1

Notations et définitions

Soient A, B et C trois groupes abéliens. On appelle forme biadditive de $A \times B$ dans C une application f de $A \times B$ dans C qui vérifie les conditions suivantes :

$$\begin{cases} \forall (a, a') \in A^2, \forall b \in B, & f(a + a', b) = f(a, b) + f(a', b) \\ \forall a \in A, \forall (b, b') \in B^2, & f(a, b + b') = f(a, b) + f(a, b') \end{cases}$$

– I – Formes sesquilineaires symétriques

Soit E un espace vectoriel de dimension finie sur \mathbb{C} . On appelle forme sesquilineaire sur E une forme biadditive b de $E \times E$ dans \mathbb{C} qui vérifie les conditions suivantes :

$$\forall \lambda \in \mathbb{C}, \forall (x, y) \in E^2, \quad \begin{cases} b(\lambda x, y) = \lambda b(x, y) \\ b(x, \lambda y) = \bar{\lambda} b(x, y) \end{cases}$$

Une telle forme est dite symétrique si l'on a :

$$\forall (x, y) \in E^2, \quad b(x, y) = \overline{b(y, x)}.$$

Une forme b sesquilineaire symétrique sur E est dite définie positive [resp. définie négative] sur un sous-espace vectoriel F de E si pour tout vecteur non nul x de F , $b(x, x)$ est un réel strictement positif [resp. strictement négatif].

On appelle espace sesquilineaire un couple (E, b) où b est une forme sesquilineaire sur un espace vectoriel E de dimension finie sur \mathbb{C} . Un espace sesquilineaire (E, b) est dit symétrique si la forme b est symétrique.

Si (E, b) est un espace sesquilineaire symétrique, l'orthogonal d'un sous-espace vectoriel F de E est noté T^\perp . C'est l'ensemble des vecteurs x de E tels que $b(x, y) = 0$ pour tout y dans F .

Une base $\mathcal{B} = (e_1, e_2, \dots, e_n)$ d'un espace sesquilineaire symétrique (E, b) est dite orthogonale si $b(e_i, e_j) = 0$ pour tous $i \neq j$. On dira qu'elle est semi-orthonormée si elle est orthogonale et si de plus $b(e_i, e_i)$ est, pour tout i , égal à -1 , 0 ou 1 .

1. Soit (E, b) un espace sesquilineaire symétrique. On suppose b non nulle.

(a) Montrer qu'il existe un vecteur $x \in E$ tel que $b(x, x)$ soit non nul.

- (b) Montrer qu'il existe un vecteur $y \in E$ tel que $b(y, y)$ soit égal à 1 ou à -1 .
2. Soit (E, b) un espace sesquilinéaire symétrique. Montrer qu'il existe une base semi-orthonormée de (E, b) .
3. On suppose que E est l'espace vectoriel \mathbb{C}^2 et que la forme b est définie par la matrice $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Construire une base semi-orthonormée de (E, b) .
4. Soient (E, b) un espace sesquilinéaire symétrique et $\mathcal{B} = (e_1, e_2, \dots, e_n)$ une base semi-orthonormée de (E, b) . On désigne par E_+ [resp. E_- , E_0] le sous-espace-vectoriel de E engendré par les vecteurs e_i vérifiant $b(e_i, e_i) = 1$ [resp. $b(e_i, e_i) = -1$, $b(e_i, e_i) = 0$]. Soit F un sous-espace-vectoriel de E .
- (a) Montrer que $F \cap (E_- \oplus E_0)$ est nul si b est définie positive sur F et que $F \cap (E_+ \oplus E_0)$ est nul si b est définie négative sur F .
- (b) En déduire que le nombre $\sum_{i=1}^n b(e_i, e_i)$ est indépendant de \mathcal{B} . Ce nombre est noté $\sigma(E, b)$ ou simplement $\sigma(E)$ s'il n'y a pas d'ambiguïté.
5. On suppose que E est l'espace vectoriel \mathbb{C}^n , avec $n \geq 1$, muni de sa base canonique $\mathcal{B} = (e_1, e_2, \dots, e_n)$, et que la forme b est définie par :

$$b(e_i, e_j) = \begin{cases} 1 & \text{si } i + j = n + 1, \\ 0 & \text{sinon.} \end{cases}$$

Calculer le nombre $\sigma(E)$.

6. Soient (E, b) un espace sesquilinéaire symétrique et x un vecteur non nul de E .
- (a) On suppose que x appartient à E^\perp . Montrer qu'il existe une base semi-orthonormée $\mathcal{B} = (e_1, e_2, \dots, e_n)$ telle que $x = e_1$.
- (b) On suppose que $b(x, x)$ est non nul. Montrer qu'il existe une base semi-orthonormée $\mathcal{B} = (e_1, e_2, \dots, e_n)$ et un réel $\lambda > 0$ tels que $x = \lambda e_1$.
- (c) On suppose que $b(x, x)$ est nul et que x n'appartient pas à E^\perp . Montrer qu'il existe une base semi-orthonormée $\mathcal{B} = (e_1, e_2, \dots, e_n)$ telle que $x = e_1 + e_2$.
7. Soit (E, b) un espace sesquilinéaire symétrique. Soit $F = \mathbb{C}x$ le sous-espace vectoriel de E engendré par un vecteur non nul $x \in E$ et $G = F^\perp$ son orthogonal. Déterminer l'espace G suivant les cas examinés dans la question **I.6**. Montrer que l'on a dans tous les cas $\sigma(E) = \sigma(F) + \sigma(G)$.
8. Soit (E, b) un espace sesquilinéaire symétrique. Soit F un sous-espace vectoriel de E engendré par un vecteur non nul $x \in E$ et $G = F^\perp$ son orthogonal. Soit (u_1, u_2, \dots, u_p) une base semi-orthonormée de (F, b) . Pour tout i compris entre 1 et p on note F_i le sous-espace vectoriel engendré par les vecteurs u_j où j est compris entre 1 et i et G_i l'orthogonal F_i^\perp de F_i . Déterminer, en fonction de $\sigma(E)$, les nombres $\sigma(F_i) + \sigma(G_i)$. En déduire la formule :

$$\sigma(E) = \sigma(F) + \sigma(F^\perp).$$

Soit (E, b) un espace sesquilinéaire. Si F est un sous-espace vectoriel de E , on appelle orthogonal à droite [resp. orthogonal à gauche] de F l'ensemble note F^\perp [resp. ${}^\perp F$] des vecteurs x de E tels que :

$$\forall y \in F, \quad b(y, x) = 0 \quad [\text{resp. } b(x, y) = 0]$$

On dit que la forme b est non dégénérée si E^\perp et ${}^\perp E$ sont nuls.

Si F est un sous-espace vectoriel de E , on dit que b est non dégénérée sur F si la restriction de b à F est non dégénérée.

1. Soient (E, b) un espace sesquilinéaire, $\mathcal{B} = (e_1, e_2, \dots, e_n)$ une base de E et M la matrice de b dans cette base.

(a) Soient x, y deux vecteurs de E et X, Y les matrices colonnes ayant comme coefficients les coordonnées de x et y dans la base \mathcal{B} . Montrer que :

$$\forall (x, y) \in E^2, \quad b(x, y) = {}^t X M \bar{Y}.$$

(b) Montrer que les conditions suivantes sont équivalentes :

- i. b est non dégénérée ;
- ii. M est inversible ;
- iii. $E^\perp = \{0\}$;
- iv. ${}^\perp E = \{0\}$.

2. Montrer que si (E, b) est un espace sesquilinéaire symétrique, alors :

$$\sigma(E, b) \equiv \dim(E) - \dim(E^\perp) \pmod{2}.$$

3. Soient (E, b) un espace sesquilinéaire et F un sous-espace vectoriel de E .

(a) Montrer que F^\perp et ${}^\perp F$ sont des sous-espaces vectoriels de E .

(b) Montrer les inégalités :

$$\begin{cases} \dim(F) + \dim(F^\perp) \geq \dim(E) \\ \dim(F) + \dim({}^\perp F) \geq \dim(E) \end{cases}$$

Montrer que ces inégalités sont des égalités si b est non dégénérée (sur E).

(c) On suppose que b est non dégénérée sur F . Montrer que :

$$E = F \oplus F^\perp = F \oplus {}^\perp F.$$

(d) On suppose que b est non dégénérée sur F . Montrer que :

$${}^\perp(F^\perp) = ({}^\perp F)^\perp = F.$$

4. Soient E l'espace vectoriel \mathbb{C}^2 muni de sa base canonique (e_1, e_2) et b la forme sesquilinéaire sur E vérifiant :

$$b(e_i, e_1) = 0, \quad b(e_i, e_2) = 1 \quad (i = 1, 2)$$

Déterminer un sous-espace vectoriel F de E tel que F^\perp et ${}^\perp F$ n'aient pas la même dimension.

5. Montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{C})$ est de rang r si et seulement si elle est équivalente à $A_r = \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$ où I_r désigne la matrice identité d'ordre r .
6. Soit (E, b) un espace sesquilinéaire. Montrer qu'il existe un endomorphisme bijectif f de E tel que la forme $(x, y) \mapsto b(f(x), y)$ soit une forme sesquilinéaire symétrique.
7. Soit (E, b) un espace sesquilinéaire. Soit ε un nombre complexe. On dit que b est ε -symétrique si l'on a :

$$\forall (x, y) \in E^2, \quad b(x, y) = \varepsilon \overline{b(y, x)}$$

On dira dans ce cas que (E, b) est ε -symétrique.

- (a) Montrer que si la forme b est ε -symétrique et non nulle, alors $\varepsilon \bar{\varepsilon} = 1$.
- (b) Soit ε un nombre complexe tel que $\varepsilon \bar{\varepsilon} = 1$. Donner un exemple d'espace sesquilinéaire (E, b) où b est ε -symétrique et non nulle.
8. Soit ε un nombre complexe tel que $\varepsilon \bar{\varepsilon} = 1$. Soit (E, b) un espace sesquilinéaire ε -symétrique.
- (a) Montrer qu'il existe un nombre complexe α non nul tel que αb soit une forme sesquilinéaire symétrique.
- (b) Soit β un nombre complexe non nul. Déterminer à quelle condition (portant sur α et β) la forme βb est symétrique. Déterminer (en fonction de $\sigma(E, \alpha b)$, α et β) le nombre $\sigma(E, \beta b)$.

– III – Espaces semi-quadratiques

Soit α un nombre complexe non nul. On pose $\varepsilon = -\frac{\alpha}{\bar{\alpha}}$. On appelle espace α -semi-quadratique un triplet (E, b, f) où E est un espace vectoriel de dimension finie sur \mathbb{C} , b une forme sesquilinéaire sur E non dégénérée et f une forme linéaire sur E et tel que :

$$\forall (x, y) \in E^2, \quad b(x, y) - \varepsilon \overline{b(y, x)} = \alpha f(x) \overline{f(y)}.$$

Un espace α -semi-quadratique (E, b, f) sera dit de type $T0$ si f est nulle et de type $T1$ sinon.

Soient $\mathcal{E} = (E, b, f)$ et $\mathcal{E}' = (E', b', f')$ deux espaces α -semi-quadratiques. On appelle isomorphisme de \mathcal{E} sur \mathcal{E}' une application linéaire bijective φ de E sur E' ayant les propriétés suivantes :

$$\begin{cases} \forall x \in E, & f'(\varphi(x)) = f(x), \\ \forall (x, y) \in E^2, & b'(\varphi(x), \varphi(y)) = b(x, y). \end{cases}$$

On dit que \mathcal{E} et \mathcal{E}' sont isomorphes s'il existe un isomorphisme de \mathcal{E} sur \mathcal{E}' .

1. Soient (E, b) un espace sesquilinéaire, f une forme linéaire non nulle sur E et u un complexe tel que $u\bar{u} = 1$. On suppose que l'on a :

$$\forall (x, y) \in E^2, \quad b(x, y) - u \overline{b(y, x)} = \alpha f(x) \overline{f(y)}.$$

Montrer que u est égal à ε .

2. Soit $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique.

- (a) Montrer qu'il existe un unique vecteur $e \in E$ vérifiant la condition suivante :

$$\forall x \in E, \quad b(x, e) = f(x).$$

Ce vecteur sera appelé vecteur centre de \mathcal{E} .

(b) Soit λ le complexe défini par :

$$f(e) = \frac{1 - \lambda}{\bar{\alpha}}.$$

Montrer que $\lambda\bar{\lambda} = 1$.

Cet élément λ sera appelé le poids de \mathcal{E} .

3. Déterminer le vecteur centre et le poids d'un espace α -semi-quadratique de type $T0$.
4. Soient $\mathcal{E} = (E, b, f)$ et $\mathcal{E}' = (E', b', f')$ deux espaces α -semi-quadratiques isomorphes. Montrer qu'ils ont même poids.
5. Soient $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique de type $T1$, e le vecteur centre de \mathcal{E} , x un vecteur non nul de E et F l'orthogonal à gauche du sous-espace vectoriel de E engendré par x .

(a) Montrer que $\ker(f)$ est égal à F si, et seulement si, x est colinéaire à e .

(b) Déterminer l'orthogonal à droite de $\ker(f)$.

6. Soit λ un complexe différent de 1 tel que $\lambda\bar{\lambda} = 1$. Montrer qu'il existe une unique forme sesquilinéaire b sur \mathbb{C} telle que (\mathbb{C}, b, Id) soit un espace α -semi-quadratique de poids λ .
7. Montrer que deux espaces α -semi-quadratiques de dimension 1 et de type $T1$ sont isomorphes si, et seulement si, ils ont même poids.
8. Soit $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique de type $T1$ de dimension 2, de poids $\lambda = 1$ et de vecteur centre e .

(a) Soit x un vecteur de E tel que $f(x) = 1$. Montrer que la partie réelle de $\frac{b(x, x)}{\alpha}$ est égale à $\frac{1}{2}$.

(b) Montrer qu'il existe un vecteur x de E tel que $f(x) = 1$ et $b(x, x) = \frac{\alpha}{2}$.

(c) En déduire que deux espaces α -semi-quadratiques de type $T1$ de dimension 2 et de poids $\lambda = 1$ sont isomorphes.

