Deuxième composition de mathématiques
X 2001 – MP

On se propose d'établir quelques propriétés des sous-groupes discrets des espaces euclidiens. Dans tout le problème, on désigne par n un entier strictement positif, par E l'espace $\mathbf{R}^n$, par $\langle \cdot \,|\, \cdot \rangle$ son produit scalaire usuel et par $\|\cdot\|$ la norme correspondante. On rappelle les faits suivants :

a) un sous-ensemble L de E est dit discret si tout élément x de L est isolé, *i.e.* admet un voisinage V dans E tel que $L \cap V = \{x\}$;

b) un groupe abélien G est isomorphe à un groupe $\mathbf{Z}^m$ si et seulement s'il admet une $\mathbf{Z}$-*base*, c'est-à-dire une famille $(e_1, \ldots, e_m)$ telle que tout élément g de G s'écrive d'une façon unique sous la forme $g = \sum_{i=1}^{m} k_i e_i$ avec $k_i \in \mathbf{Z}$.

Partie I

1. Démontrer les assertions suivantes :
   a) Un sous-groupe L de E est discret si et seulement si l'élément 0 est isolé.
   b) Tout sous-groupe discret L de E est fermé dans E.
   c) Les sous-groupes discrets de $\mathbf{R}$ sont exactement les sous-ensembles de la forme $a\mathbf{Z}$ avec $a \in \mathbf{R}_+$.
2. Soit α dans $\mathbf{R}_+^*$ et L le sous-groupe de $\mathbf{R}$, ensemble des réels de la forme $m + n\alpha$ avec n et m dans $\mathbf{Z}$. Montrer que L est discret si et seulement si α est rationnel.
3. Construire un sous-groupe discret L de $\mathbf{R}^2$ tel que sa première projection sur $\mathbf{R}$ ne soit pas discrète.
4. Soit L un sous-groupe discret de E non réduit à $\{0\}$. On se propose ici de démontrer que L est isomorphe à un sous-groupe d'un groupe de la forme $\mathbf{Z}^m$. On désigne par F le sous-espace vectoriel de E engendré par L, par m sa dimension, par $(a_1, \ldots, a_m)$ une base de F contenue dans L, et par L' le sous-groupe de L engendré par cette base. Enfin on pose
$$P = L \cap \left\{ \sum_{i=1}^{m} \lambda_i a_i \;\middle|\; \forall i \in [\![1; m]\!] \;\; 0 \leq \lambda_i < 1 \right\} .$$
   a) Vérifier que P est un ensemble fini.
   b) Étant donné un élément x de L, construire un couple (y, z) dans $L' \times P$ tel que l'on ait $x = y + z$, et démontrer son unicité.
   c) Soit encore x un élément de L ; en écrivant $kx = y_k + z_k$ (pour k dans $\mathbf{N}^*$), démontrer qu'il existe un entier d dans $\mathbf{N}^*$ tel que l'on ait $dx \in L'$.
   d) Conclure.
5. Dans cette question, L est un sous-groupe de $\mathbf{Z}^m$ avec $m \geq 2$; ses éléments seront notés $x = (x_1, \ldots, x_m)$; on posera $\pi(x) = x_m$.
   a) Démontrer qu'il existe un entier naturel k et un élément x^0 de L tels qu'on ait
$$\pi(L) = k\mathbf{Z} = \pi(x^0)\mathbf{Z}.$$
   b) On suppose ici $\pi(L)$ non réduit à $\{0\}$; étant donné un élément x de L, construire un couple $(p, \tilde{x})$ dans $\mathbf{Z} \times L$ tel que l'on ait $\tilde{x}_m = 0$ et $x = px^0 + \tilde{x}$; démontrer son unicité.

c) En déduire que tout sous-groupe discret de E est isomorphe à un groupe de la forme $\mathbf{Z}^r$.

6. On suppose ici $n = 2$ et on considère deux $\mathbf{Z}$-bases (u_1, u_2), (v_1, v_2) d'un même sous-groupe discret L de E. Comparer les aires des parallélogrammes construits respectivement sur (u_1, u_2) et (v_1, v_2).

