Groupes finis de matrices

Ici $\mathbb{K}$ est un corps commutatif, a priori, de caractéristique nulle, ce qui signifie que le morphisme d'anneaux $k \mapsto k \cdot 1$ de $\mathbb{Z}$ dans $\mathbb{K}$ est injectif, ce qui est encore équivalent à dire que l'égalité $k\lambda = 0$ dans $\mathbb{K}$ avec $k \in \mathbb{Z}$ et $\lambda \in \mathbb{K}^*$ équivaut à $k = 0$.

Un corps de caractéristique nulle est infini puisqu'il contient un sous-groupe isomorphe à $\mathbb{Z}$ (et même un sous-corps isomorphe à $\mathbb{Q}$).

Pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$, on note $\operatorname{tr}(A)$ sa trace.

On présente ici, sous forme d'exercices, quelques résultats sur les groupes finis de matrices.

Exercice 1 *Soit G un sous-groupe fini de $GL_n(\mathbb{K})$ de cardinal $p \geq 2$.*

1. *Montrer que $B = \frac{1}{p} \sum_{A \in G} A$ est la matrice dans la base canonique de $\mathbb{K}^n$ d'un projecteur.*
2. *Montrer que $\sum_{A \in G} \operatorname{tr}(A)$ est un entier divisible par p.*
3. *Montrer que si $\sum_{A \in G} \operatorname{tr}(A) = 0$, alors $\sum_{A \in G} A = 0$.*

Solution 2

1. *Il s'agit de montrer que $B^2 = B$.*
   On a :
   $$B^2 = BB = \frac{1}{p} \sum_{A \in G} BA$$
   avec :
   $$BA = \frac{1}{p} \sum_{A' \in G} A'A = \frac{1}{p} \sum_{A'' \in G} A'' = B$$
   du fait que l'application $A' \mapsto A'A$ réalise une permutation de G, ce qui donne :
   $$B^2 = \frac{1}{p} \sum_{A \in G} B = B$$
2. *La matrice B étant celle d'un projecteur, on a $\operatorname{tr}(B) = \operatorname{rang}(B) = \dim(\operatorname{Im}(B)) \in \mathbb{N}$ et en conséquence $\sum_{A \in G} \operatorname{tr}(A) = p \operatorname{tr}(B)$ est un entier divisible par p.*
3. *Si $\sum_{A \in G} \operatorname{tr}(A) = 0$, on a alors $p \operatorname{tr}(B) = 0$ et $\operatorname{rang}(B) = \operatorname{tr}(B) = 0$ puisque $\mathbb{K}$ est de caractéristique nulle, donc $\operatorname{Im}(B) = \{0\}$ et $B = 0$, soit $\sum_{A \in G} A = 0$.*

Exercice 3 *Soit F un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ contenant I_n et stable par le produit matriciel. Montrer que $G = F \cap GL_n(\mathbb{K})$ est un sous-groupe infini de $GL_n(\mathbb{K})$.*

Solution 4 *G est infini puisqu'il contient toutes les homothéties λI_n de rapport $\lambda \in \mathbb{K}^*$ (F est un espace vectoriel qui contient I_n et $\mathbb{K}$ est infini).*
Si A, B sont dans G, alors AB est également dans G puisque F est stable par le produit matriciel. Il reste à montrer que si $A \in G$, alors A^{-1} est dans F, ce qui résulte du fait que A^{-1} est un polynôme en A pour $A \in GL_n(\mathbb{K})$. En effet, le théorème de Cayley-Hamilton nous dit que si $P(X) = \sum_{k=0}^{n} \alpha_k X^k$ est le polynôme caractéristique de A, on a alors $P(A) = 0$ et avec $\alpha_0 = \det(A) \neq 0$, on déduit que $A^{-1} = -\frac{1}{\alpha_0} \sum_{k=1}^{n} \alpha_k A^{k-1} \in F$ puisque F contient I_n est stable par le produit et c'est un espace vectoriel.

Exercice 5 *On se place sur $\mathbb{R}^n$ muni du produit scalaire euclidien canonique noté $\langle \cdot \mid \cdot \rangle$ et on se donne G un sous-groupe fini G de $GL(\mathbb{R}^n)$.*

1. *Montrer que l'application :*
$$\varphi : (x, y) \mapsto \sum_{g \in G} \langle g(x) \mid g(y) \rangle$$
définit un produit scalaire sur $\mathbb{R}^n$.
2. *Montrer que pour tout* $g \in G$ *et tous* x, y *dans* $\mathbb{R}^n$, *on a :*
$$\varphi(g(x), y) = \varphi\left(x, g^{-1}(y)\right)$$
3. *Montrer que si* F *est un sous-espace vectoriel de* $\mathbb{R}^n$ *stable par tous les éléments de* G, *il admet alors un supplémentaire stable par tous les éléments de* G.