9. Soient $\mathcal{E} = (E, b, f)$ et $\mathcal{E}' = (E', b', f')$ deux espaces α -semi-quadratiques. Montrer qu'il existe une unique forme sesquilinéaire b'' sur $E'' = E \times E'$ et une unique forme linéaire f'' sur E'' vérifiant les conditions suivantes :

(a) $\forall (x, x') \in E \times E', f''(x, x') = f(x) + f'(x')$;

(b) $\forall (x, y) \in E^2, b''((x, 0), (y, 0)) = b(x, y)$;

(c) $\forall (x', y') \in E^2, b''((0, x'), (0, y')) = b'(x', y')$;

(d) $\forall (x, y') \in E \times E', b''((x, 0), (0, y')) = 0$;

(e) $\mathcal{E}'' = (E'', b'', f'')$ est un espace α -semi-quadratique.

Calculer $b''((x, x'), (y, y'))$ pour tous (x, x') et (y, y') dans E'' .

L'espace α -semi-quadratique \mathcal{E}'' sera appelé produit orthogonal de \mathcal{E} et de \mathcal{E}' et noté $\mathcal{E} \times \mathcal{E}'$.

10. Soient $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique et F un sous-espace vectoriel de E . On suppose que b est non dégénérée sur F . On note b_0 et f_0 les restrictions de b et f à F , b_1 et f_1 les restrictions de b et f à F^\perp , b_2 et f_2 les restrictions de b et f à ${}^\perp F$.

- (a) Montrer que $\mathcal{F} = (F, b_0, f_0)$, $\mathcal{F}^\perp = (F^\perp, b_1, f_1)$ et ${}^\perp\mathcal{F} = ({}^\perp F, b_2, f_2)$ sont des espaces α -semi-quadratiques.
- (b) Montrer que \mathcal{E} est isomorphe au produit orthogonal de \mathcal{F} et de \mathcal{F}^\perp , ainsi qu'au produit orthogonal de ${}^\perp\mathcal{F}$ et de \mathcal{F} .
11. Soient $\mathcal{E} = (E, b, f)$ et $\mathcal{E}' = (E', b', f')$ deux espaces α -semi-quadratiques, e et e' leurs vecteurs centres, λ et λ' leurs poids.
- (a) Déterminer le vecteur centre du produit orthogonal \mathcal{E}'' de \mathcal{E} et de \mathcal{E}' .
- (b) Montrer que le poids de \mathcal{E}'' est égal à $\lambda\lambda'$.
12. Soient $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique et F le noyau de f .
- (a) Montrer que b est non dégénérée sur F si, et seulement si, le poids de \mathcal{E} est différent de 1 ou si \mathcal{E} est de type $T0$.
- (b) Montrer que $i\bar{\alpha}b$ est une forme symétrique sur F .
- Si $\mathcal{E} = (E, b, f)$ est un espace α -semi-quadratique, on appelle pseudo-signature de \mathcal{E} le nombre $\text{ps}(\mathcal{E}) = \sigma(\ker(f), i\bar{\alpha}b)$.
13. Soient $\mathcal{E} = (E, b, f)$ et $\mathcal{E}' = (E', b', f')$ deux espaces α -semi-quadratiques. On suppose que \mathcal{E} ou \mathcal{E}' est de type $T0$. Déterminer la pseudo-signature de $\mathcal{E} \times \mathcal{E}'$ en fonction des pseudo-signatures de \mathcal{E} et de \mathcal{E}' .
14. Soient $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique de type $T1$ et E_1, E_2 deux sous-espaces vectoriels de E tels que $E = E_1 \oplus E_2$. On suppose que E_2 est l'orthogonal à droite de E_1 et que f n'est nulle ni sur E_1 ni sur E_2 .

(a) Montrer que les restrictions de b et f induisent sur E_1 et E_2 deux structures d'espaces α -semi-quadratiques de type $T1$, que l'on notera \mathcal{E}_1 et \mathcal{E}_2 .

(b) Soient e_1 et e_2 les vecteurs centres de \mathcal{E}_1 et \mathcal{E}_2 , F le noyau de f , F_1 et F_2 les intersections de F avec E_1 et E_2 .

i. Montrer l'inclusion :

$$F \cap (F_1 \oplus F_2)^\perp \subset \mathbb{C}e_1 \oplus \mathbb{C}e_2.$$

ii. En déduire que l'intersection de F et de $(F_1 \oplus F_2)^\perp$ est engendrée par e_1 et e_2 si les poids de \mathcal{E}_1 et \mathcal{E}_2 sont égaux à 1, et par $f(e_2)e_1 - f(e_1)e_2$ sinon.

(c) Soient λ, λ_1 et λ_2 les poids de $\mathcal{E}, \mathcal{E}_1$ et \mathcal{E}_2 . Montrer que le nombre $\text{ps}(\mathcal{E}) - \text{ps}(\mathcal{E}_1) - \text{ps}(\mathcal{E}_2)$ est égal à 1, 0 ou -1 suivant que $\Im(\lambda_1) + \Im(\lambda_2) - \Im(\lambda)$ est strictement positif, nul ou strictement négatif (on peut utiliser les résultats de la première partie).

Soient $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique et λ son poids. On pose

$$\sigma(\mathcal{E}) = \begin{cases} \text{ps}(\mathcal{E}) & \text{si } \lambda = 1 \\ \text{ps}(\mathcal{E}) + 1 - \frac{\arg(\lambda)}{\pi} & \text{si } \lambda \neq 1 \end{cases}$$

Le nombre $\sigma(\mathcal{E})$ est appelé signature de \mathcal{E} .

15. Soit $\mathcal{E} = (E, b, f)$ un espace α -semi-quadratique de dimension n , de signature σ , de poids λ et de pseudo-signature s .
- (a) Montrer que $\lambda = 1$ si, et seulement si, $\sigma - n$ est un entier pair.

(b) En déduire les formules :

$$\begin{cases} \lambda = e^{i\pi(n-\sigma)} \\ s = \begin{cases} \sigma & \text{si } \sigma - n \in 2\mathbb{Z} \\ n + 1 + 2 \left[\frac{\sigma - n}{2} \right] & \text{sinon} \end{cases} \end{cases}$$

16. On reprend les notations et hypothèses de la question 14. On pose $\lambda_1 = e^{i\beta}$, $\lambda_2 = e^{i\gamma}$ avec $0 \leq \beta < 2\pi$, $0 \leq \gamma < 2\pi$ et $k = 1, 2$ ou 3 suivant que $\beta + \gamma - 2\pi$ est strictement négatif, nul ou strictement positif.
- (a) Calculer $\sigma(\mathcal{E}) - \sigma(\mathcal{E}_1) - \sigma(\mathcal{E}_2) - (\text{ps}(\mathcal{E}) - \text{ps}(\mathcal{E}_1) - \text{ps}(\mathcal{E}_2))$ en fonction de β , γ et k .
- (b) En déduire que $\sigma(\mathcal{E}) = \sigma(\mathcal{E}_1) + \sigma(\mathcal{E}_2)$.
- (c) Montrer que la signature d'un produit orthogonal de deux espaces α -semi-quadratiques est la somme de leurs signatures.
17. Soit σ un réel dans $[-1, 1]$. Montrer qu'il existe un espace α -semi-quadratique \mathcal{E} de dimension 1 et de signature σ .
18. Soient σ un réel et n un entier. Montrer qu'il existe un espace α -semi-quadratique \mathcal{E} de dimension n et de signature σ si, et seulement si, $|\sigma| \leq n$.
19. Montrer que deux espaces α -semi-quadratiques \mathcal{E} et \mathcal{E}' sont isomorphes si, et seulement si, ils ont même dimension, même type et même signature.

Agrégation externe 2003. Épreuve 1

Pour tout entier $n \geq 1$, on note $GL_n(\mathbb{C})$ le groupe des matrices carrées inversibles de taille n à coefficients dans le corps \mathbb{C} des nombres complexes.

On note U_n le sous-groupe de $GL_n(\mathbb{C})$ formé des matrices unitaires.

Si V est un espace vectoriel complexe, on peut restreindre à $\mathbb{R} \times V$ la loi de multiplication par les complexes $\mathbb{C} \times V \rightarrow V$ et on obtient alors sur le groupe additif de V une structure d'espace vectoriel réel qu'on appelle espace vectoriel réel sous-jacent à V .

Pour tout espace vectoriel complexe V de dimension $n \geq 1$, on note $End(V)$ l'algèbre des endomorphismes de V et $GL(V)$ le groupe des automorphismes de V .

On note Id_V l'automorphisme identité de V .

On dit qu'une partie non vide X de $End(V)$ est diagonalisable s'il existe une base de V telle que la matrice dans cette base de tout élément de X soit diagonale.

Une forme hermitienne sur V est une application $\Phi : V \times V \rightarrow \mathbb{C}$ qui est sesquilinéaire (i. e. linéaire à droite et antilinéaire à gauche) et telle que $\Phi(y, x) = \overline{\Phi(x, y)}$ pour tous x, y dans V .

Une telle forme est dite définie positive si le réel $\Phi(x, x)$ est strictement positif pour tout vecteur non nul x de V .

On appelle espace hermitien un espace vectoriel complexe de dimension finie muni d'une forme hermitienne définie positive.

Si Φ est une forme hermitienne définie positive sur V , on rappelle que pour tout $u \in End(V)$, l'adjoint (pour Φ) de u , noté u^* est l'endomorphisme de V défini par :

$$\forall (x, y) \in V^2, \quad \Phi(u(x), y) = \Phi(x, u^*(y)).$$

On dit que u est hermitien (pour Φ) si $u^* = u$ et qu'il est unitaire (pour Φ) si $u^* \circ u = Id_V$.

On note $U(V)$ le sous-groupe de $GL(V)$ formé des endomorphismes de V unitaires pour Φ et $SU(V)$ le sous-groupe de $U(V)$ formé des endomorphismes unitaires de déterminant égal à 1.

Si E est un espace vectoriel réel et q une forme quadratique définie positive sur E , on rappelle qu'une isométrie de q est un endomorphisme de E tel que $q(u(x)) = q(x)$ pour tout x dans E . On note $O(q)$ le sous-groupe du groupe des automorphismes de E constitué des isométries de q et $SO(q)$ le sous-groupe de $O(q)$ formé des isométries de déterminant égal à 1.

– I – Généralités

Pour cette partie, V désigne un espace vectoriel complexe de dimension $n \geq 1$.

1. Soient u, v dans $GL(V)$. Pour tout $\lambda \in \mathbb{C}$, on note :

$$\begin{cases} t = v \circ u \circ v^{-1} \\ U_\lambda = \ker(u - \lambda Id_V) \\ T_\lambda = \ker(t - \lambda Id_V) \end{cases}$$

- (a) Calculer, pour tout $\lambda \in \mathbb{C}$, T_λ en fonction de U_λ et de v .
 - (b) Montrer que si u et v commutent, on a alors $v(U_\lambda) = U_\lambda$ pour tout $\lambda \in \mathbb{C}$.
 - (c) On suppose que u et v commutent et que v est diagonalisable. Montrer que pour toute valeur propre λ de u , v induit un endomorphisme diagonalisable de U_λ .
2. Montrer que tout élément d'ordre fini de $GL(V)$ est diagonalisable.
 3. Soit X une partie de $End(V)$ formée d'endomorphismes diagonalisables qui commutent deux à deux. Montrer que X est diagonalisable.
 4. Donner un exemple de sous-groupe abélien de $GL(\mathbb{C}^2)$ qui ne soit pas diagonalisable.
 5. Soit Ψ une forme hermitienne définie positive sur V et G un sous-groupe fini de $GL(V)$. Construire, à partir de Ψ , une forme hermitienne définie positive Φ sur V telle que tous les éléments de G soient unitaires pour Φ .
 6. En déduire qu'un sous-groupe fini de $GL_n(\mathbb{C})$ est conjugué à un sous-groupe de U_n .

– II – Le cas où n vaut 2

Pour cette partie, V désigne un espace vectoriel complexe de dimension $n = 2$ muni d'une forme hermitienne définie positive Φ .

On note E l'ensemble des endomorphismes hermitiens de V de trace nulle.

Cet ensemble E est un sous-espace vectoriel de l'espace vectoriel réel sous-jacent à $End(V)$.

On définit l'application q sur E par :

$$\forall x \in E, \quad q(x) = -\det(x).$$

1. Calculer la dimension sur \mathbb{R} de E .
2. Montrer que q est une forme quadratique définie positive sur E et déterminer sa forme polaire (i. e. la forme bilinéaire symétrique $B : E \times E \rightarrow \mathbb{R}$ telle que $q(x) = B(x, x)$ pour tout x dans E).
3. Montrer que pour tout a dans $U(V)$ et tout x dans E , axa^{-1} est dans E .
Pour tout a dans $U(V)$, on note $\varphi(a)$ l'application $x \mapsto axa^{-1}$. C'est un endomorphisme de E .
4. Montrer que pour tout a dans $U(V)$, $\varphi(a)$ est une isométrie de q .
L'application $\varphi : a \mapsto \varphi(a)$ est un morphisme de groupes de $U(V)$ vers $O(q)$ (on ne demande pas de le vérifier).
5. Déterminer le noyau de φ .
6. Soit a dans $U(V)$ qui n'est pas dans le noyau de φ . Montrer que $\varphi(a)$ est une rotation de E en précisant, après le choix d'une orientation de E , un couple (*axe, angle*) de cette rotation en termes de vecteurs propres et valeurs propres de a .
7. Déterminer l'image de φ .

8. Montrer que $SU(V)$ contient un sous-groupe fini G dont tout sous-groupe abélien distingué est d'indice au moins 60 (on pourra utiliser le groupe des isométries positives d'un icosaèdre régulier, en admettant qu'un espace affine euclidien de dimension 3 contient un tel icosaèdre).
9. On désigne par G un sous-groupe de $U(V)$ et par Z le sous-groupe de G formé des homothéties qui appartiennent à G .
On suppose que Z est distinct de G .
On note $H = \frac{G}{Z}$ le groupe quotient de G par son sous-groupe distingué H et m est le cardinal de H .
Les éléments de G qui ne sont pas dans Z ont exactement deux droites propres (qui sont orthogonales). On note \mathcal{D} l'ensemble des droites de V ainsi obtenues.