Partie II

7. Dans cette question, on désigne par B la base canonique de E et par $\mathrm{GL}(E)$ le groupe des automorphismes linéaires de E. Pour toute partie X de E, on note $L(X)$ le sous-groupe de E engendré par X.

   Soit G un sous-groupe fini de $\mathrm{GL}(E)$ tel que les matrices des éléments de G dans la base B soient à coefficients rationnels. On note GB l'ensemble des vecteurs $g(x)$ où $g \in G$ et $x \in B$.

   a) Démontrer qu'il existe d dans $\mathbf{N}^*$ tel que l'on ait $dL(GB) \subset L(B)$.

   b) Démontrer l'existence d'une base de E dans laquelle les matrices des éléments de G sont à coefficients entiers.

8. Soit A une matrice à n lignes et n colonnes, à coefficients rationnels, d'ordre fini r (c'est-à-dire que $A^r = I_n$ et que r est le plus petit entier strictement positif ayant cette propriété).

   a) Démontrer que le polynôme caractéristique de A est à coefficients entiers.

   b) On suppose ici $n = 2$. Démontrer que r ne peut prendre que les valeurs $1, 2, 3, 4, 6$ et donner, pour chacune de ces valeurs, un exemple de matrice d'ordre r à coefficients entiers.

Partie III

On désigne par $\mathscr{O}(E)$ le groupe des automorphismes linéaires orthogonaux de E :

$$\mathscr{O}(E) = \{u \in \mathrm{GL}(E) \,|\, \forall x \in \ \|u(x)\| = \|x\|\}$$

et par $AO(E)$ l'ensemble des applications de E dans lui-même de la forme $x \mapsto u(x) + a$ avec $u \in \mathscr{O}(E)$ et $a \in E$; on écrit alors $g = (u, a)$. On note e l'élément neutre de $\mathscr{O}(E)$.

9. On munit $\mathscr{L}(E)$ de la norme donnée par $\|u\| = \sup_{x \in E, \|x\|=1} \|u(x)\|$. Démontrer que $\mathscr{O}(E)$ est compact.

10. a) Vérifier que $AO(E)$ est un groupe, écrire sa loi de groupe, préciser son élément neutre, puis l'inverse d'un élément (u, a).

    b) Calculer $(u, a)(e, b)(u, a)^{-1}$.

11. On note ρ le morphisme de $AO(E)$ dans $\mathscr{O}(E)$ défini par $\rho(u, a) = u$. On fixe un sous-groupe discret L de E qui engendre linéairement E et on note G le sous-groupe de $AO(E)$ formé des éléments g tels que $g(L) = L$.

    a) Vérifier que, si un élément (u, a) de $AO(E)$ appartient à G, il en est de même de $(u, 0)$ et (e, a).

    b) Démontrer que $\rho(G)$ est fini.

    c) Déterminer G dans le cas où $n = 2$ et où L est l'ensemble des couples (x_1, x_2) tels que $x_1 \in 2\mathbf{Z}$, $x_2 \in \mathbf{Z}$.

Deuxième composition de mathématiques – X 2001 – MP

Partie I

1. a) Soit L un sous-groupe de E. Si L est discret alors 0 appartient à L et est donc isolé. Si 0 est isolé, on dispose d'un voisinage V de 0 tel que $V \cap L = \{0\}$. Pour x dans L, $V + x$ est un voisinage de x et, puisque L est invariant par translation par x, $(V + x) \cap L = (V + x) \cap (L + x) = (V \cap L) + x = \{0\} + \{x\} = \{x\}$, donc x est isolé. Par conséquent $\boxed{L \text{ est discret si et seulement si l'élément 0 est isolé.}}$

   b) Soit L un sous-groupe discret de E et (x_k) une suite d'éléments de L convergeant dans E. On note x sa limite. Alors $(x_{k+1} - x_k)$ est une suite d'éléments de L convergeant vers 0, donc puisque 0 est isolé, elle est nulle à partir d'un certain rang, i.e. (x_k) est stationnaire. Sa limite est donc un terme de la suite. On en conclut que $\boxed{L \text{ est fermé dans } E.}$

   c) Soit a dans $\mathbf{R}_+$. On note $V_a =]-a; a[$ si $a > 0$ et $V = \mathbf{R}$ sinon. L'ensemble $a\mathbf{Z}$ est un sous-groupe de $\mathbf{R}$ et, d'après la question 1a, puisque V_a est voisinage de 0 vérifiant $V_a \cap a\mathbf{Z} = \{0\}$, $a\mathbf{Z}$ est discret.