Solution 6

1. *Comme une somme de produits scalaires est un produit scalaire, il suffit de montrer que pour tout* $g \in G \subset GL(\mathbb{R}^n)$, *l'application* $(x, y) \mapsto \langle g(x) \mid g(y) \rangle$ *définit un produit scalaire sur* $\mathbb{R}^n$, *ce qui résulte du fait que* g *est un isomorphisme.*
2. *Pour* $g \in G$ *et* x, y *dans* $\mathbb{R}^n$, *on a :*
$$\begin{aligned} \varphi(g(x), y) &= \sum_{u \in G} \langle u(g(x)) \mid u(y) \rangle = \sum_{u \in G} \left\langle u \circ g(x) \mid u \circ g\left(g^{-1}(y)\right) \right\rangle \\ &= \sum_{v \in G} \left\langle v(x) \mid v\left(g^{-1}(y)\right) \right\rangle = \varphi\left(x, g^{-1}(y)\right) \end{aligned}$$
du fait que l'application $u \mapsto u \circ g$ *est une permutation de* G.
3. *Soient* $H = F^{\varphi, \perp}$ *le supplémentaire orthogonal de* F *pour le produit scalaire* φ *et* $g \in G$.
Comme F *est stable par* g, *on a* $g(F) = F$ $(g(F) \subset F$ *et l'égalité par les dimensions car* g *est un automorphisme) et* $g^{-1}(F) = F$. *Il en résulte que pour tout* $x \in H$ *et* $y \in F$, *on a* $\varphi(g(x), y) = \varphi\left(x, g^{-1}(y)\right) = 0$ *et* $g(x) \in H$. *On a donc* $g(H) \subset H$ *et l'égalité par les dimensions. L'espace vectoriel* H *est donc un supplémentaire de* F *stable par* G.

Exercice 7 *Avec cet exercice, on propose une démonstration du théorème de réduction des matrices orthogonales réelles. Ce résultat sera utile pour l'exercice qui suit.*
On se place dans un espace euclidien E *de dimension* $n \geq 1$.
Un endomorphisme $u \in \mathcal{L}(E)$ *est dit orthogonal si :*
$$\forall (x, y) \in E^2, \ \langle u(x) \mid u(y) \rangle = \langle x \mid y \rangle .$$
On note $\mathcal{O}(E)$ *l'ensemble des endomorphismes orthogonaux de* E.
On rappelle que $u \in \mathcal{O}(E)$ *si, et seulement si, pour toute base orthonormée* $\mathcal{B}$ *de* E *la matrice* A *de* u *dans* $\mathcal{B}$ *est telle que* $A\,{}^tA = {}^tAA = I_n$. *Une telle matrice* A *est dite orthogonale et on note* $\mathcal{O}_n(\mathbb{R})$ *le groupe multiplicatif de toutes ces matrices orthogonales.*

1. *Montrer que pour tout endomorphisme* u *de* E *il existe un sous espace vectoriel* P *de* E *de dimension* 1 *ou* 2 *stable par* u.
2. *Soit* $u \in \mathcal{O}(E)$. *Montrer qu'il existe des sous espaces vectoriels de* E, $P_1, \cdots, P_r$, *de dimension égale à* 1 *ou* 2, *deux à deux orthogonaux, stables par* u *et tels que* $E = \overset{r}{\underset{j=1}{\oplus}} P_j$.
3. *Vérifier que si* $A \in \mathcal{O}_n(\mathbb{R})$, *on a alors* $\det(A) = \pm 1$ *et les seules valeurs propres réelles possibles de* A *sont* -1 *et* 1.
4. *Soit* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}_2(\mathbb{R})$. *Montrer que l'on a :*
$$A = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \text{ ou } A = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$
avec $\theta \in [0, 2\pi[$ *et que dans le deuxième cas,* A *est orthogonalement semblable à* $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

5. *Soit $A \in \mathcal{O}_n(\mathbb{R})$ avec $n \geq 2$. Montrer qu'il existe une matrice $P \in \mathcal{O}_n(\mathbb{R})$ telle que :*

$$P^{-1}AP = \begin{pmatrix} I_p & 0 & 0 & 0 & \cdots & 0 \\ 0 & -I_q & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & R_1 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & R_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & R_r \end{pmatrix},$$

où, pour tout $k \in \{1, \cdots, r\}$, on a noté :

$$R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$$

avec $\theta_k \in]0, 2\pi[- \{\pi\}$ et p, q, r sont des entiers naturels tels $p + q + 2r = n$ (si l'un de ces entiers est nul, les blocs de matrices correspondants n'existent pas).

Solution 8

1. *Si u a une valeur propre réelle λ, alors pour tout vecteur propre associé $x \in E \setminus \{0\}$, la droite $D = \mathbb{R}x$ est stable par u.*
   Sinon $n \geq 2$ et le polynôme minimal π_u se décompose dans l'anneau factoriel $\mathbb{R}[X]$ en produit de facteurs irréductibles de degré 2 (les valeurs propres de u sont les racines de π_u). Ce polynôme π_u s'écrit donc $\pi_u(X) = \left(X^2 + bX + c\right) Q(X)$ avec $b^2 - 4c < 0$ et $Q(u) \neq 0$ (π_u est le polynôme non nul de plus petit degré annulant u). De l'égalité :

$$0 = \pi_u(u) = \left(u^2 + bu + cId\right) \circ Q(u)$$

   on déduit alors que l'endomorphisme $u^2 + bu + cId$ n'est pas injectif, c'est-à-dire que son noyau n'est pas réduit à $\{0\}$. Pour tout vecteur x non nul dans ce noyau on vérifie alors que $P = \mathrm{Vect}\{x, u(x)\}$ est un sous espace vectoriel de dimension 2 stable par u. En effet, P est de dimension 2 puisque x n'est pas vecteur propre de u et avec $u^2(x) + bu(x) + cx = 0$ on déduit que $u^2(x)$ est dans P, ce qui entraîne que P est stable par u.