(a)

- i. Montrer que pour tous g dans G et D dans \mathcal{D} , la droite $g(D)$ est dans \mathcal{D} .
- ii. Montrer que l'application (g, D) de $G \times \mathcal{D}$ dans \mathcal{D} induit une action du groupe H sur l'ensemble \mathcal{D} .

On note $(h, D) \mapsto h \cdot D$ cette action et pour tout $D \in \mathcal{D}$, e_D désigne le cardinal du stabilisateur de D dans H .

(b) Montrer que :

- i. $e_D \geq 2$ pour tout $D \in \mathcal{D}$;
- ii. $2(m - 1) = \sum_{D \in \mathcal{D}} (e_D - 1)$;
- iii. si D, D' sont dans la même orbite sous l'action de H alors $e_D = e_{D'}$.

(c) On note $\Omega_1, \dots, \Omega_r$ les orbites de \mathcal{D} sous l'action de H et pour tout i compris entre 1 et r , e_i désigne la valeur commune des e_D pour $D \in \Omega_i$. On range ces orbites de manière à avoir $e_1 \leq e_2 \leq \dots \leq e_r$.

- i. Calculer $\sum_{i=1}^r \left(1 - \frac{1}{e_i}\right)$ en fonction de m .
- ii. Montrer que r vaut 2 ou 3.

(d) Montrer que si r vaut 2, alors G est abélien.

(e) Montrer que si r vaut 3 et $e_1 = e_2 = 2$, $e_3 \geq 2$, alors G possède un sous-groupe abélien distingué d'indice 2.

10. En examinant les possibilités autres que celles envisagées en **II.9d** et **II.9e**, montrer que tous sous-groupe fini G de $GL_2(\mathbb{C})$ possède un sous-groupe abélien distingué d'indice au plus 60 dans G .

– III – La méthode de Frobenius

Pour cette partie, n est un entier au moins égal à 2 et V désigne un espace vectoriel hermitien de dimension n . On note Φ la forme hermitienne définie positive donnée sur V .

1. Pour cette question, on fixe un réel $\tau \in \left[0, \frac{\pi}{2}\right[$ et un élément v de $U(V)$. On suppose que pour chaque valeur propre γ de v , il existe $\theta \in [-\tau, \tau]$ tel que $\gamma = e^{i\theta}$.

- (a) Montrer que pour tout vecteur non nul x de V , il existe un réel $r > 0$ et un réel $\alpha \in [-\tau, \tau]$ tels que $\Phi(v(x), x) = re^{i\alpha}$.
- (b) Soit u dans $U(V)$ et $t = v \circ u \circ v^{-1}$. Pour tout $\lambda \in \mathbb{C}$, on note $U_\lambda = \ker(u - \lambda Id_V)$, $T_\lambda = \ker(t - \lambda Id_V)$ et on note U_λ^\perp l'orthogonal de U_λ dans V .
- Montrer que $T_\lambda \cap U_\lambda^\perp = \{0\}$.
 - On suppose de plus que u et t commutent. Montrer que pour tout $\lambda \in \mathbb{C}$ on a $T_\lambda = U_\lambda$, de sorte que $t = u$ et que u et v commutent.
- (c) Soit s dans $U(V)$. On suppose que pour chaque valeur propre σ de s , il existe $\alpha \in [-\tau, \tau]$ tel que $\sigma = e^{i\alpha}$.
Montrer que pour toute valeur propre μ de $v \circ s^{-1}$, il existe $\beta \in [-2\tau, 2\tau]$ tel que $\mu = e^{i\beta}$ (on pourra considérer un vecteur x de V tel que $(v - \mu s)(x) = 0$).
Pour $g \in \text{End}(V)$, on note $N(g)$ la trace de $g^* \circ g$. Si $A = ((a_{i,j}))_{1 \leq i,j \leq n}$ est la matrice de g dans une base orthonormée de V , on a $N(g) = \sum_{1 \leq i,j \leq n} |a_{i,j}|^2$, de sorte que N est une forme quadratique définie positive sur l'espace vectoriel réel E sous-jacent à $\text{End}(V)$. On note $g \mapsto \|g\| = \sqrt{N(g)}$ la norme euclidienne correspondante sur E .
- (d) Montrer que pour tout u dans $U(V)$, on a :

$$N(vuv^{-1}u^{-1} - Id_V) \leq 4 \sin^2(\tau) N(u - Id_V)$$

(on pourra, en prenant une base de vecteurs propres de v , estimer la quantité $N(v(u - Id_V) - (u - Id_V)v)$).

2. Pour cette question G désigne un sous-groupe fini de $U(V)$. On note S l'ensemble des éléments s de G tels que pour toute valeur propre σ de s , il existe $\alpha \in \left] -\frac{\pi}{6}, \frac{\pi}{6} \right[$ tel que $\sigma = e^{i\alpha}$. On note A le sous-groupe de G engendré par S .

- (a) Soient v dans S et u dans G . On définit par récurrence sur l'entier naturel k , un élément u_k de $U(V)$ en posant :

$$u_0 = u \text{ et } u_{k+1} = vu_k v^{-1} u_k^{-1} \text{ pour tout } k \in \mathbb{N}.$$

- Montrer que pour k assez grand on a $u_k = Id_V$.
 - On suppose en outre que pour toute valeur propre λ de u , il existe $\theta \in \left] -\frac{\pi}{2}, \frac{\pi}{2} \right[$ tel que $\lambda = e^{i\theta}$. Montrer que u et v commutent (on pourra remarquer que, pour $k \geq 1$, dire que $u_{k+1} = Id_V$ signifie que v commute à $u_{k-1} v u_{k-1}^{-1}$).
- (b) Montrer qu'il existe un réel $\eta > 0$ indépendant de n tel que deux éléments g et h de G vérifiant $N(g - h) < \eta$ vérifient aussi $h^{-1}g \in S$.
- (c) Prouver que l'indice de A dans G vaut au plus :

$$a(n) = \left(2\sqrt{\frac{n}{\eta}} + 1 \right)^{2n^2} - \left(2\sqrt{\frac{n}{\eta}} - 1 \right)^{2n^2}$$

(prendre un système de représentants de G/A dans G ; il sera commode de noter m la mesure de la boule unité de l'espace vectoriel euclidien E).

3. Conclure en prouvant le théorème de Jordan : tout sous-groupe fini G de $GL_n(\mathbb{C})$ possède un sous-groupe abélien distingué d'indice au plus $a(n)$ dans G .

Agrégation externe 2004. Épreuve 1

Si R est un anneau commutatif unitaire, on note 1 son élément unité et R^\times le groupe des éléments inversibles de R .

Si m, n sont deux entiers naturels non nuls, on note $\mathcal{M}_{m,n}(R)$ l'ensemble des matrices à m lignes et n colonnes à coefficients dans R . Pour simplifier on note $\mathcal{M}_n(R)$ l'anneau des matrices carrées $\mathcal{M}_{n,n}(R)$.

On note $GL_n(R)$ le groupe des éléments de $\mathcal{M}_n(R)$ de déterminant dans R^\times .

On note I_n la matrice identité de $\mathcal{M}_n(R)$.

Le sous-ensemble de $\mathcal{M}_n(R)$ formé des matrices symétriques est noté $S_n(R)$.

Pour tout nombre premier p , on note \mathbb{F}_p le corps $\frac{\mathbb{Z}}{p\mathbb{Z}}$ des classes résiduelles modulo p .

Pour ce problème, on se fixe un nombre premier impair p et on considère deux matrices symétriques $S \in S_m(\mathbb{F}_p)$ et $T \in S_n(\mathbb{F}_p)$ de déterminants respectifs s et t non nuls.

On note :

$$\mathcal{A}_p(S, T) = \{X \in \mathcal{M}_{m,n}(\mathbb{F}_p) \mid {}^t X S X = T\}$$

et $A_p(S, T)$ est le cardinal de $\mathcal{A}_p(S, T)$.

Pour tout entier naturel non nul n , on note $[1, n]$ l'ensemble des entiers compris entre 1 et n .

– I – Un cas particulier

Pour cette partie, $m = 2$, $n = 1$, s et t sont deux éléments non nuls de \mathbb{F}_p , $S = \begin{pmatrix} 1 & 0 \\ 0 & s \end{pmatrix}$ et $T = (t)$ est identifié à t . Ainsi $A_p(S, T)$ est le nombre de couples (x, y) de \mathbb{F}_p^2 tels que $x^2 + sy^2 = t$.

1. On suppose que $-s$ est un carré dans \mathbb{F}_p . Calculer $A_p(S, T)$.
2. Pour la suite de cette partie, on suppose que $-s$ n'est pas un carré dans \mathbb{F}_p .
 - (a) Montrer que le polynôme $X^2 + s$ est irréductible sur \mathbb{F}_p . Soit \mathbb{K} un corps de rupture. Quel le cardinal de \mathbb{K} ?
 - (b) Soit $F : \mathbb{K} \rightarrow \mathbb{K}$, $z \mapsto z^p$. Montrer que F est un automorphisme involutif de corps et déterminer ses points fixes.
 - (c) Soit α une racine de $X^2 + s$ dans \mathbb{K} . Montrer que $F(\alpha) = -\alpha$.
3. Soit $N : \mathbb{K}^\times \rightarrow \mathbb{K}^\times$, $z \mapsto z^{p+1}$.
 - (a) Montrer que N est un morphisme de groupes d'image contenue dans \mathbb{F}_p^\times .

- (b) Déterminer le cardinal du noyau et de l'image de N .
 (c) Calculer $N(x + \alpha y)$ pour x, y dans \mathbb{F}_p non tous deux nuls.
4. Calculer $A_p(S, T)$.

– II – Préliminaires

Pour cette partie, m est un entier naturel non nul et V un \mathbb{F}_p -espace vectoriel de dimension m .

1. Soit $b : V \times V \rightarrow \mathbb{F}_p$ une forme bilinéaire symétrique sur V .
- (a) Montrer que si $b(x, x)$ est nul pour tout x dans V , alors la forme bilinéaire b est nulle.
- (b) Montrer que V possède une base $(e_i)_{1 \leq i \leq m}$ orthogonale pour b .
- (c) En déduire qu'il existe une matrice diagonale $D \in \mathcal{M}_m(\mathbb{F}_p)$ et une matrice inversible $P \in GL_m(\mathbb{F}_p)$ telles que $S = {}^tPDP$.
2. Pour cette question, $V = \mathcal{M}_{m,1}(\mathbb{F}_p)$ et b est définie par $b(X, Y) = {}^tXSY$.
 Montrer que pour tout entier naturel non nul n et toute matrice $T = ((t_{i,j}))_{1 \leq i, j \leq n}$ dans $S_n(\mathbb{F}_p)$, $A_p(S, T)$ est le nombre de n -uplets (v_1, \dots, v_n) d'éléments de V vérifiant $b(v_i, v_j) = t_{i,j}$ pour tous i, j dans $[1, n]$.
3. Vérifier que pour toutes matrices $P \in GL_m(\mathbb{F}_p)$ et $Q \in GL_n(\mathbb{F}_p)$, on a :

$$A_p(S, T) = A_p({}^tPSP, {}^tQTQ).$$

4. Soit Φ la fonction indicatrice d'Euler qui à un entier naturel non nul r associe le nombre d'entiers de $[1, r]$ premiers à r .
- (a) Montrer que pour tout entier naturel non nul r , on a $\sum_{d/r} \Phi(d) = r$, la somme étant étendue à tous les entiers strictement positifs d diviseurs de r .
- (b) Soit \mathbb{K} un corps fini commutatif à q éléments. Démontrer que pour tout entier strictement positif d diviseur de $q - 1$, l'ensemble des éléments de \mathbb{K}^\times d'ordre divisant d est de cardinal au plus d .
- (c) En déduire que pour tout entier strictement positif d diviseur de $q - 1$, \mathbb{K}^\times possède 0 ou $\Phi(d)$ éléments d'ordre exactement d .
- (d) En déduire que \mathbb{K}^\times est cyclique.

– III – Le cas $n = 1$

Soit $n = 1$; on a alors $T = t \in \mathbb{F}_p$ et $2st \neq 0$ où l'on rappelle que $s = \det(S)$.

Soit $\omega = \exp\left(\frac{2i\pi}{p}\right)$ une racine primitive p -ème de l'unité.

Pour $\alpha \in \mathbb{Z}$ le nombre complexe ω^α ne dépend que de la classe a de α modulo p ; on le note ω^a : on admettra que l'on définit ainsi un morphisme $a \mapsto \omega^a$ du groupe additif \mathbb{F}_p dans le groupe multiplicatif \mathbb{C}^\times .

Pour $a \in \mathbb{F}_p^\times$, on pose $\left(\frac{a}{p}\right) = 1$ s'il existe $b \in \mathbb{F}_p^\times$ tel que $a = b^2$ et $\left(\frac{a}{p}\right) = -1$ sinon.

1.

(a) Montrer qu'il y a dans \mathbb{F}_p^\times autant de carrés que de non carrés et que l'application $a \mapsto \left(\frac{a}{p}\right)$ est un morphisme de groupes multiplicatifs de \mathbb{F}_p^\times dans \mathbb{C}^\times .

(b) Pour $b \in \mathbb{F}_p$ calculer $\sum_{a \in \mathbb{F}_p} \omega^{ab}$.

(c) Pour $c \in \mathbb{F}_p^\times$, on pose $G_c = \sum_{a \in \mathbb{F}_p} \omega^{ca^2}$ et $H_c = \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right) \omega^{ca}$.

Démontrer qu'on a :

$$G_c = H_c = \left(\frac{c}{p}\right) G_1.$$

Dans ce qui suit, G_1 sera noté G .

2.

(a) Montrer que :

$$pA_p(S, T) = \sum_{a, X} \omega^{a(tXSX-t)}$$

où a parcourt \mathbb{F}_p et X parcourt $\mathcal{M}_{m,1}(\mathbb{F}_p)$.

(b) Soit D une matrice diagonale inversible élément de $\mathcal{M}_m(\mathbb{F}_p)$, de termes diagonaux s_1, \dots, s_m . Montrer que :

$$pA_p(D, T) = p^m + \left(\frac{\det(D)}{p}\right) G^m \sum_{a \in \mathbb{F}_p^\times} \left(\frac{a}{p}\right)^m \omega^{-at}.$$

(c) Montrer que $G^2 = \left(\frac{-1}{p}\right) p$ (on pourra appliquer à un cas particulier le résultat démontré dans la question précédente).