   Réciproquement, soit L un sous-groupe discret de $\mathbf{R}$. D'après la question précédente L est fermé. Si $L = \{0\}$ alors $L = 0\mathbf{Z}$; sinon on dispose de r dans $\mathbf{R}_+^*$ tel que $]-r; r[\cap L = \{0\}$ et de x non nul dans L. Alors $-x$ et donc aussi $|x|$ appartiennent à L, et donc $L \cap \mathbf{R}_+^*$ est une partie non vide, minorée de $\mathbf{R}$, égale à $L \cap [r; +\infty[$. C'est donc une partie fermée, en tant qu'intersection de fermés. Sa borne inférieure est donc un minimum. On peut donc poser $a = \min L \cap \mathbf{R}_+^*$ et on en déduit $a\mathbf{Z} \subset L$. Par division euclidienne, pour x dans L, on dispose de y dans $a\mathbf{Z}$ tel que $0 \leq x - y < a$ et comme $x - y \in L$, il vient $x - y = 0$, i.e. $x \in a\mathbf{Z}$. Donc $\boxed{\text{les sous-groupes discrets de } \mathbf{R} \text{ sont exactement les sous-ensembles de la forme } a\mathbf{Z}.}$

2. Remarquons que L est le sous-groupe de $\mathbf{R}$ engendré par 1 et α, et est donc bien un sous-groupe de $\mathbf{R}$. Si L est discret, on dispose de a dans $\mathbf{R}_+$ tel que $L = a\mathbf{Z}$ et donc aussi de p et q dans $\mathbf{Z}$ tels que $1 = qa$ et $\alpha = pa$. Il en résulte $q \neq 0$ et $\alpha = p/q$, donc α est rationnel. Réciproquement, si α est rationnel, on dispose de p et q dans $\mathbf{Z}$ tels que $\alpha = p/q$, de sorte que L est inclus dans $\frac{1}{q}\mathbf{Z}$. Comme ce dernier est discret, L l'est aussi. Par conséquent $\boxed{L \text{ est discret si et seulement si } \alpha \text{ est rationnel.}}$

3. Soit α un nombre irrationnel, par exemple $\alpha = \sqrt{2}$ et L le sous-groupe de $\mathbf{R}^2$ engendré par $(1, 1)$ et $(\alpha, 0)$, i.e. l'ensemble des couples de la forme $(m + n\alpha, m)$ avec m et n dans $\mathbf{Z}$. Soit $\varepsilon = \min(1, |\alpha|)$ et (x, y) dans L tel que $0 \leq |x|, |y| < \varepsilon$. Puisque y est un entier il vient $y = 0$ et on dispose de m dans $\mathbf{Z}$ tel que $x = m\alpha$ et donc $x = 0$. Comme $]-\varepsilon; \varepsilon[^2$ est ouvert comme produit d'ouverts, c'est un voisinage de $(0, 0)$ dans $\mathbf{R}^2$ et on en conclut que L est discret d'après la question 1a. Sa première projection n'est pas discrète d'après la question précédente et donc $\boxed{\left\{(m + n\sqrt{2}, m) \;\middle|\; (m, n) \in \mathbf{Z}^2\right\} \text{ est discret mais sa première projection ne l'est pas.}}$

4. a) Par inégalité triangulaire, P est borné. S'il était infini, on disposerait d'une suite injective à valeurs dans P et donc aussi, puisque E est de dimension finie et d'après le théorème de Bolzano-Weierstrass, d'une suite injective convergente à valeurs dans P. Les accroissements d'une telle suite tendent alors vers 0, sont à valeurs dans L, puisque L est un groupe, et sont non nuls, par injectivité de la suite. Ainsi 0 ne serait pas isolé dans L. Il résulte donc de la question 1a que $\boxed{P \text{ est fini.}}$

b) Comme x est dans L donc dans F, on dispose de scalaires (λ_i) tels que $x = \sum_{i=1}^{m} \lambda_i a_i$. Le couple (y, z) donné par