2. *On procède par récurrence sur la dimension $n \geq 1$ de E.*
   Pour $n = 1$ ou 2, le résultat est évident.
   Supposons le acquis pour tout endomorphisme orthogonal sur un espace vectoriel euclidien de dimension p comprise entre 1 et $n - 1$, avec $n \geq 3$.
   Si P_1 est un sous espace vectoriel de E non réduit à $\{0\}$ de dimension au plus égale à 2 stable par $u \in \mathcal{O}(E)$, alors $P_1^\perp$ est stable par u. En effet $u(P_1) \subset P_1$ et $u \in GL(E)$ entraînent $u(P_1) = P_1$ (un isomorphisme conserve la dimension), donc tout $y \in P_1$ s'écrit $y = u(x)$ avec $x \in P_1$ et pour tout $z \in P_1^\perp$, on a :

$$\langle u(z) \mid y \rangle = \langle u(z) \mid u(x) \rangle = \langle z \mid x \rangle = 0$$

   c'est-à-dire que $u(z) \in P_1^\perp$.
   Comme $1 \leq n - 2 \leq \dim\left(P_1^\perp\right) \leq n - 1$, on peut trouver des sous espaces vectoriels de E, $P_2, \cdots, P_r$, de dimension au plus 2, deux à deux orthogonaux et stables par la restriction de u à $P_1^\perp$, donc par u, tels que $P_1^\perp = \overset{r}{\underset{j=2}{\oplus}} P_j$. On a alors $E = P_1 \oplus P_1^\perp = \overset{r}{\underset{j=1}{\oplus}} P_j$.

3. *Pour tout $A \in \mathcal{O}_n(\mathbb{R})$, on a $A\,{}^tA = I_n$ et $\det\left(A\,{}^tA\right) = (\det(A))^2 = 1$, donc $\det(A) = \pm 1$.*
   Si λ est une valeur propre réelle de A et x un vecteur propre associé unitaire de $\|Ax\| = \|x\|$, on déduit que $\lambda = \pm 1$.

4. *Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{O}_2(\mathbb{R})$, les égalités $A\,{}^tA = I_n$ et $\det(A) = \pm 1$ se traduisent par :*

$$\begin{cases} a^2 + b^2 = c^2 + d^2 = 1, \\ ac + bd = 0 \\ ad - bc = \pm 1 \end{cases}$$

Des deux premières égalités, on déduit qu'il existe deux réels α et β tels que $(a,b) = (\cos(\alpha), \sin(\alpha))$ et $(c,d) = (\cos(\beta), \sin(\beta))$ et avec les deux dernières, qu'on a $\cos(\alpha - \beta) = 0$ et $\sin(\alpha - \beta) = \pm 1$. On a donc $\beta = \alpha \pm \frac{\pi}{2}$.
Pour $\beta = \alpha + \frac{\pi}{2}$, on a :

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

avec $\theta = -\alpha + 2k\pi \in [0, 2\pi[$.
Pour $\beta = \alpha - \frac{\pi}{2}$, on a :

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

avec $\theta = -\alpha + 2k\pi \in [0, 2\pi[$. Cette matrice est symétrique, donc $A^2 = A\,{}^tA = I_n$ et elle est diagonalisable puisque annulée par $X^2 - 1$ qui est scindé à racines simples dans $\mathbb{R}$. Comme $A \neq \pm I_n$, elle est orthogonalement semblable à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Ce que l'on peut vérifier avec :

$$\begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & \sin\left(\frac{\theta}{2}\right) \\ -\sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix}$$

5. *On procède par récurrence sur $n \geq 2$.*
Pour $n = 2$, c'est fait.
Supposons le résultat acquis pour toute matrice orthogonale d'ordre p compris entre 2 et $n-1$ et soit A une matrice orthogonale d'ordre $n \geq 3$.
On désigne par u l'endomorphisme orthogonal ayant A pour matrice dans la base canonique de $E = \mathbb{R}^n$ muni de sa structure euclidienne canonique.
Si u admet 1 ou -1 comme valeur propre, pour tout vecteur propre unitaire x associé à cette valeur propre, le sous espace vectoriel $(\mathbb{R}x)^\perp$ est stable par u (pour $y \in (\mathbb{R}x)^\perp$, on a $\langle u(y) \mid x \rangle = \pm \langle u(y) \mid u(x) \rangle = \pm \langle y \mid x \rangle = 0$) et il existe alors une base orthonormée $\mathcal{B}$ de $(\mathbb{R}x)^\perp$ dans laquelle la matrice de la restriction de u à $(\mathbb{R}x)^\perp$ est de la forme :

$$A' = \begin{pmatrix} I_p & 0 & 0 & 0 & \cdots & 0 \\ 0 & -I_q & 0 & \ddots & \ddots & \vdots \\ 0 & 0 & R_1 & 0 & \ddots & 0 \\ 0 & \ddots & 0 & R_2 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & R_r \end{pmatrix}.$$