3. Pour $a \in \mathbb{F}_p^\times$ et k entier naturel, on pose $\varepsilon_k^{(p)}(a) = \left(\frac{(-1)^{\frac{k}{2}} a}{p}\right)$ si k est pair et $\varepsilon_k^{(p)}(a) = 0$ sinon.

(a) Montrer que :

$$A_p(S, T) = \begin{cases} p^{m-1} \left(1 - \varepsilon_m^{(p)}(s) p^{-\frac{m}{2}}\right) & \text{si } m \text{ est pair} \\ p^{m-1} \left(1 + \varepsilon_{m-1}^{(p)}(st) p^{\frac{1-m}{2}}\right) & \text{si } m \text{ est impair} \end{cases}$$

(b) Préciser pour quelles valeurs de m , s et t la quantité $A_p(S, T)$ s'annule.

– IV – Le cas n quelconque

On suppose que $m \geq n$.

Soient $n \geq 2$ et $T \in S_n(\mathbb{F}_p)$ de déterminant $t \in \mathbb{F}_p^\times$. On suppose que $T = \begin{pmatrix} \delta & 0 \\ 0 & T_1 \end{pmatrix}$ avec $\delta \in \mathbb{F}_p^\times$ et $T_1 \in S_{n-1}(\mathbb{F}_p)$ inversible de déterminant t_1 .

1.

- (a) Montrer que l'application qui à $X \in \mathcal{A}_p(S, T)$ fait correspondre sa première colonne induit une application γ de $\mathcal{A}_p(S, T)$ dans $\mathcal{A}_p(S, \delta)$.
- (b) Soit $C_1 \in \mathcal{A}_p(S, \delta)$. Montrer qu'il existe une matrice symétrique inversible S_1 dans $\mathcal{M}_{m-1}(\mathbb{F}_p)$ dont le déterminant s_1 vérifie $\left(\frac{\delta s_1}{p}\right) = \left(\frac{s}{p}\right)$ et telle que $\gamma^{-1}(C_1)$ soit de cardinal $A_p(S_1, T_1)$ (on pourra utiliser l'interprétation de question 2 des Préliminaire (partie **II**) en introduisant l'orthogonal W du vecteur C_1 pour la forme b de matrice S dans la base canonique de $V = \mathcal{M}_{m,1}(\mathbb{F}_p)$).

2.

- (a) En procédant par récurrence sur n , montrer que :

$$A_p(S, T) = p^{mn - \frac{n(n+1)}{2}} \psi_{p,m,n}(s, t) \prod_{m-n < 2k < m} \left(1 - \frac{1}{p^{2k}}\right),$$

où :

$$\psi_{p,m,n}(s, t) = \left(1 - \varepsilon_m^{(p)}(s) p^{-\frac{m}{2}}\right) \left(1 + \varepsilon_{m-n}^{(p)}(st) p^{\frac{n-m}{2}}\right).$$

3. À quelles conditions $A_p(S, T)$ est-il nul ?

Agrégation externe 2005. Épreuve 1

Les corps considérés dans le problème sont supposés commutatifs. Pour tout entier $n \geq 1$, on note $\mathcal{M}_n(\mathbb{C})$ l'anneau des matrices carrées à n lignes et n colonnes à coefficients dans \mathbb{C} , $\mathcal{M}_n(\mathbb{Z})$ le sous-anneau de $\mathcal{M}_n(\mathbb{C})$ formé des matrices à coefficients dans \mathbb{Z} , et $\mathcal{C}_n(\mathbb{Z})$ l'ensemble des vecteurs colonnes à n lignes à coefficients dans \mathbb{Z} .

Pour tout ensemble Z , on note $S(Z)$ le groupe des bijections de Z sur lui-même. Si X et Y sont deux ensembles, on note Y^X l'ensemble des applications de X dans Y .

– I –

1. Soit A une matrice de $\mathcal{M}_n(\mathbb{C})$.
 - (a) Montrer que $A \in \mathcal{M}_n(\mathbb{Z})$ si, et seulement si, pour tout X dans $\mathcal{C}_n(\mathbb{Z})$, on a $AX \in \mathcal{C}_n(\mathbb{Z})$.
 - (b) Soit A une matrice de $\mathcal{M}_n(\mathbb{Z})$ dont le déterminant, noté $\det(A)$, est non nul et soit A^{-1} son inverse dans $\mathcal{M}_n(\mathbb{C})$. Montrer que $A^{-1} \in \mathcal{M}_n(\mathbb{Z})$ si, et seulement si, $|\det(A)| = 1$.
2. On munit \mathbb{R}^n d'un produit scalaire noté $\langle \cdot, \cdot \rangle$. Pour toute partie Y de \mathbb{R}^n , on note

$$Y^* = \{x \in \mathbb{R}^n \mid \forall y \in \mathbb{R}^n, \langle x, y \rangle \in \mathbb{Z}\}.$$

Si $B = (v_i)_{1 \leq i \leq n}$ est une base de \mathbb{R}^n , on note

$$L_B = \left\{ \sum_{i=1}^n m_i v_i \mid (m_1, \dots, m_n) \in \mathbb{Z}^n \right\}$$

le sous-groupe additif de $(\mathbb{R}^n, +)$ engendré par B ; de plus, on note G_B la matrice de $\langle \cdot, \cdot \rangle$ dans la base B , c'est-à-dire la matrice symétrique définie positive dont le (i, j) -ième coefficient vaut $\langle v_i, v_j \rangle$.

- (a) Soit $x \in \mathbb{R}^n$. Montrer que $x \in L_B^*$ si, et seulement si, il existe $X \in \mathcal{C}_n(\mathbb{Z})$ tel que $G_B^{-1}X$ est le vecteur colonne formé des composantes de x dans la base B .
 - (b) On suppose que $L_B \subset L_B^*$. Montrer que $G_B \in \mathcal{M}_n(\mathbb{Z})$, et que $\det(G_B) = 1$ si, et seulement si, $L_B^* = L_B$.
3. On note $(e_i)_{1 \leq i \leq n}$ la base canonique de \mathbb{R}^n et $(e_i^*)_{1 \leq i \leq n}$ sa base duale. Soit L un sous-groupe du groupe additif $(\mathbb{R}^n, +)$, tel que $2\mathbb{Z}^n \subset L \subset \mathbb{Z}^n$. Pour $1 \leq i \leq n$, on pose $L_i = L \cap F_i$, où F_i est le sous-espace vectoriel de \mathbb{R}^n engendré par $\{e_i, \dots, e_n\}$.

- (a) Montrer que, pour tout i , $1 \leq i \leq n$, il existe $a_i \in \{1, 2\}$, tel que $e_i^*(L_i) = a_i\mathbb{Z}$.
- (b) Pour $1 \leq i \leq n$, soit $u_i \in L_i$ tel que $e_i^*(u_i) = a_i$. Montrer que $(u_i)_{1 \leq i \leq n}$ engendre L et est une base de \mathbb{R}^n .
4. Soit C un $\frac{\mathbb{Z}}{2\mathbb{Z}}$ -sous-espace vectoriel de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$, et $L = \rho^{-1}(C)$ où ρ est l'application de \mathbb{Z}^n sur $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$ définie par $\rho(m_1, \dots, m_n) = (\widetilde{m}_1, \dots, \widetilde{m}_n)$, \widetilde{m} étant la classe de m modulo 2.
- Dans cette question, le produit scalaire $\langle \cdot, \cdot \rangle$ est défini par $\langle x, y \rangle = \frac{1}{2} \sum_{i=1}^n x_i y_i$, pour tout couple de vecteurs $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ de \mathbb{R}^n . De plus, on munit $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$ de la forme bilinéaire non dégénérée, définie, pour tout couple de vecteurs $x = (x_1, \dots, x_n)$ et $y = (y_1, \dots, y_n)$ de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^n$, par $x \cdot y = \sum_{i=1}^n x_i y_i$.
- (a) Montrer qu'il existe une base B de \mathbb{R}^n engendrant L , et que $L^* = \rho^{-1}(C^\perp)$ où C^\perp est l'orthogonal de C relativement à la forme bilinéaire définie ci-dessus.
- (b) On suppose que $C \subset C^\perp$. Montrer que G_B est à coefficients entiers, et que $\det(G_B) = 1$ si, et seulement si, $C = C^\perp$.

– II –

1. Soit \mathbb{K} un corps, A un \mathbb{K} -espace affine de dimension finie $r \geq 3$, et F le sous-espace vectoriel de \mathbb{K}^A formé des fonctions affines $f : A \rightarrow \mathbb{K}$.
- (a) Montrer que F est de dimension $r + 1$.
- (b) Soit $G_{aff}(A)$ le groupe affine de A , c'est-à-dire le groupe des applications affines bijectives de A dans lui-même. Montrer que :
- $$G_{aff}(A) = \{\sigma \in S(A) \mid \forall f \in F, f \circ \sigma \in F\}.$$
2. On suppose ici que \mathbb{K} est un corps fini et on note q son nombre d'éléments. Soit \cdot la forme bilinéaire non dégénérée sur \mathbb{K}^A définie, pour $f, g \in \mathbb{K}^A$ par $f \cdot g = \sum_{x \in A} f(x)g(x)$. On note F^\perp l'orthogonal de F relativement à cette forme bilinéaire.
- (a) Soit $f \in F$ non constante. Montrer que, pour tout $a \in \mathbb{K}$, l'ensemble $f^{-1}(\{a\})$ a q^{r-1} éléments.
- (b) Montrer que $F \subset F^\perp$, et que $F = F^\perp$ si, et seulement si, $q = 2$ et $r = 3$.
3. Dans cette question, on suppose que $\mathbb{K} = \frac{\mathbb{Z}}{2\mathbb{Z}}$ et que A est l'espace affine \mathbb{K}^3 , dont on numérote les points par $P_0 = (0, 0, 0)$, $P_1 = (1, 0, 0)$, $P_2 = (1, 1, 0)$, $P_3 = (0, 1, 1)$, $P_4 = (1, 0, 1)$, $P_5 = (0, 1, 0)$, $P_6 = (0, 0, 1)$ et $P_7 = (1, 1, 1)$. Soit $\varphi : \mathbb{K}^A \rightarrow \mathbb{K}^8$ l'application linéaire bijective définie par $f \mapsto (f(P_0), \dots, f(P_7))$. et H le sous-espace vectoriel de \mathbb{K}^8 égal à $\varphi(F)$.
- (a) Combien H possède-t-il d'éléments ayant exactement 4 composantes non nulles ?

(b) Montrer qu'une base de H est

$$\{(1, 1, 1, 1, 1, 1, 1, 1), (0, 1, 1, 0, 1, 0, 0, 1), (0, 0, 1, 1, 0, 1, 0, 1), (0, 0, 0, 1, 1, 0, 1, 1)\}$$

4. On utilise dans cette question les notations de la question **I.4**. On suppose que $n = 8$ et $C = H$.

(a) Montrer que : $\inf \{\langle x, x \rangle \mid x \in L - \{0\}\} = 2$.

(b) Combien L possède-t-il d'éléments x tels que $\langle x, x \rangle = 2$?

(c) Dédurre de ce qui précède :

- i. L'existence d'une matrice symétrique définie positive dans $\mathcal{M}_8(\mathbb{Z})$, de déterminant 1 et dont les termes diagonaux sont pairs.
- ii. L'existence d'une base B de l'espace euclidien usuel \mathbb{R}^8 , possédant la propriété suivante : soit S l'ensemble des boules fermées de rayon 1 (pour la norme euclidienne) centrées en les points de L_B . Les éléments de S sont deux à deux d'intérieurs disjoints, et chaque élément de S est tangent¹ à 240 autres.

Dans la suite du problème, k désigne un corps de caractéristique différente de 2, $Q = \{x \in k \mid \exists y \in k - \{0\}, x = y^2\}$ l'ensemble de ses carrés non nuls, et $X = \mathbb{P}^1(k) = k \cup \{\infty\}$ la droite projective sur k . On rappelle que l'application $\alpha : GL_2(k) \rightarrow S(X)$ qui à $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

associe l'homographie $\alpha(M) : x \mapsto \frac{ax + b}{cx + d}$ est un morphisme de groupes. On note $\ker(\alpha)$ son noyau, c'est-à-dire $\alpha^{-1}(\{Id_X\})$.

On rappelle également que, si $c = 0$, on a $\alpha(M)(\infty) = \infty$, et que, si $c \neq 0$, $\alpha(M)(\infty) = \frac{a}{c}$ et $\alpha(M)\left(-\frac{d}{c}\right) = \infty$.

On note $SL_2(k)$ le sous-groupe de $GL_2(k)$ formé des matrices de déterminant 1 et $N = PSL_2(k)$ l'image de $SL_2(k)$ par α .

– III –

1.

(a) Montrer que $SL_2(k) \cap \ker(\alpha) = \{-I_2, I_2\}$, où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(b) Soit $M \in GL_2(k)$; montrer que $\alpha(M) \in N$ si, et seulement si, $\det(M) \in Q$.

2. Si k est un corps fini à q éléments, calculer le nombre d'éléments de N en fonction de q .

3. Montrer que les homographies $x \mapsto h_i(x) = ix$ (pour $i \in Q$), $x \mapsto t_j(x) = x + j$ (pour $j \in k$) et $x \mapsto w(x) = -\frac{1}{x}$ appartiennent à N et l'engendrent.

4. Soit f un élément d'ordre 2 de N .

(a) Montrer que f est conjugué dans N à une homographie de la forme $x \mapsto w_i(x) = -\frac{i}{x}$ avec $i \in Q$.

¹deux boules fermées sont dites tangentes si la distance de leurs centres est égale à la somme de leurs rayons.

- (b) Montrer que si k a au moins cinq éléments, il existe un conjugué g de f dans N ne commutant pas avec f (on pourra calculer $t_a \circ w_i \circ t_a^{-1}$).
5. Soit A un $\frac{\mathbb{Z}}{2\mathbb{Z}}$ -espace affine de direction \vec{A} et $G_{aff}(A)$ son groupe affine.
- (a) Montrer que, si P est un sous-groupe de $G_{aff}(A)$ ne contenant pas de translation différente de l'application identique, alors P est isomorphe à un sous-groupe de $GL(\vec{A})$.
- (b) On suppose que k a au moins cinq éléments. Montrer que, si N est isomorphe à un sous-groupe de $G_{aff}(A)$, il est isomorphe à un sous-groupe de $GL(\vec{A})$.