$$y = \sum_{i=1}^{m} [\,\lambda_i\,] a_i \quad \text{et} \quad z = \sum_{i=1}^{m} (\lambda_i - [\,\lambda_i\,]) a_i$$

convient. Soit (y', z') dans $L' \times P$, alors $y - y'$ est dans L' et $z' - z$ dans $P - P$, i.e. $z' - z$ est combinaison linéaire des (a_i) avec des coefficients dans $]-1; 1[$. Par indépendance linéaire des (a_i) on en déduit que $y - y'$ et $z' - z$ sont donnés par les mêmes combinaisons linéaires, i.e. avec des coefficients dans $\mathbf{Z}$ et dans $]-1; 1[$. C'est donc la combinaison linéaire nulle, i.e. $y - y' = z' - z = 0$: un tel couple (y, z) existe et est unique.

c) D'après la question précédente et puisque L est un groupe, on dispose de deux suites (y_k) et (z_k) à valeurs dans L' et P respectivement telles que, pour k dans $\mathbf{N}^*$, on ait $kx \in L$ et $kx = y_k + z_k$. Comme P est fini, la suite (z_k) n'est pas injective. On dispose de k et ℓ deux entiers naturels tels que $0 < k < \ell$ et $z_k = z_\ell$. Il vient en posant $d = \ell - k$, $dx = x_\ell - x_k = y_\ell - y_k$ et donc, puisque L' est un groupe, $dx \in L'$.

d) Puisque P est fini et que, d'après la question précédente on dispose pour tout x dans P d'un entier d dans $\mathbf{N}^*$ tel que $dx \in L'$, quitte à prendre le ppcm de tous ces entiers, on peut supposer que cet entier est le même pour tous les éléments de P. On note μ_d l'homothétie de rapport d. On a donc $\mu_d(P) \subset L'$. Comme L' est un groupe, on a aussi $\mu_d(L') \subset L'$ et donc, puisque $L \subset L' + P$ d'après la question 4b, on a, par linéarité de μ_d et puisque L' est un groupe, $\mu_d(L) \subset L' + L' = L'$. Puisque L est un groupe, il en va de même pour $\mu_d(L)$ car une application linéaire est en particulier un morphisme de groupes. Par définition de L' et indépendance des (a_i), L' est isomorphe à $\mathbf{Z}^m$ par l'application φ qui à un élément de F associe ses coordonnées dans la base (a_i). Il en résulte que $\varphi \circ \mu_d$ est un morphisme de groupes injectif de L dans $\mathbf{Z}^d$. En notant H l'image de L par cette application, H est alors un sous-groupe de $\mathbf{Z}^m$ et $\varphi \circ \mu_d$ induit un isomorphisme entre L et H, i.e. L est isomorphe à un sous-groupe de $\mathbf{Z}^m$.

5. a) Puisque π est linéaire, c'est un morphisme de groupes. Donc son image est un sous-groupe de $\mathbf{Z}$. C'est donc un sous-groupe discret de $\mathbf{R}$ et il est de la forme $a\mathbf{Z}$ avec $a \in \mathbf{R}_+$ d'après la question 1c et comme il contient a et est inclus dans $\mathbf{Z}$, on a $a \in \mathbf{N}$. On choisit x^0 un antécédent de a par π et on note $k = a$, ainsi $k \in \mathbf{N}^*$, $x^0 \in L$, $\pi(L) = k\mathbf{Z} = \pi(x^0)\mathbf{Z}$.

b) On a $\pi(x) \in \pi(L) = \pi(x^0)\mathbf{Z}$. On dispose donc de p dans $\mathbf{Z}$ tel que $\pi(x) = p\pi(x^0)$ et donc, par linéarité de π, $\pi(x - px^0) = 0$. En posant $\tilde{x} = x - px^0$, on a $\tilde{x} \in L$ car L est un groupe et x et x^0 en sont des éléments. Par conséquent $\tilde{x} \in L$ et $\tilde{x}_m = 0$, et $x = px^0 + \tilde{x}$. Soit (q, y) dans $\mathbf{Z} \times L$ avec $\pi(y) = 0$ et $x = qx^0 + y$. On a alors $(p - q)x^0 = y - \tilde{x} \in \mathrm{Ker}(\pi)$ et donc, puisque $\pi(L)$, et donc aussi $\pi(x^0)$, n'est pas nul, $p - q = 0$. Il en résulte $y = \tilde{x}$ et ainsi il existe un unique couple $(p, \tilde{x})$ dans $\mathbf{Z} \times L$ avec $\tilde{x}_m = 0$ et $x = px^0 + \tilde{x}$.