Dans la base orthonormée $\{x\} \cup \mathcal{B}$ la matrice de u est $A'' = \begin{pmatrix} \pm 1 & 0 \\ 0 & A' \end{pmatrix}$, qui se ramène bien à la forme souhaitée en permuttant au besoin x avec l'un des vecteurs de $\mathcal{B}$.
Si toutes les valeurs propres de u sont complexes non réelles, on a alors une décomposition $E = \overset{r}{\underset{k=1}{\oplus}} P_k$ où les P_k sont de dimension 2, deux à deux orthogonaux et stables par u. L'étude du cas $n = 2$ nous dit alors qu'il existe, pour tout k compris entre 1 et r, une base orthonormée $\mathcal{B}_k$ de P_k dans laquelle la matrice de u est de la forme :

$$R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix},$$

avec $\theta_k \in]0, 2\pi[- \{\pi\}$. En réunissant toutes ces bases, on obtient une base orthonormée de E dans *laquelle la matrice de u est :*

$$A' = \begin{pmatrix} R_1 & 0 & \cdots & 0 \\ 0 & R_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & R_r \end{pmatrix}.$$

Exercice 9 *Soit G un sous-ensemble de $\mathcal{O}_n(\mathbb{R})$. Montrer que s'il existe $m \in \mathbb{N}^*$ tel que $A^m = I_n$ pour tout $A \in G$ (dans le cas où G est un groupe, on dit qu'il est d'exposant fini), alors l'ensemble :*

$$\mathrm{tr}(G) = \{\mathrm{tr}(A) \mid A \in G\}$$

est fini.

Solution 10 *On sait que toute matrice $A \in O_n(\mathbb{R})$ est orthogonalement semblable à une matrice diagonale par blocs de la forme :*

$$D = \mathrm{diag}(I_p, -I_q, R_1, \cdots, R_r)$$

où $R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$ avec $\theta_k \in]0, 2\pi[- \{\pi\}$.
Dans le cas où toute matrice de G est orthogonalement semblable à une matrice de la forme $\mathrm{diag}(I_p, -I_q)$, on a :

$$\mathrm{tr}(G) \subset \left\{p - q \mid (p, q) \in \mathbb{N}^2 \text{ et } p + q = n\right\}$$

et cet ensemble est fini.
S'il existe dans G une matrice A orthogonalement semblable à une matrice de la forme $D = \mathrm{diag}(I_p, -I_q, R_1, \cdots, R_r$ alors la matrice A^m est semblable à :

$$D^m = \mathrm{diag}(I_p, (-1)^m I_q, R(m\theta_1), \cdots, R(m\theta_r))$$

et la condition $A^m = I_n$ impose $m\theta_k \in]0, 2m\pi[\cap 2\pi\mathbb{Z}$, ce qui entraîne que les θ_k ne prennent qu'un nombre fini de valeurs et :

$$\mathrm{tr}(G) \subset \left\{p - q + 2\sum_{k=1}^{r} \cos(\theta_k) \mid (p, q, r) \in \mathbb{N}^3,\ p + q + 2r = n,\ m\theta_k \in]0, 2m\pi[\cap 2\pi\mathbb{Z}\right\}$$

est fini.

Exercice 11 *On se propose de montrer que si G est un sous-groupe de $\mathcal{O}_n(\mathbb{R})$ tel que $\mathrm{tr}(G)$ soit fini, alors G est fini.*
Soient G un sous-groupe de $\mathcal{O}_n(\mathbb{R})$, F le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{R})$ engendré par G et $\mathcal{B} = (A_i)_{1 \leq i \leq p}$ une base de F extraite de G.

1. *Montrer que l'application $(A, B) \mapsto \langle A \mid B \rangle = \mathrm{tr}\left(A\ {}^tB\right)$ définit un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$.*
2. *Montrer que la matrice $B = \left(\left(\mathrm{tr}\left(A_i\ {}^tA_j\right)\right)\right)_{1 \leq i,j \leq p}$ est inversible dans $\mathcal{M}_p(\mathbb{R})$.*
3. *Montrer que si $\mathrm{tr}(G)$ est fini, alors G est fini.*
4. *Le résultat de la question précédente est-il encore vrai pour un sous-groupe de $GL_n(\mathbb{R})$?*

Solution 12

1. *On vérifie facilement que l'application $\langle \cdot \mid \cdot \rangle$ est bilinéaire (linéarité de la trace et de la transposition et bilinéarité du produit) et symétrique ($\mathrm{tr}\left(B\ {}^tA\right) = \mathrm{tr}\left({}^t\left(B\ {}^tA\right)\right) = \mathrm{tr}\left(A\ {}^tB\right)$). Pour $A = ((a_{ii}))_{1 \leq i,j \leq n}$ dans $\mathcal{M}_n(\mathbb{R})$, on a :*

$$\begin{aligned} \langle A \mid A \rangle = \mathrm{tr}\left(A\ {}^tA\right) &= \sum_{i=1}^{n} \left(\left(A\ {}^tA\right)\right)_{ii} \\ &= \sum_{i=1}^{n} (a_{i1}, \cdots, a_{in})\ {}^t(a_{i1}, \cdots, a_{in}) \\ &= \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij}^2 \end{aligned}$$

et en conséquence l'application $\langle \cdot \mid \cdot \rangle$ est définie positive. C'est donc un produit scalaire sur $\mathcal{M}_n(\mathbb{R})$. C'est en fait le produit scalaire canonique de $\mathcal{M}_n(\mathbb{R})$ identifié à $\mathbb{R}^{n^2}$.