– IV –

On note $\mathbf{1} : X \rightarrow \frac{\mathbb{Z}}{2\mathbb{Z}}$ la fonction constante égale à 1, $\mathbf{0} : X \rightarrow \frac{\mathbb{Z}}{2\mathbb{Z}}$ la fonction nulle, on note $-Q = \{-x \mid x \in Q\}$ et on suppose que k vérifie la propriété (*) suivante :

(*) $k - \{0\}$ est l'union disjointe de Q et $-Q$.

- Montrer que, si k a q éléments, l'hypothèse (*) est équivalente à $q \equiv -1 \pmod{4}$.
- On note $u : X \rightarrow \frac{\mathbb{Z}}{2\mathbb{Z}}$ l'application qui vaut 1 si $x \in Q \cup \{\infty\}$ et 0 sinon. Pour tout élément $r \in k$, on pose $u_r = u \circ t_r$.
 - Montrer que, pour tout $i \in Q$ et $r \in k$, on a $u_r \circ h_i = u_{r_i}$.
 - Montrer que $u + u \circ w = \mathbf{1}$, puis que $u + u_{w(r)} + u_r \circ w = \begin{cases} \mathbf{1} & \text{si } r \in Q \\ \mathbf{0} & \text{si } r \in -Q \end{cases}$
 - On suppose que k est un corps fini. Montrer que $\sum_{r \in k} u_r = \mathbf{1}$.
 - Soit R le sous-espace vectoriel de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^X$ engendré par les fonctions u_r , $r \in k$.
Montrer que

$$PSL_2(k) \subset \{\sigma \in S(X) \mid \forall f \in R, f \circ \sigma \in R\}.$$

- On suppose ici que $k = \frac{\mathbb{Z}}{7\mathbb{Z}}$. Soit $\psi : \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^X \rightarrow \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^8$ l'application linéaire bijective définie par

$$f \mapsto (f(\bar{0}), f(\bar{1}), f(\bar{2}), f(\bar{3}), f(\bar{4}), f(\bar{5}), f(\bar{6}), f(\infty))$$

où, pour tout entier $x \in \mathbb{Z}$, \bar{x} est la classe de x modulo 7.

- Montrer que $\psi(R) = H$, où H est le sous-espace vectoriel de $\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^8$ défini en **II.3**.
- En déduire que $PSL_2\left(\frac{\mathbb{Z}}{7\mathbb{Z}}\right)$ est isomorphe à $GL_3\left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)$.

Agrégation externe 2006. Épreuve 1

Préambule et notations préliminaires

Ce problème introduit les opérateurs de Dunkl de paramètre k dont on admet la commutativité.

On étudie d'abord le cas $k = 0$, puis le rang 1 et enfin certaines propriétés remarquables en dimension n . On utilise ces opérateurs pour démontrer une formule de MacDonald sur l'intégrale de Mehta, ce qui n'est pas fait ici.

Les deux premières parties sont indépendantes. La troisième partie n'utilise que le I.2.

- On désigne par \mathbb{N} l'ensemble des entiers naturels positifs ou nuls et par \mathbb{R} l'ensemble des nombres réels.
- **Dans ce problème n est un entier supérieur ou égal à 2.** On note e_1, \dots, e_n la base canonique de \mathbb{R}^n . On munit \mathbb{R}^n de sa structure euclidienne usuelle dont le produit scalaire est noté (\cdot, \cdot) .
- On note $\mathbb{R}[X_1, \dots, X_n]$ l'algèbre des polynômes en n indéterminées à coefficients dans \mathbb{R} . Tout polynôme P de $\mathbb{R}[X_1, \dots, X_n]$ s'écrit de manière unique :

$$P = \sum_{\alpha=(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n} a_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$$

où les a_α sont des réels nuls sauf pour un nombre fini d'entre eux.

Pour un polynôme P donné, **on note** $\text{supp}(P)$ **l'ensemble des α tels que $a_\alpha \neq 0$** avec la convention $\text{supp}(0) = \emptyset$. Ainsi on peut écrire $P = \sum_{\alpha \in \text{supp}(P)} a_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$.

Si P est un polynôme de $\mathbb{R}[X_1, \dots, X_n]$, P désigne aussi, par abus de notation, la fonction polynomiale associée et on note $P(x)$ l'évaluation de P en $x \in \mathbb{R}^n$.

- Le monôme $X_1^{\alpha_1} \dots X_n^{\alpha_n}$ est de degré $\sum_{i=1}^n \alpha_i$. Un polynôme P non nul est dit homogène de degré d si P est combinaison linéaire non nulle de monômes de degré d . On note alors $\text{deg}(P)$ ce degré.

On note Δ le polynôme $\prod_{1 \leq i < j \leq n} (X_j - X_i)$; il est homogène de degré $\frac{n(n-1)}{2}$.

- Si A et B sont deux opérateurs on note $A^2 = A \circ A$ et $[A, B]$ le commutateur $A \circ B - B \circ A$. On rappelle la formule $[A^2, B] = [A, B] \circ A + A \circ [A, B]$.
- On rappelle qu'il existe une action à gauche, linéaire et notée dans ce problème ρ , du groupe symétrique \mathfrak{S}_{nn} sur $\mathbb{R}[X_1, \dots, X_n]$. Pour $\sigma \in \mathfrak{S}_{nn}$ et $P = \sum_{\alpha \in \text{supp}(P)} a_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$,

¹Par convention, une somme indexée par l'ensemble vide est nulle.

cette action est définie par :

$$\rho(\sigma)(P) = \sum_{\alpha \in \text{supp}(P)} a_{\alpha} X_{\sigma(1)}^{\alpha_1} \cdots X_{\sigma(n)}^{\alpha_n}$$

On note aussi pour simplifier ${}^{\sigma}P = \rho(\sigma)(P)$.

On dit que P est symétrique si on a ${}^{\sigma}P = P$ pour tout $\sigma \in \mathfrak{S}_{nn}$.

– I – Le cas classique

1. Soit $P = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ avec $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. On note pour $1 \leq i < j \leq n$, $\theta_{i,j}$ la transposition (i, j) . Calculer :

$$\frac{P - \theta_{i,j} P}{X_i - X_j}$$

2. En déduire que, pour tout polynôme P de $\mathbb{R}[X_1, \dots, X_n]$ et pour toute transposition $\theta_{i,j}$ (avec $1 \leq i < j \leq n$), $P - \theta_{i,j} P$ est divisible par $X_i - X_j$.

On dira qu'un polynôme P est antisymétrique si, pour toute transposition $\theta \in \mathfrak{S}_n$, on a $\theta P = -P$.

3. Soit σ un élément de \mathfrak{S}_n . On note $\varepsilon(\sigma)$ sa signature. Montrer que tout polynôme P antisymétrique vérifie $\sigma P = \varepsilon(\sigma) P$.

4. Montrer que le polynôme $\Delta = \prod_{1 \leq i < j \leq n} (X_j - X_i)$ est antisymétrique.

5. Soit $P \in \mathbb{R}[X_1, \dots, X_n]$ un polynôme antisymétrique. Montrer qu'il est divisible par Δ dans l'anneau $\mathbb{R}[X_1, \dots, X_n]$.

Pour P polynôme de $\mathbb{R}[X_1, \dots, X_n]$, on note $P(\partial)$ l'opérateur différentiel obtenu en substituant aux symboles X_i les opérateurs différentiels $\frac{\partial}{\partial X_i}$. Cette substitution est possible car, pour $1 \leq i \leq n$ les opérateurs $\frac{\partial}{\partial X_i}$ commutent deux à deux. Si P s'écrit

$\sum_{\alpha \in \text{supp}(P)} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, on a donc :

$$P(\partial) = \sum_{\alpha \in \text{supp}(P)} a_\alpha \frac{\partial^{|\alpha|}}{\partial X_1^{\alpha_1} \cdots \partial X_n^{\alpha_n}},$$

avec $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Si P et Q sont deux polynômes, on note $P \cdot Q$ leur produit et on vérifie facilement (mais on ne demande pas de le faire) que l'on a l'égalité d'opérateurs :

$$(P \cdot Q)(\partial) = P(\partial) \circ Q(\partial).$$

On définit une forme bilinéaire sur $\mathbb{R}[X_1, \dots, X_n]$ notée $\langle \cdot, \cdot \rangle$ et donnée pour P et Q polynômes de $\mathbb{R}[X_1, \dots, X_n]$ par : $\langle P, Q \rangle = P(\partial)(Q)(0, \dots, 0)$ (on évalue en 0 le polynôme $P(\partial)(Q)$).

6. Soient P et Q deux polynômes homogènes non nuls avec $\deg(P) \neq \deg(Q)$. Montrer que l'on a $\langle P, Q \rangle = 0$.

7. Pour P, Q, R dans $\mathbb{R}[X_1, \dots, X_n]$, montrer que l'on a :

$$\langle PQ, R \rangle = \langle Q, P(\partial)(R) \rangle.$$

8. Montrer que la forme bilinéaire $\langle \cdot, \cdot \rangle$ détermine un produit scalaire défini positif sur $\mathbb{R}[X_1, \dots, X_n]$ (on pourra travailler dans une base adaptée).

9. Pour $\sigma \in \mathfrak{S}_n$ et P, Q polynômes de $\mathbb{R}[X_1, \dots, X_n]$, montrer que l'on a :

$$\langle \sigma P, \sigma Q \rangle = \langle P, Q \rangle.$$

10. Montrer que l'on a :

$$\langle \Delta, \Delta \rangle = \Delta(\partial)(\Delta) = 1!2! \cdots n!$$

(on pourra utiliser le développement du déterminant de Vandermonde :

$$\begin{vmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ 1 & X_2 & \cdots & X_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{vmatrix}$$

dont on admettra par ailleurs l'expression factorisée).

– II – Opérateur de Dunkl en rang 1

Dans cette partie, k désigne un **paramètre réel strictement positif**.

Pour $f \in \mathcal{C}^\infty(\mathbb{R})$, on définit la fonction $T(f)$ pour $x \neq 0$ par :

$$T(f)(x) = f'(x) + k \frac{f(x) - f(-x)}{x}$$

(on a noté f' la dérivée de la fonction f).

1. En utilisant la formule :

$$\frac{f(x) - f(-x)}{x} = \int_{-1}^1 f'(xt) dt$$

montrer que $T(f)$ se prolonge en une fonction de classe \mathcal{C}^∞ sur \mathbb{R} . On la note encore $T(f)$.

2. Pour m entier positif ou nul, calculer $T(p_m)$ où p_m est la fonction polynomiale définie pour $x \in \mathbb{R}$ par $p_m(x) = x^m$.

Pour $f \in \mathcal{C}^\infty(\mathbb{R})$, on définit la fonction $V_k(f)$ pour $x \in \mathbb{R}$ par :

$$V_k(f)(x) = b_k \int_{-1}^1 f(xt) (1-t)^{k-1} (1+t)^k dt$$

avec b_k un réel choisi de telle sorte que l'on ait $V_k(1) = 1$. La fonction $V_k(f)$ est clairement dans $\mathcal{C}^\infty(\mathbb{R})$ (on ne demande pas de la vérifier et on ne cherchera pas à expliciter b_k).

3. Pour $f \in \mathcal{C}^\infty(\mathbb{R})$, montrer que l'on a $T(V_k(f)) = V_k(f')$.

Pour $\lambda \in \mathbb{R}$ on note e_λ la fonction exponentielle $t \mapsto e^{\lambda t}$. On pose $E_\lambda = V_k(e_\lambda)$ et J_λ la fonction définie pour $x \in \mathbb{R}$ par :

$$J_\lambda(x) = \frac{E_\lambda(x) + E_\lambda(-x)}{2}.$$

4. Dédurre de ce qui précède que l'on a $T(E_\lambda) = \lambda E_\lambda$.

5. On suppose que $\lambda \neq 0$. Montrer que l'on a, pour tout $x \in \mathbb{R}$:

$$E_\lambda(x) = J_\lambda(x) + \frac{1}{\lambda} \frac{dJ_\lambda}{dx}(x).$$

6. Montrer que J_λ vérifie l'équation différentielle :

$$xy''(x) + 2ky'(x) = \lambda^2 xy(x).$$

– III – Opérateur de Dunkl en dimension n

Cette partie utilise les notations préliminaires et la question **I.2**.

Dorénavant k désigne un paramètre réel. On note R^+ le sous-ensemble fini de \mathbb{R}^n défini par :

$$R^+ = \{e_i - e_j \mid 1 \leq i < j \leq n\}.$$

Pour $\beta = e_i - e_j \in R^+$ (avec $i < j$), on note abusivement $X_\beta = X_i - X_j$ et on écrit θ_β ou $\theta_{i,j}$ la transposition (i, j) du groupe symétrique \mathfrak{S}_n . D'après la question **I.2**, on peut définir une application linéaire Δ_β de $\mathbb{R}[X_1, \dots, X_n]$ donnée pour $Q \in \mathbb{R}[X_1, \dots, X_n]$ par :

$$\Delta_\beta(Q) = \frac{Q - \theta_{i,j}Q}{X_i - X_j} = \frac{Q - \theta_\beta Q}{X_\beta}.$$

Pour tout entier ℓ tel que $1 \leq \ell \leq n$, on introduit l'opérateur de Dunkl d'indice ℓ , noté $T_\ell(k)$ (on notera aussi T_ℓ s'il n'y a pas de confusion possible), défini pour tout polynôme $Q \in \mathbb{R}[X_1, \dots, X_n]$ par :

$$\begin{aligned} T_\ell(k)(Q) &= \frac{\partial Q}{\partial X_\ell} + k \sum_{1 \leq i < j \leq n} (e_\ell, e_i - e_j) \frac{Q - \theta_{i,j}Q}{X_i - X_j} \\ &= \frac{\partial Q}{\partial X_\ell} + k \sum_{\beta \in R^+} (e_\ell, \beta) \Delta_\beta(Q) \end{aligned}$$

(on rappelle que (\cdot, \cdot) désigne le produit scalaire usuel sur \mathbb{R}^n).