2. *La matrice B est la matrice du produit scalaire $\langle \cdot \mid \cdot \rangle$ de F dans la base $\mathcal{B}$. Elle est donc inversible de déterminant strictement positif (c'est une matrice de Gram).*
3. *Tout matrice $A \in G$ s'écrit, de manière unique :*

$$A = \sum_{j=1}^{p} \lambda_j(A) A_j,$$

les $\lambda_j(A)$, pour j compris entre 1 et p, étant réels. On a alors pour tout i compris entre 1 et p :

$$\langle A_i \mid A \rangle = \sum_{j=1}^{p} \lambda_j(A) \langle A_i \mid A_j \rangle$$

et en notant :

$$\lambda(A) = \begin{pmatrix} \lambda_1(A) \\ \vdots \\ \lambda_p(A) \end{pmatrix}, \ \tau(A) = \begin{pmatrix} \langle A_1 \mid A \rangle \\ \vdots \\ \langle A_p \mid A \rangle \end{pmatrix},$$

cela s'écrit $\tau(A) = B\lambda(A)$, ce qui équivaut à $\lambda(A) = B^{-1}\tau(A)$, puisque B est inversible.
D'autre part, pour $A \in G \subset \mathcal{O}_n(\mathbb{R})$, on a ${}^tA = A^{-1} \in G$ et $A_i\,{}^tA = A_iA^{-1} \in G$ pour tout i compris entre 1 et p. Avec l'hypothèse $\mathrm{tr}(G)$ fini, on déduit alors que $\tau(A)$ ne prend qu'un nombre fini de valeurs dans $\mathbb{R}^p$ quand A décrit G et il en est de même de $\lambda(A) = B^{-1}\tau(A)$. Il en résulte que le groupe G est fini.
Avec l'exercice précédent, on en déduit qu'un sous-groupe G d'exposant fini de $\mathcal{O}_n(\mathbb{R})$ est fini.
4. *L'ensemble G des matrices triangulaires supérieures réelles à diagonale unité forme un sous-groupe infini de $GL_n(\mathbb{R})$ tel que $\mathrm{tr}(G) = \{n\}$. Le résultat de la question précédente n'est donc pas vrai sur $GL_n(\mathbb{R})$.*

Exercice 13 *Cet exercice nous sera utile pour celui qui suit.*
On dit qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente s'il existe un entier q strictement positif tel que $A^{q-1} \neq 0$ et $A^q = 0$ (q est l'indice de nilpotence de A).

1. *Montrer que si $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente, alors 0 est valeur propre de A et $\mathrm{Tr}(A) = 0$.*
2. *Montrer qu'une matrice $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente si et seulement si $\mathrm{tr}\left(A^k\right) = 0$ pour tout entier naturel non nul k.*

Solution 14

1. *Si $A \in \mathcal{M}_n(\mathbb{K})$ est nilpotente d'ordre $q \geq 1$, son polynôme minimal est alors $\pi_A(X) = X^q$ avec $q \geq 1$ (on a $A^q = 0$, donc π_A divise X^q $A^{q-1} \neq 0$ nous dit que $\pi_A(X) = X^q$) et 0 est l'unique valeur propre de A.*
Pour montrer que la trace d'une matrice nilpotente est nulle, on procède par récurrence sur $n \geq 1$ (pour $\mathbb{K}$ algébriquement clos, cette trace est la somme des valeurs propres et c'est terminé).
Pour $n = 1$, l'unique matrice nilpotente est la matrice nulle.
Supposons le résultat acquis pour $1 \leq p \leq n-1$ et soit $A \in \mathcal{M}_n(\mathbb{K})$ nilpotente d'ordre $q \geq 1$. On désigne par u l'endomorphisme canoniquement associé à A. Comme 0 est valeur propre de u, il existe un vecteur non nul e_1 dans le noyau de u et en complétant ce vecteur en une base $\mathcal{B}$ de E, la matrice de u dans cette base est de la forme $B = \begin{pmatrix} 0 & \alpha \\ 0 & C \end{pmatrix}$ où $\alpha \in \mathcal{M}_{1,n-1}(\mathbb{K})$ et $C \in \mathcal{M}_{n-1}(\mathbb{K})$. Avec $B^q = \begin{pmatrix} 0 & \alpha C^{q-1} \\ 0 & C^q \end{pmatrix} = 0$, on déduit que C est nilpotente et en conséquence $\mathrm{Tr}(C) = 0$ (hypothèse de récurrence), ce qui entraîne $\mathrm{Tr}(A) = \mathrm{Tr}(B) = \mathrm{Tr}(C) = 0$.

2. Si A est nilpotente dans $\mathcal{M}_n(\mathbb{K})$, il en est de même de A^k pour tout entier naturel non nul k et $\operatorname{tr}(A^k) = 0$.
   Pour la réciproque, on procède par récurrence sur $n \geq 1$. Pour $n = 1$, on a $\operatorname{tr}(A) = A$ et le résultat est trivial. Supposons le acquis pour les matrices réelles d'ordre au plus égal à n et soit $A \in \mathcal{M}_{n+1}(\mathbb{K})$ telle que $\operatorname{tr}(A^k) = 0$ pour tout $k \geq 1$. Si $P(X) = \sum_{k=0}^{n+1} \alpha_k X^k$ est le polynôme caractéristique de A, avec $P(A) = 0$ et $\operatorname{tr}(A^k) = 0$ pour $k = 1, \cdots, n+1$, on déduit que $\operatorname{tr}(P(A)) = n\alpha_0 = 0$ et $\alpha_0 = \det(A) = 0$ puisque $\mathbb{K}$ est de caractéristique nulle, c'est-à-dire que 0 est valeur propre de A et il existe une matrice $P \in GL_{n+1}(\mathbb{K})$ telle que $P^{-1}AP = \begin{pmatrix} 0 & b \\ 0 & C \end{pmatrix}$ où $b \in \mathcal{M}_{1,n}(\mathbb{K})$ et $C \in \mathcal{M}_n(\mathbb{K})$. Avec $P^{-1}A^kP = \begin{pmatrix} 0 & bC^{k-1} \\ 0 & C^k \end{pmatrix}$, on déduit que $\operatorname{tr}(C^k) = \operatorname{tr}(A^k) = 0$ pour tout $k \geq 1$ et avec l'hypothèse de récurrence il en résulte que C est nilpotente. Enfin, en notant p l'indice de nilpotence de C, avec $A^{p+1} = P \begin{pmatrix} 0 & bC^p \\ 0 & C^{p+1} \end{pmatrix} P^{-1} = 0$, on déduit que A est nilpotente.

Exercice 15 *Soient G un sous-groupe de $GL_n(\mathbb{K})$, F le sous-espace vectoriel de $\mathcal{M}_n(\mathbb{K})$ engendré par G et $\mathcal{B} = (A_i)_{1 \leq i \leq p}$ une base de F extraite de G.*

1. On considère l'application :

$$\varphi: \begin{array}{ccc} G & \to & \mathbb{K}^p \\ A & \mapsto & (\operatorname{tr}(AA_1), \cdots, \operatorname{tr}(AA_p)) \end{array}$$

   et A, B dans G telles que $\varphi(A) = \varphi(B)$.
   (a) Montrer que $\operatorname{tr}(AB^{-1}M) = \operatorname{tr}(M)$ pour tout $M \in G$.
   (b) En notant $C = AB^{-1}$, en déduire que $\operatorname{tr}(C^k) = n$ pour tout $k \geq 1$, puis que $C - I_n$ est nilpotente.
   (c) En déduire que, si on suppose de plus que toutes les matrices de G sont diagonalisables, alors φ est injective.
2. Montrer que si toutes les matrices de G sont diagonalisables et si $\operatorname{tr}(G)$ est fini, alors G est fini.
3. Déduire de ce qui précède qu'un sous-groupe G de $GL_n(\mathbb{C})$ est fini si, et seulement si, il est d'exposant fini (c'est-à-dire qu'il existe $m \in \mathbb{N}^*$ tel que $A^m = I_n$ pour tout $A \in G$). Ce résultat est un théorème de Burnside.

Solution 16

1.
   (a) Si A, B dans G sont telles que $\varphi(A) = \varphi(B)$, on a alors $\operatorname{tr}((A - B)A_j) = 0$ pour tout j compris entre 1 et p et $\operatorname{tr}((A - B)M) = 0$ pour tout $M \in F$. On a alors $\operatorname{tr}((AB^{-1} - I_n)BM) = 0$ pour tout $M \in G$, ce qui équivaut à $\operatorname{tr}((AB^{-1} - I_n)M) = 0$ pour tout $M \in G$ puisque l'application $M \mapsto BM$ est une permutation de G.
   (b) On a $C = AB^{-1} \in G$ (G est un groupe) et $\operatorname{tr}(CM) = \operatorname{tr}(M)$ pour tout $M \in G$, ce qui entraîne $\operatorname{tr}(C) = \operatorname{tr}(I_n) = n$ et par récurrence $\operatorname{tr}(C^k) = n$ pour tout $k \geq 1$. On a alors, pour tout $k \geq 1$:

$$\operatorname{tr}\left((C - I_n)^k\right) = \sum_{j=0}^{k} C_k^j (-1)^j \operatorname{tr}\left(C^{k-j}\right) = n \sum_{j=0}^{k} C_k^j (-1)^j = n(1-1)^k = 0.$$

   Il en résulte que $C - I_n$ est nilpotente.
   (c) La matrice C étant dans G est diagonalisable et il en est de même de $C - I_n$. Cette matrice est donc diagonalisable et nilpotente et en conséquence nulle (sa seule valeur propre est 0). On a donc $C = AB^{-1} = I_n$ et $A = B$. L'application φ est donc injective.
2. Si $\operatorname{tr}(G)$ est fini, alors $\varphi(G)$ est une partie finie de $\mathbb{R}^p$ en bijection avec G et G est fini.