1. Soit Q un polynôme homogène non nul. Montrer que pour tout entier ℓ tel que $1 \leq \ell \leq n$, le polynôme $T_\ell(k)(Q)$ est nul ou homogène de degré $\deg(Q) - 1$.
2. Montrer que l'on a, pour tout polynôme Q , tout $\sigma \in \mathfrak{S}_n$ et tout entier ℓ tel que $1 \leq \ell \leq n$:

$$\sigma(T_\ell(k)(Q)) = T_{\sigma(\ell)}(k)(\sigma Q).$$

Pour tout entier ℓ tel que $1 \leq \ell \leq n$, on note M_ℓ l'opérateur de multiplication par X_ℓ . Pour tout $Q \in \mathbb{R}[X_1, \dots, X_n]$, on a donc :

$$M_\ell(Q) = X_\ell \cdot Q.$$

On définit l'opérateur $D(k)$ par $D(k) = \sum_{\ell=1}^n T_\ell(k)^2$.

3. Pour P, Q polynômes de $\mathbb{R}[X_1, \dots, X_n]$ et $\beta \in R^+$ montrer que l'on a :

$$\Delta_\beta(P \cdot Q) = P \cdot \Delta_\beta(Q) + \Delta_\beta(P) \cdot (\theta_\beta Q)$$

(on rappelle que l'on a noté $P \cdot Q$ le produit de P et Q).

4. En utilisant la question précédente, montrer que, pour tout couple (i, j) d'entiers tels que $1 \leq i, j \leq n$, l'on a, entre opérateurs de $\mathbb{R}[X_1, \dots, X_n]$, l'égalité :

$$[T_j(k), M_i] = (e_i, e_j) Id + k \sum_{\beta \in R^+} (\beta, e_i) (\beta, e_j) \rho(\theta_\beta)$$

(on rappelle que le membre de gauche est le commutateur, $\rho(\theta_\beta)$ désigne l'action de la transposition θ_β dans $\mathbb{R}[X_1, \dots, X_n]$ et Id désigne l'application identique de $\mathbb{R}[X_1, \dots, X_n]$).

5. Pour tout entier ℓ tel que $1 \leq \ell \leq n$, déduire des questions précédentes que l'on a, entre opérateurs de $\mathbb{R}[X_1, \dots, X_n]$, l'égalité :

$$[D(k), M_\ell] = 2T_\ell(k)$$

(on pourra utiliser la formule du préambule sur le commutateur).

Agrégation externe 2007. Épreuve 1

Les quatre premières parties du problème sont largement indépendantes

Partie I

Dans cette partie **I**, on étudie une méthode de calcul de l'inverse d'un élément a d'un groupe multiplicatif G de cardinal fini $N \in \mathbb{N}^*$. L'élément neutre de G est noté 1 .

« Écrire un algorithme » signifie le rédiger en français, sous une forme rappelant un programme d'un langage tel que Pascal, Maple, Matlab, etc.

Le coût d'un algorithme est le nombre de multiplications dans le groupe G que nécessite son exécution. On ne tiendra pas compte des autres opérations (en particulier celles dans \mathbb{N}).

1. Justifier le fait que a^{N-1} est inverse de a dans G .
2. On écrit la décomposition en base 2 de $N - 1$ sous la forme :

$$N - 1 = \sum_{i=0}^k x_i 2^i \text{ avec } k \in \mathbb{N}, x_i \in \{0, 1\} \text{ pour } i \in \{0, \dots, k\} \text{ et } x_k \neq 0.$$

On considère les suites finies $(a_i)_{0 \leq i \leq k+1}$ et $(b_i)_{0 \leq i \leq k+1}$ définies par :

$$a_0 = 1, b_0 = a \text{ et pour } i \in \{0, \dots, k\}, a_{i+1} = a_i b_i^{x_i}, b_{i+1} = b_i^2.$$

- (a) Démontrer que a_{k+1} est l'inverse de a dans G .
 - (b) En déduire un algorithme de calcul de a^{-1} et préciser, en fonction de k , son coût dans le pire des cas (c'est-à-dire le nombre maximum de multiplications dans G que nécessite le calcul de a^{-1} ; on ne tiendra pas compte du coût éventuel du calcul des x_i , $0 \leq i \leq k$). L'algorithme doit prendre comme arguments a et N .
3. **Exemple.** Dans cette question, G est le groupe des éléments inversibles de $\mathbb{Z}/148\mathbb{Z}$. On note encore a la classe dans $\mathbb{Z}/148\mathbb{Z}$ d'un élément a de \mathbb{Z} .
 - (a) Déterminer le cardinal N de G .
 - (b) Démontrer que 5 est un élément de G et déterminer son inverse par la méthode de la question **I.2**.
 - (c) Donner une autre méthode pour déterminer cet inverse.

Partie II

1.

- (a) Soit π un élément d'un groupe multiplicatif G , e un entier relatif et $\alpha = \pi^e$.
On considère l'application f_α de $\mathbb{Z} \times G$ dans G^2 définie par $f_\alpha(k, \tau) = (\pi^k, \tau\alpha^k)$.
Exhiber une fonction φ_e de G^2 dans G , ne dépendant que de e et vérifiant :

$$\tau = \varphi_e \circ f_\alpha(k, \tau) \text{ pour tout } (k, \tau) \in \mathbb{Z} \times G.$$

- (b) On suppose le groupe G et l'élément π connus de tous les membres d'une association. L'un d'eux, **A**, garde secret l'entier e et rend public l'élément $\alpha = \pi^e$, ainsi donc que la fonction f_α . On recherche une procédure permettant à chacun d'envoyer à **A** un message crypté sous la forme d'un (ou de plusieurs) élément(s) τ de G , telle que la seule connaissance de e suffise à retrouver le message initial.
Justifier le fait que, si l'auteur décompose son message en parties telles que chacune puisse être représentée par un élément τ_i du groupe, choisit pour chacune d'elles un entier k_i et envoie les couples $f_\alpha(k_i, \tau_i) = (\lambda_i, \mu_i)$ à **A**, alors ce dernier peut les décrypter grâce à φ_e .

2. Dans cette question, G est le groupe \mathbb{F}_{29}^* des inversibles du corps à 29 éléments et les nombres $\pi = 2$ et $\alpha = 18$ sont supposés publics.

Chaque associé sait que les entiers $(1, 2, \dots, 26, 27, 28)$ modulo 29, dans cet ordre, représentent les éléments du 28-uplet $(A, B, \dots, Z, \cdot, \cdot)$, où \cdot figure l'espace séparant deux mots et \cdot est le point de fin de phrase.

3. Sachant que l'algorithme de décryptage employé par **A** repose sur les seules tables ci-dessous des résidus modulo 29 des puissances dix-septièmes des entiers entre 2 et 28 :

λ	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
λ^{17}	21	2	6	9	13	24	10	4	15	3	12	22	11	18	7	17

λ	18	19	20	21	22	23	24	25	26	27	28
λ^{17}	26	14	25	19	5	16	20	23	27	8	28

conjecturer la valeur de e et la contrôler grâce à α .

- (a) Décrypter le message suivant (on donne la suite des couples (λ_i, μ_i)) :

$$(16, 17), (18, 24), (28, 22), (17, 21), (23, 23), (24, 8).$$

Partie III

Dans cette partie **III**, le corps de base est le corps fini \mathbb{F}_{16} à 16 éléments, unique à isomorphisme près.

1.

- (a) Comment peut-on construire \mathbb{F}_{16} ?
 (b) Démontrer que le groupe multiplicatif \mathbb{F}_{16}^* est formé des puissances successives d'un élément ω vérifiant l'égalité $\omega^4 + \omega^3 + 1 = 0$.
 (c) Démontrer que $\omega, \omega^2, \omega^4$ et ω^8 sont les racines du polynôme $X^4 + X^3 + 1$ dans \mathbb{F}_{16} .
 (d) Démontrer que la famille $(\omega, \omega^2, \omega^4, \omega^8)$ est une base de \mathbb{F}_{16} sur \mathbb{F}_2 .

2. (a) Soit $a \in \mathbb{F}_{16}$. Résoudre dans \mathbb{F}_{16} l'équation $x^5 = a$, en discutant éventuellement selon la valeur de a .
- (b) Démontrer qu'il existe quatre éléments $\gamma \in \mathbb{F}_{16}$ tels que, pour chacun d'eux, la famille $(\gamma, \gamma^2, \gamma^4, \gamma^8)$ est une base de \mathbb{F}_{16} sur \mathbb{F}_2 telle que le produit de deux de ses éléments appartient à la base ou est égal à 1.
Expliquer rapidement pourquoi les calculs dans \mathbb{F}_{16} sont plus faciles dans une telle base.

Partie IV

Une *cubique* sur un corps \mathbb{K} est l'ensemble Γ des points $M = (x, y) \in \mathbb{K}^2$ annulant un polynôme du troisième degré :

$$P(X, Y) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2 + fXY + gY^2 + hX + iY + j$$

à coefficients dans \mathbb{K} .

Dans toute la suite, P est supposé non nul.

Remarque : il existe plusieurs polynômes donnant le même sous-ensemble de \mathbb{K}^2 , comme le montre l'exemple des polynômes XY^2 et X^2Y . Il est systématiquement sous-entendu que l'on a fait un choix particulier de P (ou de l'un de ses produits par les éléments de \mathbb{K}^*).

Cette partie étudie quelques cubiques particulières sur le corps \mathbb{R} .

1. Dans cette question, on prend la cubique Γ définie par le polynôme $P = X^3 - Y \in \mathbb{R}[X, Y]$.
 - (a) La tracer à main levée.
 - (b) Démontrer que toute droite coupe Γ en exactement un ou trois points en comptant leur multiplicité éventuelle et que, lorsqu'il existe trois points d'intersection notés $A = (x_A, y_A)$, $B = (x_B, y_B)$, $C = (x_C, y_C)$:

$$x_A + x_B + x_C = 0.$$

On note Ω le point de coordonnées $(0, 0)$ de Γ . Pour tout couple (A, B) de points de Γ , on considère le troisième point C d'intersection avec Γ de la droite AB (ou de la tangente en A à Γ si $B = A$), puis le troisième point d'intersection $A * B$ de la droite ΩC avec Γ . Ceci définit sur Γ une loi multiplicative $*$ (on peut compléter le dessin du **IV.1.a**).

- (c) Démontrer que $(\Gamma, *)$ est un groupe isomorphe à $(\mathbb{R}, +)$.
2. Reprendre la question **1.** pour $P = X^3 - 3XY - 1 \in \mathbb{R}[X, Y]$ et $\Omega = (1, 0)$, en précisant à quel groupe usuel est isomorphe $(\Gamma, *)$ dans cet exemple.
3. On étudie dans la suite des cubiques du plan projectif.
On considère un polynôme non nul homogène à trois variables :

$$\bar{P}(X, Y, Z) = aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3.$$

La cubique associée est l'ensemble Γ des points du plan projectif dont les coordonnées homogènes (X, Y, Z) vérifient $\bar{P}(X, Y, Z) = 0$.

Démontrer que l'intersection de Γ avec toute droite du plan projectif est constituée d'exactly un ou trois points, en comptant toujours les multiplicités éventuelles.

4. Dans cette question **4.** on considère $P = Y^3 - X^2 - Y^2$ et le polynôme homogène associé $\overline{P}(X, Y, Z) = Y^3 - X^2Z - Y^2Z$.

(a) Dans cette question **4.a.** on se place dans le plan affine euclidien \mathbb{R}^2 et on considère la courbe γ d'équation $y^3 = x^2 + y^2$ privée du point $(0, 0)$.

En choisissant un paramétrage de γ (par exemple en coordonnées polaires), étudier cette courbe et la tracer, en précisant l'allure des branches infinies s'il en existe.

On ne demande pas d'étudier les éventuels points d'inflexion.

Dans la suite de la question **4.** on considère dans le plan projectif la cubique Γ d'équation $Y^3 - X^2Z - Y^2Z = 0$, privée du point de coordonnées $(0, 0, 1)$

On choisit pour Ω le point à l'infini $(1, 0, 0)$ et on définit le composé $A * B$ de deux points quelconques de Γ comme en **IV.1.**

(b) Montrer que Γ admet comme paramétrage :

$$\begin{cases} X = \cos \theta \\ Y = \sin \theta \\ Z = \sin^3 \theta \end{cases} \quad (\theta \text{ décrivant } \mathbb{R})$$

Si A et B sont deux points de Γ , caractériser le point C tel que $C = A * B$.

(c) Démontrer que $(\Gamma, *)$ est isomorphe à un groupe usuel que l'on précisera. Quels sont les points d'ordre 6 ?

Partie V

Dans cette partie V, on étudie la courbe Γ' définie dans le plan \mathbb{F}_{16}^2 par l'équation :

$$y^2 + y = x^3 + x.$$

1. Montrer que la courbe Γ' contient au plus 32 points de \mathbb{F}_{16}^2 .
2. On introduit le polynôme homogène :

$$\overline{P}(X, Y, Z) = X^3 + XZ^2 - Y^2Z - YZ^2$$

Définir, par analogie avec la partie **IV**, un point à l'infini Ω et une multiplication interne à l'ensemble Γ réunion de Γ' et de Ω .

(a) Montrer que cette multiplication, notée $*$, est commutative et admet un élément neutre, vis-à-vis duquel tout point admet un inverse.

(b) Calculer l'inverse d'un élément $A = (\alpha, \beta)$ de Γ' .

On admettra que cette loi est associative et munit donc Γ d'une structure de groupe commutatif.

3. On se propose de calculer le carré $A^2 = A * A$ d'un élément $A = (\alpha, \beta)$ de Γ' .

On est amené à considérer la droite D passant par A telle que son intersection avec Γ' admet A comme point double.

(a) Montrer que cette droite – appelée tangente en A à la courbe Γ' – a pour équation :

$$P'_X(\alpha, \beta)(x - \alpha) + P'_Y(\alpha, \beta)(y - \beta) = 0$$

où P'_X et P'_Y désignent les polynômes dérivés du polynôme P , respectivement par rapport à X et Y .

- (b) Déterminer les coordonnées de $A * A$.
 - (c) En déduire que, pour tout point A de $\Gamma' : A^4 = A^{-1}$.
 - (d) En déduire le cardinal de Γ et sa décomposition en produit direct de groupes cycliques.
4. Indiquer brièvement comment implanter un système de cryptographie du type de celui de la partie **II** à l'aide de Γ .