3. *Le théorème de Lagrange nous dit qu'un groupe fini est d'exposant fini.*
   Si G est un sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini, il existe alors un entier $m \geq 1$ tel que $A^m = I_n$ pour tout $A \in G$ et toutes les matrices de A sont diagonalisables du fait qu'elles sont annulées par le polynôme $X^m - 1$ qui est scindé à racines simples dans $\mathbb{C}$. Les valeurs propres de tout $A \in G$ étant racines de $X^m - 1$ sont dans le groupe Γ_m de ces racines de l'unité et en conséquence en nombre fini quand A décrit G. Il en résulte que $\operatorname{tr}(G)$ est fini est fini et aussi G.

Exercice 17 *Montrer que pour tout nombre premier $p \geq 2$ et tout entier $n \geq 1$, on a :*

$$\begin{aligned}\operatorname{card}(GL_n(\mathbb{Z}_p)) &= (p^n - 1)(p^n - p)\cdots\left(p^n - p^{n-1}\right)\\ &= p^{\frac{n(n-1)}{2}}(p^n - 1)\left(p^{n-1} - 1\right)\cdots(p-1)\end{aligned}$$

et qu'il existe dans $GL_n(\mathbb{Z}_p)$ un sous-groupe d'ordre $p^{\frac{n(n-1)}{2}}$.

Solution 18 *Pour $n = 1$, $GL_1(\mathbb{Z}_p)$ est isomorphe à $\mathbb{Z}_p^{\times} = \mathbb{Z}_p \setminus \{0\}$ qui a $p-1$ éléments.*
De manière général, $GL_n(\mathbb{Z}_p)$ est en bijection avec l'ensemble de toutes les bases de $\mathbb{Z}_p^n$ par l'application qui associe à une base $\mathcal{B}$ de $\mathbb{Z}_p^n$ la matrice de passage de la base canonique à $\mathcal{B}$.
Pour dénombrer ces bases, on procède comme suit : pour le premier vecteur de base, il y a $p^n - 1$ possibilités (tous les vecteurs de $\mathbb{Z}_p^n \setminus \{0\}$) ; ce premier vecteur e_1 étant choisi, le deuxième vecteur doit être choisi dans $\mathbb{Z}_p^n \setminus \mathbb{Z}_p e_1$ et il y a $p^n - p$ possibilités ; les deux premiers vecteurs e_1 et e_2 étant choisi, le troisième vecteur doit être choisi dans $\mathbb{Z}_p^n \setminus \mathbb{Z}_p e_1 \oplus \mathbb{Z}_p e_2$ et il y a $p^n - p^2$ possibilités ; continuant ainsi de suite, on aboutit à :

$$\begin{aligned}\operatorname{card}(GL_n(\mathbb{Z}_p)) &= (p^n - 1)(p^n - p)\cdots\left(p^n - p^{n-1}\right)\\ &= p^{1+2+\cdots+(n-1)}(p^n - 1)\left(p^{n-1} - 1\right)\cdots(p^n - 1)\\ &= p^{\frac{n(n-1)}{2}}(p^n - 1)\left(p^{n-1} - 1\right)\cdots(p^n - 1)\end{aligned}$$

Le groupe H formé des matrices triangulaires supérieures de termes diagonaux tous égaux à 1 est un sous-groupe d'ordre $p^{\frac{n(n-1)}{2}}$ de $GL_n(\mathbb{Z}_p)$.

Exercice 19 *Soit $\mathbb{K}$ un corps fini (et commutatif, d'après le théorème de Wedderburn) et φ un morphisme de groupes de $GL_n(\mathbb{K})$ dans $\mathbb{K}^*$. On note $(E_{ij})_{1 \leq i,j \leq n}$ la base canonique de $\mathcal{M}_n(\mathbb{K})$. Pour $\lambda \in \mathbb{K}^*$ on note :*

$$D_\lambda = I_n + (\lambda - 1)E_{nn}$$

une matrice de dilatation et pour $\lambda \in \mathbb{K}$, $i \neq j$ compris entre 1 et n :

$$T_\lambda = I_n + \lambda E_{ij}$$

une matrice de transvection (le couple (i,j) avec $i \neq j$ est fixé).

1. *Montrer qu'il existe un entier naturel r tel que :*
   $$\forall \lambda \in \mathbb{K}^*,\ \varphi(D_\lambda) = \lambda^r.$$
2. *Montrer que, pour $i \neq j$ fixés entre 1 et n et λ, μ dans $\mathbb{K}$, on a $T_\lambda T_\mu = T_{\lambda+\mu}$.*
3. *Que dire d'un morphisme de groupes de $(\mathbb{K}, +)$ dans $(\mathbb{K}^*, \cdot)$?*
4. *Montrer que, pour $i \neq j$ fixés entre 1 et n, on a :*
   $$\forall \lambda \in \mathbb{K},\ \varphi(T_\lambda) = 1.$$
5. *Déduire de ce qui précède que :*
   $$\forall A \in GL_n(\mathbb{K}),\ \varphi(A) = (\det(A))^r.$$

Solution 20 *On remarque que pour tout* $\lambda \in \mathbb{K}$ *on a* $\det(E_\lambda) = 1$ *et pour tout* $\lambda \in \mathbb{K}^*$, $\det(D_\lambda) = \lambda$.
On rappelle que si $T_\lambda = T_\lambda^{(i,j)}$ *est une matrice de transvection, alors la multiplication à gauche [resp. à droite] d'une matrice* A *par* T_λ *revient à effectuer l'opération élémentaire :*

$$L_i \mapsto L_i + \lambda L_j \ \ (\textit{rep. } C_j \mapsto C_j + \lambda C_i)$$

où L_i *[resp.* C_j*] désigne la ligne numéro* i *[resp. la colonne numéro* j*] de* A.
De plus $GL_n(\mathbb{K})$ *est engendré par l'ensembles des matrices de transvection ou dilatation, c'est-à-dire que tout matrice* $A \in GL_n(\mathbb{K})$ *s'écrit* $A = T_1 \cdots T_\alpha D_{\det(A)} T_{\alpha+1} \cdots T_\beta$, *où les* T_k *sont des matrices de transvection.*

1. *On sait que* $\mathbb{K}^*$ *est cyclique, soit* $\mathbb{K}^* = \left\{1, \mu, \cdots, \mu^{q-1}\right\}$. *Tout élément* λ *de* $\mathbb{K}^*$ *s'écrit donc* $\lambda = \mu^k$ *où* k *est compris entre* 0 *et* $q-1$ *et avec :*

$$D_\lambda = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & 1 & 0 \\ 0 & \cdots & 0 & \lambda \end{pmatrix} = D_\mu^k$$

   on a $\varphi(D_\lambda) = \varphi(D_\mu)^k$. *Puis en écrivant que* $\varphi(D_\mu) = \mu^r$ *dans* $\mathbb{K}^*$, *où* r *est un entier compris entre* 0 *et* $q-1$, *on déduit que* $\varphi(D_\lambda) = \mu^{rk} = \left(\mu^k\right)^r = \lambda^r$.
2. *Pour* $1 \leq i \neq j \leq n$, *on a* $E_{ij}^2 = 0$, *ce qui entraîne pour* λ, μ *dans* $\mathbb{K}$ *:*

$$T_\lambda T_\mu = I_n + (\lambda + \mu) E_{ij} + \lambda\mu E_{ij}^2 = T_{\lambda+\mu}.$$

   On peut aussi dire que $T_\lambda T_\mu$ *est déduit de* T_μ *en ajoutant à sa ligne* i *sa ligne* j *multipliée par* λ, *ce qui donne la matrice* $T_{\lambda+\mu}$.
   Prenant $\mu = -\lambda$, *on a* $T_\lambda T_{-\lambda} = T_0 = I_n$, *ce qui signifie que* T_λ *est inversible d'inverse* $T_{-\lambda}$ *(pour les mêmes indices* $i \neq j$*).*
3. *Soit* ψ *un morphisme de groupes de* $(\mathbb{K}, +)$ *dans* $(\mathbb{K}^*, \cdot)$. *Ces groupes étant finis, on a :*

$$\mathrm{card}(\mathbb{K}) = \mathrm{card}(\ker(\psi))\,\mathrm{card}(\mathrm{Im}(\psi)),$$

   c'est-à-dire que $\mathrm{card}(\mathrm{Im}(\psi))$ *divise* $q+1 = \mathrm{card}(\mathbb{K})$. *Mais* $\mathrm{Im}(\psi)$ *étant un sous-groupe de* $\mathbb{K}^*$ *a un cardinal qui divise* q *et nécessairement* $\mathrm{card}(\mathrm{Im}(\psi)) = 1$ *du fait que* $q+1$ *et* q *sont premiers entre eux. On a donc* $\mathrm{Im}(\psi) = \{\psi(0)\} = \{1\}$, *ce qui signifie que* ψ *est la fonction constante égale à* 1.
   L'exemple de la fonction exponentielle réelle ou complexe nous montre que ce résultat est faux pour un corps infini.
4. *Avec :*

$$\forall (\lambda, \mu) \in \mathbb{K}^2,\ \varphi(T_{\lambda+\mu}) = \varphi(T_\lambda T_\mu) = \varphi(T_\lambda)\varphi(T_\mu),$$

   on déduit que l'application $\psi : \lambda \mapsto \varphi(T_\lambda)$ *réalise un morphisme de groupes de* $(\mathbb{K}, +)$ *dans* $(\mathbb{K}^*, \cdot)$ *et nécessairement* $\varphi(T_\lambda) = 1$ *pour toute matrice de transvection* T_λ.
5. *Sachant que toute matrice* $A \in GL_n(\mathbb{K})$ *s'écrit* $A = T_1 \cdots T_\alpha D_{\det(A)} T_{\alpha+1} \cdots T_\beta$, *où les* T_k *sont des matrices de transvection, on déduit de ce qui précède que* $\varphi(A) = (\det(A))^r$.