Agrégation externe 2009. Épreuve 1

Notations et préliminaires

Tous les corps figurant dans le problème sont supposés commutatifs.

- \mathbb{N} désigne l'ensemble des nombres entiers naturels.
- \mathbb{N}^* désigne l'ensemble des nombres entiers naturels non nuls.
- Pour tous entiers naturels a et b tels que $a \leq b$, l'ensemble $\llbracket a, b \rrbracket$ désigne $[a, b] \cap \mathbb{N}$.
- \mathbb{R} désigne l'ensemble des nombres réels.
- \mathbb{R}^* désigne l'ensemble des nombres réels non nuls.
- \mathbb{R}^+ désigne l'ensemble des nombres réels positifs.
- \mathbb{C} désigne l'ensemble des nombres complexes.
- \mathbb{C}^* désigne l'ensemble des nombres complexes non nuls.
- \mathbb{K} étant un corps, on note $\mathbb{K}[X]$ l'ensemble des polynômes à coefficients dans \mathbb{K} , $\mathbb{K}_n[X]$ l'ensemble des polynômes de degré $\leq n$ à coefficients dans \mathbb{K} , pour tout entier naturel n .
- $\mathcal{M}_n(\mathbb{K})$ désigne l'ensemble des matrices carrées de taille $n \geq 1$ à coefficients dans \mathbb{K} .
- $GL_n(\mathbb{K})$ désigne l'ensemble des matrices inversibles de $\mathcal{M}_n(\mathbb{K})$. Si $A \in GL_n(\mathbb{K})$, on note A^{-1} son inverse.
- On dira que deux sous-espaces vectoriels V et W de $\mathcal{M}_n(\mathbb{K})$ sont **conjugués** s'il existe $P \in GL_n(\mathbb{K})$ telle que :

$$W = P^{-1}VP = \{P^{-1}MP \mid M \in V\}.$$

- I_n désigne l'élément unité de $\mathcal{M}_n(\mathbb{K})$.
- Pour A dans $\mathcal{M}_n(\mathbb{K})$ on désigne par tA la transposée de A , $\text{Tr}(A)$ la trace de A , $\det(A)$ le déterminant de A et P_A son polynôme caractéristique sur \mathbb{K} c'est-à-dire :

$$P_A(X) = \det(A - XI_n).$$

- Pour E un \mathbb{K} -espace vectoriel, on note $\mathcal{L}(E)$ l'algèbre des endomorphismes de E et Id_E l'application identité de E .
- Si u est un endomorphisme diagonalisable d'un \mathbb{K} -espace vectoriel E de dimension finie, on pose $\text{Sp}(u)$ le spectre de u , c'est-à-dire l'ensemble des valeurs propres de u .
- Pour u un endomorphisme d'un \mathbb{K} -espace vectoriel E de dimension finie et pour $\lambda \in \text{Sp}(u)$, on pose $E_\lambda(u) = \ker(u - \lambda Id_E)$ le sous-espace propre de u associé à λ .

Objet du problème

Dans ce problème, on se propose d'étudier les sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{K})$ constitués de matrices diagonalisables.

Plus précisément, si n est un entier $n \geq 1$ et \mathbb{K} un corps, on note $\mathcal{MT}(n, \mathbb{K})$ l'affirmation suivante :

– Pour toutes matrices A et B diagonalisables dans $\mathcal{M}_n(\mathbb{K})$, la propriété :

(a) A et B commutent

est équivalente à la propriété

(b) pour tout $\lambda \in \mathbb{K}$, $A + \lambda B$ est diagonalisable dans $\mathcal{M}_n(\mathbb{K})$.

L'un des objectifs de ce problème est de montrer que cette affirmation est vraie dans le cas complexe c'est-à-dire que $\mathcal{MT}(n, \mathbb{C})$ est vraie pour tout $n \geq 1$, qui est un résultat dû à Motzkin-Taussky, 1952.

Dans toute la suite, lorsqu'il sera demandé d'étudier l'affirmation $\mathcal{MT}(n, \mathbb{K})$, il faudra examiner successivement si les implications (a) \Rightarrow (b) et (b) \Rightarrow (a) sont vraies.

Les parties **I**, **II** et **III** peuvent être traitées de manière indépendante.

Partie I

– I.A – Le sens direct et le cas $n = 2$

1. Soit \mathbb{K} un corps et E un \mathbb{K} -espace vectoriel de dimension finie.

On considère u et v deux endomorphismes diagonalisables de E qui commutent, c'est-à-dire tels que $u \circ v = v \circ u$.

(a) Montrer que les sous-espaces propres de v sont stables par u , c'est-à-dire que si F est un sous-espace propre de v , on a $u(F) \subset F$.

(b) Montrer que u induit sur chaque sous-espace propre de v un endomorphisme diagonalisable.

(c) En déduire l'existence d'une base commune de réduction dans E pour les endomorphismes u et v , c'est-à-dire qu'il existe une base \mathcal{B} de E telle que celle-ci soit une base de vecteurs propres à la fois de u et de v .

2. Plus généralement, on considère $(u_i)_{i \in I}$ une famille d'endomorphismes diagonalisables de E . On suppose en outre que ces endomorphismes commutent deux à deux :

$$(\forall (i, j) \in I^2), u_i \circ u_j = u_j \circ u_i$$

Montrer l'existence d'une base commune de réduction dans E pour la famille $(u_i)_{i \in I}$, c'est-à-dire qu'il existe une base \mathcal{B} de E qui est une base de vecteurs propres pour chaque endomorphisme u_i , $i \in I$.

(Indication : on pourra raisonner par récurrence sur la dimension de E , en étudiant à part le cas où $(u_i)_{i \in I}$ est une famille d'homothéties).

3. Montrer que l'implication (a) \Rightarrow (b) est vraie dans l'affirmation $\mathcal{MT}(n, \mathbb{K})$, pour tout entier $n \geq 1$ et tout corps \mathbb{K} .

4. Étudier l'implication (b) \Rightarrow (a) dans l'affirmation $\mathcal{MT}(2, \mathbb{R})$.

5. On étudie l'implication (b) \Rightarrow (a) dans l'affirmation $\mathcal{MT}(2, \mathbb{C})$.

Soit A et B deux matrices diagonalisables de $\mathcal{M}_2(\mathbb{C})$ satisfaisant à la propriété (b) de $\mathcal{MT}(2, \mathbb{C})$.

(a) Montrer que l'on peut se ramener au cas où B est une matrice diagonale de $\mathcal{M}_2(\mathbb{C})$ avec au moins une valeur propre nulle.

(b) En supposant que B est une matrice diagonale non nulle avec une valeur propre nulle, démontrer l'existence d'un nombre complexe λ_0 tel que $A + \lambda_0 B$ ait une valeur propre double.

- (c) En déduire que l'implication $(b) \Rightarrow (a)$ dans $\mathcal{MT}(2, \mathbb{C})$ est vraie.
6. On suppose ici que $\mathbb{K} = \mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$, où p est un nombre premier et n un nombre entier ≥ 1 .
- (a) Montrer que $A \in \mathcal{M}_n(\mathbb{F}_p)$ est diagonalisable si, et seulement si, $A^p = A$.
- (b) Démontrer l'affirmation $\mathcal{MT}(n, \mathbb{F}_2)$.
- (c) Démontrer l'affirmation $\mathcal{MT}(n, \mathbb{F}_p)$, dans le cas $p \geq 3$.
(*Indication* : on pourra suivre le même plan que dans le cas complexe rencontré à la question **I.A.5.**)

– I.B – Application de la réduction simultanée

- 1.
- (a) On suppose ici que \mathbb{K} est un corps de caractéristique différente de 2.
On considère un sous-groupe multiplicatif fini G de $GL_n(\mathbb{K})$ où n est un entier ≥ 1 .
On suppose que :
- $$(\forall M \in G), M^2 = I_n$$
- (b) En déduire que pour $(n, m) \in (\mathbb{N}^*)^2$ les groupes multiplicatifs $GL_n(\mathbb{K})$ et $GL_m(\mathbb{K})$ sont isomorphes si, et seulement si, $n = m$. Montrer que G est abélien de cardinal inférieur ou égal à 2^n .
2. Dans cette question $\mathbb{K} = \mathbb{C}$ et n est un nombre entier ≥ 1 .
On considère A et B deux matrices de $\mathcal{M}_n(\mathbb{C})$ et on introduit l'endomorphisme de $\mathcal{M}_n(\mathbb{C})$:

$$\Phi_{A,B} : M \mapsto AM + MB.$$

- (a) On supposant que A est diagonalisable et que $B = 0$, établir que $\Phi_{A,B}$ est diagonalisable.
- (b) On supposant A et B diagonalisables, établir que $\Phi_{A,B}$ est diagonalisable.
- (c) Démontrer la réciproque, c'est-à-dire que si $\Phi_{A,B}$ est diagonalisable, A et B le sont.
(*Indication* : On pourra utiliser la décomposition de Jordan-Dunford de A et B).
- (d) Lorsque A et B sont diagonalisables, déterminer les éléments propres de $\Phi_{A,B}$ en fonction de ceux de A et de tB .
3. Dans cette question $\mathbb{K} = \mathbb{R}$ et on note $\mathcal{S}_2(\mathbb{R})$ l'ensemble des matrices symétriques réelles de $\mathcal{M}_2(\mathbb{R})$. Soit V un hyperplan vectoriel de $\mathcal{M}_2(\mathbb{R})$ constitué de matrices diagonalisables sur \mathbb{R} . On se propose de montrer que V est conjugué à $\mathcal{S}_2(\mathbb{R})$.
- (a) Montrer que V contient la matrice I_n .
- (b) Montrer que V est conjugué au sous-espace vectoriel engendré par (I_2, A, B) avec :
- $$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } B = \begin{pmatrix} 0 & \omega^2 \\ 1 & 0 \end{pmatrix}$$
- où ω est un nombre réel non nul.
- (c) En déduire le résultat.
4. Montrer que tout espace vectoriel formé de matrices diagonalisables de $\mathcal{M}_2(\mathbb{R})$ est conjugué à un sous-espace vectoriel de $\mathcal{S}_2(\mathbb{R})$.

Partie II : Le cas $n = 3$

On suppose que \mathbb{K} est un corps de caractéristique nulle. On rappelle les définitions suivantes :
Pour les polynômes de $\mathbb{K}[X]$:

$$P(X) = \sum_{k=0}^m a_k X^k \text{ et } Q(X) = \sum_{k=0}^n b_k X^k$$

où m et n sont deux entiers ≥ 1 , on définit le **résultant** de P et Q par le déterminant de taille $m+n$:

$$\text{Res}(P, Q) = \begin{vmatrix} a_m & 0 & \cdots & 0 & b_n & 0 & \cdots & 0 \\ a_{m-1} & \ddots & \ddots & \vdots & b_{n-1} & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots & \ddots & \ddots & 0 \\ \vdots & & \ddots & a_m & \vdots & & \ddots & b_n \\ \vdots & & & a_{m-1} & \vdots & & & b_{n-1} \\ \vdots & & & \vdots & \vdots & & & \vdots \\ a_0 & & & \vdots & b_0 & & & \vdots \\ 0 & a_0 & & \vdots & 0 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_0 & 0 & \cdots & 0 & b_0 \end{vmatrix}$$

$\underbrace{\hspace{15em}}_{n \text{ colonnes}}$
 $\underbrace{\hspace{15em}}_{m \text{ colonnes}}$

Pour tout $P \in \mathbb{K}[X]$ de degré $n \geq 1$ de coefficient dominant a_n , on définit le **discriminant** de P par :

$$\Delta(P) = \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} R(P, P')$$

1. On considère α, β et γ trois scalaires de \mathbb{K} . Montrer que le discriminant du polynôme :

$$P = -X^3 + \alpha X^2 + \beta X + \gamma$$

est :

$$-27\gamma^2 - 18\gamma\alpha\beta + \alpha^2\beta^2 - 4\alpha^3\gamma + 4\beta^3.$$

2. On pose dans $\mathcal{M}_3(\mathbb{K})$:

$$M = \begin{pmatrix} m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 \\ m_7 & m_8 & m_9 \end{pmatrix} \text{ et } N = \begin{pmatrix} s & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

On suppose s distinct de 0 et 1. Montrer que le discriminant du polynôme caractéristique de $M + \lambda N$ est un polynôme de degré 6 en λ dont le coefficient dominant est $(s(1-s))^2$.

3. On pose dans $\mathcal{M}_3(\mathbb{K})$:

$$B = \begin{pmatrix} b_1 & b_2 & b_3 \\ b_4 & b_5 & b_6 \\ b_7 & b_8 & b_9 \end{pmatrix} \text{ et } Q = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et on note :

$$P_B = -X^3 + aX^2 + bX + c.$$

(a) Montrer que si $\begin{vmatrix} b_1 & b_2 \\ b_4 & b_5 \end{vmatrix} = 0$, on a :

$$(\forall \lambda \in \mathbb{K}), P_{B+\lambda Q} = -X^3 + (a + \lambda)X^2 + (b - (b_1 + b_5)\lambda)X + c.$$

(b) Montrer alors que si en plus $b_1 + b_5 \neq 0$, le discriminant de $P_{B+\lambda Q}$ est un polynôme de degré quatre en λ et déterminer son coefficient dominant.

4. Ici $\mathbb{K} = \mathbb{C}$; on se propose de démontrer l'implication $(b) \Rightarrow (a)$ de l'affirmation $\mathcal{MT}(3, \mathbb{C})$. Soit A et B deux matrices diagonalisables de $\mathcal{M}_3(\mathbb{C})$ satisfaisant à la propriété (b) de $\mathcal{MT}(3, \mathbb{C})$; on note \mathcal{F} le \mathbb{C} -espace vectoriel engendré dans $\mathcal{M}_3(\mathbb{C})$ par I_3, A et B .

(a) Montrer que \mathcal{F} est un sous-espace vectoriel de matrices diagonalisables de $\mathcal{M}_3(\mathbb{C})$ et que si la dimension de \mathcal{F} est strictement inférieure à 3, les matrices A et B commutent.

(b) On suppose que la dimension de \mathcal{F} est égale à 3. Montrer que l'on peut se ramener par conjugaison au cas où $A = \text{Diag}(0, 0, 1)$ et B est un projecteur de rang 1.

(c) En déduire que l'implication $(b) \Rightarrow (a)$ de l'affirmation $\mathcal{MT}(3, \mathbb{C})$ est vraie.

Partie III : Le cas général dans \mathbb{C}

III-A : Bases holomorphes

1. Soit Ω_0 un disque ouvert de \mathbb{C} contenant l'origine; on considère une application holomorphe M de Ω_0 dans $\mathcal{M}_n(\mathbb{C})$, c'est-à-dire telle que chaque coefficient m_{ij} de M définisse une fonction holomorphe de Ω_0 dans \mathbb{C} , pour $(i, j) \in \llbracket 1, n \rrbracket^2$.

Pour tout $z \in \Omega_0 \setminus \{0\}$, on note $V(z)$ le noyau de la matrice $M(z)$.

Démontrer l'existence d'un réel $\rho > 0$ et d'un entier $m \geq 0$ tels que :

$$(\forall z \in \Omega_0), (0 < |z| < \rho) \Rightarrow (\dim V(z) = m)$$

(Indication : on pourra considérer les mineurs de $M(z)$.)

On suppose $m \geq 1$ dans la suite.

2. Sous les hypothèses ci-dessus et avec les mêmes notations, démontrer l'existence d'un nombre réel $r > 0$ et de m fonctions ψ_1, \dots, ψ_m holomorphes sur $D_r = \{z \in \Omega_0 \mid |z| < r\}$, à valeurs dans \mathbb{C}^n , telles que pour tout $z \in D_r \setminus \{0\}$, les vecteurs $\psi_1(z), \dots, \psi_m(z)$ engendrent $V(z)$ et $\psi_1(0), \dots, \psi_m(0)$ sont tous non nuls.

(Indication : on pourra commencer par trouver des vecteurs $\tilde{\psi}_1(z), \dots, \tilde{\psi}_m(z)$ méromorphes en z qui engendrent $V(z)$.)

3. Toujours avec les mêmes notations, notons Z^* l'ensemble des couples $(z, \psi) \in \Omega_0 \times \mathbb{C}^n$ tels que $z \neq 0$ et $\psi \in V(z)$, Z l'adhérence de Z^* dans $\Omega_0 \times \mathbb{C}^n$ et $V(0)$ (qui n'a pas encore été défini) le sous-ensemble de \mathbb{C}^n tel que :

$$\{0\} \times V(0) = Z \cap (\{0\} \times \mathbb{C}^n)$$

(a) On suppose que la famille $(\psi_1(0), \dots, \psi_m(0))$ est libre. Démontrer que $V(0)$ est un sous-espace vectoriel de \mathbb{C}^n de dimension m .

(b) Montrer qu'il existe une famille (ψ_1, \dots, ψ_m) , comme à la question **III.A.2.** telle que la famille $(\psi_1(0), \dots, \psi_m(0))$ soit libre et en déduire que $V(0)$ est un sous-espace vectoriel de \mathbb{C}^n de dimension m .

(Indication : partant d'une famille quelconque (Φ_1, \dots, Φ_m) vérifiant **III.A.2.** on pourra construire des familles $(\psi_1, \dots, \psi_k, \Phi_{k+1}, \dots, \Phi_m)$ par récurrence sur k .)

4. On considère une application holomorphe \mathcal{N} d'un ouvert \mathcal{U} de \mathbb{C} dans $\mathcal{M}_n(\mathbb{C})$, un point μ_0 de \mathbb{C} et un cercle Γ centré en μ_0 , orienté dans le sens direct.

On suppose que pour tout $\lambda \in \mathcal{U}$, la matrice $\mathcal{N}(\lambda)$ est diagonalisable, que :

$$(\forall \lambda \in \mathcal{U}), (\forall \mu \in \Gamma), \mathcal{N}(\lambda) - \mu I_n \in GL_n(\mathbb{C})$$

et on note $R(\lambda, \mu) = (\mathcal{N}(\lambda) - \mu I_n)^{-1}$.

- (a) Démontrer que la formule suivante :

$$\Pi(\lambda) = -\frac{1}{2i\pi} \int_{\Gamma} R(\lambda, \mu) d\mu$$

définit une application holomorphe Π de \mathcal{U} dans $\mathcal{M}_n(\mathbb{C})$.

- (b) Soit λ_0 un point de \mathcal{U} ; on suppose que μ_0 est l'unique valeur propre de $\mathcal{N}(\lambda_0)$ entourée par le cercle Γ . Démontrer que $\Pi(\lambda_0)$ est la projection de sur $E_{\mu_0}(\mathcal{N}(\lambda_0))$, le sous-espace propre de $\mathcal{N}(\lambda_0)$ associé à μ_0 , parallèlement à la somme des autres sous-espaces propres de $\mathcal{N}(\lambda_0)$.
5. Démontrer que pour tout $\lambda \in \mathcal{U}$, la matrice $\Pi(\lambda)$ est un projecteur, somme de projecteurs sur des sous-espaces propres de $\mathcal{N}(\lambda)$ associés à des valeurs propres entourées par Γ .

III-B : Courbes spectrales

Dans cette partie le corps de base est $\mathbb{K} = \mathbb{C}$ et \mathbf{D} désigne le disque ouvert $\mathbf{D} = \{z \in \mathbb{C} \mid |z| < 1\}$. Soient A et B deux matrices dans $\mathcal{M}_n(\mathbb{C})$, pour $n \in \mathbb{N}^*$, on pose :

$$(\forall (\lambda, \mu) \in \mathbb{C}^2), P(\lambda, \mu) = P_{A+\lambda B}(\mu) = \det(A + \lambda B - \mu I_n)$$

Pour $\lambda \in \mathbb{C}$, le polynôme caractéristique de $A + \lambda B$ sera noté P_λ .

On définit l'ensemble :

$$\mathcal{C} = \{(\lambda, \mu) \in \mathbb{C}^2 \mid P(\lambda, \mu) = 0\}$$

On appelle **multiplicité** (dans \mathcal{C}) d'un point $x = (\lambda, \mu)$ de \mathcal{C} , la multiplicité de la racine μ du polynôme P_λ , notée $d(x)$.

Nous **admettrons** le théorème suivant qui permet de paramétrer localement l'ensemble \mathcal{C} par des injections holomorphes de \mathbf{D} dans \mathbb{C}^2 :

Quelque soit $x_0 = (\lambda_0, \mu_0) \in \mathcal{C}$, il existe $\ell \in \mathbb{N}^*$ et deux familles finies d'applications holomorphes de \mathbf{D} dans \mathbb{C} , $(f_\alpha)_{1 \leq \alpha \leq \ell}$ et $(g_\alpha)_{1 \leq \alpha \leq \ell}$ qui vérifient les conditions suivantes :

- (i) $(\forall \alpha \in \llbracket 1, \ell \rrbracket), f_\alpha(0) = \lambda_0$ et $g_\alpha(0) = \mu_0$
- (ii) $(\forall z \in \mathbf{D}), (\forall \alpha \in \llbracket 1, \ell \rrbracket), (f_\alpha(z), g_\alpha(z)) \in \mathcal{C}$
- (iii) $(\exists \eta > 0), \forall (\lambda, \mu) \in \mathbb{C}^2,$

$$(|\lambda - \lambda_0| \leq \eta, |\mu - \mu_0| \leq \eta) \Rightarrow ((\exists \alpha \in \llbracket 1, \ell \rrbracket), (\exists z \in \mathbf{D}), \lambda = f_\alpha(z) \text{ et } \mu = g_\alpha(z))$$

- (iv) $(\forall \alpha \in \llbracket 1, \ell \rrbracket), (\forall (z, w) \in \mathbf{D}^2), (f_\alpha(z) = f_\alpha(w), g_\alpha(z) = g_\alpha(w)) \Rightarrow (z = w)$
- (v) $(\forall (\alpha, \beta) \in \llbracket 1, \ell \rrbracket^2, \alpha \neq \beta), (\forall (z, w) \in (\mathbf{D} \setminus \{0\})^2), ((f_\alpha(z), g_\alpha(z)) \neq (f_\beta(w), g_\beta(w)))$
- (vi) $(\forall z \in \mathbf{D} \setminus \{0\}), (\forall \alpha \in \llbracket 1, \ell \rrbracket), f'_\alpha(z) \neq 0$

Nous noterons $F_\alpha = (f_\alpha, g_\alpha)$ les applications associées de \mathbf{D} dans \mathbb{C}^2 , pour tout $\alpha \in \llbracket 1, \ell \rrbracket$.

Remarque : la condition (ii) signifie que $F_\alpha(\mathbf{D}) \subset \mathcal{C}$, (iii) que l'ensemble $\bigcup_{1 \leq \alpha \leq \ell} F_\alpha(\mathbf{D})$

contient un voisinage de z_0 dans \mathcal{C} , (iv) que chaque F_α est injective et (v) que $(F_\alpha(\mathbf{D}) \setminus \{0\})_{1 \leq \alpha \leq \ell}$ est une famille d'ensembles deux à deux disjoints. La condition (vi) est particulière à notre situation où chaque polynôme P_λ est de degré n en μ , pour tout $\lambda \in \mathbb{C}$.

Pour $\alpha \in \llbracket 1, \ell \rrbracket$, l'ensemble $F_\alpha(\mathbf{D})$ s'appelle une **branche locale** de \mathcal{C} en x_0 .

Nous **admettrons** que la multiplicité dans \mathcal{C} est constante dans une branche épointée, c'est-à-dire que $d(x)$ ne dépend que de x si $x \neq x_0$ et $x \in F_\alpha(\mathbf{D})$; on la notera d_α , pour tout $\alpha \in \llbracket 1, \ell \rrbracket$.

On appelle **ramification** e_α d'une branche $F_\alpha(\mathbf{D})$ en x_0 l'ordre du zéro 0 de $f_\alpha - \lambda_0$, qui existe puisque f_α est non constante; nous **admettrons** alors que pour tout $\lambda \in \mathbb{C} \setminus \{0\}$ suffisamment proche de λ_0 , le nombre de points $x = (\lambda, \mu) \in F_\alpha(\mathbf{D})$ est exactement e_α , pour tout $\alpha \in \llbracket 1, \ell \rrbracket$.

Enfin, nous **supposerons** que pour $\lambda_0 \in \mathbb{C}$ fixé, si μ_0 et μ'_0 sont deux racines distinctes de P_{λ_0} , les branches locales de \mathcal{C} en $x_0 = (\lambda_0, \mu_0)$ sont disjointes des branches locales de \mathcal{C} en $x'_0 = (\lambda'_0, \mu'_0)$.

1. Soit $(F_\alpha(\mathbf{D}))_{\alpha \in \llbracket 1, \ell \rrbracket}$ la famille des branches locales de \mathcal{C} en un point $x_0 = (\lambda_0, \mu_0)$ de \mathcal{C} . Démontrer que la multiplicité de x_0 dans \mathcal{C} vérifie :

$$d(x_0) = \sum_{\alpha=1}^{\ell} e_\alpha d_\alpha$$

2. On suppose jusqu'à la fin du problème que $A + \lambda B$ est diagonalisable, pour λ dans \mathbb{C} . Soit $(F_\alpha(\mathbf{D}))_{\alpha \in \llbracket 1, \ell \rrbracket}$ la famille des branches locales de \mathcal{C} en $x_0 = (\lambda_0, \mu_0)$ et z un point de $\mathbf{D} \setminus \{0\}$.

On définit l'espace vectoriel, pour $\alpha \in \llbracket 1, \ell \rrbracket$:

$$V_\alpha(z) = \{\psi \in \mathbb{C}^n \mid (A + f_\alpha(z)B)\psi = g_\alpha(z)\psi\}$$

et l'espace vectoriel associé $V_\alpha(0)$ comme en **III.A.3**.

Nous admettrons la relation suivante :

$$E_{\mu_0}(A + \lambda_0 B) = \sum_{\alpha=1}^{\ell} V_\alpha(0)$$

Montrer alors que la ramification e_α de $F_\alpha(\mathbf{D})$ est égale à 1, pour tout $\alpha \in \llbracket 1, \ell \rrbracket$.

3.

- (a) Établir l'existence de n fonctions entières $\mu_i : \mathbb{C} \rightarrow \mathbb{C}$ telles que \mathcal{C} coïncide avec la réunion des graphes de μ_i , $1 \leq i \leq n$.
- (b) Démontrer l'existence de nombres complexes a_i, b_i , $1 \leq i \leq n$, tels que :

$$(\forall i \in \llbracket 1, n \rrbracket), (\forall \lambda \in \mathbb{C}), \mu_i(\lambda) = a_i + \lambda b_i$$

4. Notation : pour $i \in \llbracket 1, n \rrbracket$, $\lambda \in \mathbb{C}$ et $r > 0$, $\Gamma_i(\lambda, r)$ désigne le cercle de centre $\mu_i(\lambda)$ et de rayon r .

- (a) Démontrer l'existence de réels $\rho > 0$ et $A > 0$ tel que, pour tout $\lambda \in \mathbb{C}$ et tout $r > 0$:

$$(0 < r < \rho) \text{ et } (|\lambda| > A) \Rightarrow (\forall i \in \llbracket 1, n \rrbracket), (\forall \mu \in \Gamma_i(\lambda, r)), A + \lambda B - \mu I_n \text{ inversible}$$

- (b) On note $R(\lambda, \mu)$ l'inverse de $A + \lambda B - \mu I_n$ lorsqu'il existe et on fixe $0 < r < \rho$.
Démontrer que pour tout $j \in \llbracket 1, n \rrbracket$, la formule :

$$\Pi_{j,r}(\lambda) = -\frac{1}{2i\pi} \int_{\Gamma_j(\lambda,r)} R(\lambda, \mu) d\mu$$

définit une application holomorphe Π de l'ouvert $\mathcal{U}_A = \{\lambda \in \mathbb{C} \mid |\lambda| > A\}$ dans $\mathcal{M}_n(\mathbb{C})$.

- (c) Démontrer que, si en plus B est diagonalisable, chaque $\Pi_{j,r}(\lambda)$ admet une limite dans $\mathcal{M}_n(\mathbb{C})$ lorsque $|\lambda|$ tend vers l'infini, pour tout $j \in \llbracket 1, n \rrbracket$.
5. On considère A et B deux matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$. On suppose que $A + \lambda B$ est diagonalisable, pour tout $\lambda \in \mathbb{C}$. Démontrer que A et B commutent.