c) Remarquons, avec les notations de la question précédente et en notant ρ la projection sur les $m - 1$ premières coordonnées, que $L \cap \mathrm{Ker}(\pi)$ et $\rho(L \cap \mathrm{Ker}(\pi))$ sont des groupes, le premier comme intersection de deux groupes, le second comme image d'un groupe par un

morphisme. D'après la question précédente L est en bijection avec $\mathbf{Z} \times \rho(L \cap \mathrm{Ker}(\pi))$ par l'application $x \mapsto (p, \rho(\tilde{x}))$, de réciproque donnée par $(q, y) \mapsto px_0 + (y, 0)$. Comme ces deux applications sont des morphismes de groupes, on en déduit que L est isomorphe à $\mathbf{Z} \times \rho(L \cap \mathrm{Ker}(\pi))$. Si au contraire $\pi(L) = \{0\}$, alors L est isomorphe à $\rho(L)$. Autrement dit L est isomorphe à $\mathbf{Z} \times L'$ ou à L' avec L' un sous-groupe de $\mathbf{Z}^{m-1}$.

Soit, pour d dans $\mathbf{N}$, le prédicat $(\mathbf{H}_d)$ donné par : tout sous-groupe de $\mathbf{Z}^d$ est isomorphe à un groupe de la forme $\mathbf{Z}^r$ avec $r \leq d$. Comme $\mathbf{Z}^0 = \{0\}$ et que $\{0\}$ n'a que des sous-groupes triviaux, $(\mathbf{H}_0)$ est vrai. On a déjà remarqué que les sous-groupes de $\mathbf{Z}$ sont des sous-groupes discrets de $\mathbf{R}$ de la forme $a\mathbf{Z}$ avec $a \in \mathbf{Z}$ et sont donc isomorphes soit à $\mathbf{Z}^0$ si $a = 0$, soit à $\mathbf{Z}$ sinon. Soit maintenant d un entier avec $d \geq 2$ et L un sous-groupe de $\mathbf{Z}^d$. D'après ce qui précède L est isomorphe à $\mathbf{Z}^s \times L'$ avec $s \in \{0; 1\}$ et L' un sous-groupe de $\mathbf{Z}^{d-1}$. Il en résulte $(\mathbf{H}_{d-1}) \Longrightarrow (\mathbf{H}_d)$ et donc, par principe de récurrence, tout sous-groupe d'un groupe de la forme $\mathbf{Z}^d$ est aussi de cette forme.

Soit maintenant L' un sous-groupe discret de E. Si $L' = \{0\}$, alors L est isomorphe à $\mathbf{Z}^0$. Sinon, d'après la question 4, L' est isomorphe à un sous-groupe d'un certain $\mathbf{Z}^m$ et est donc également de la forme $\mathbf{Z}^r$, avec $r \leq m \leq n$. En résumé

tout sous-groupe discret de E est de la forme $\mathbf{Z}^r$ avec $r \leq n$.

6. Soit P la matrice de passage de (u_1, u_2) à (v_1, v_2). Puisque (u_1, u_2) est une $\mathbf{Z}$-base de L, les coordonnées de (v_1, v_2) dans cette base sont entières et donc P est à coefficients entiers. Il en va donc de même pour son déterminant. Comme P^{-1} est la matrice de passage de (v_1, v_2) à (u_1, u_2), elle est aussi à coefficients et donc à déterminant entiers. Comme $\det(P^{-1})$ est aussi l'inverse de $\det(P)$, ce dernier est un entier d'inverse entier, i.e. $|\det(P)| = 1$. Si A et B sont les matrices de (u_1, u_2) et (v_1, v_2) respectivement relativement à la base canonique, on a donc $|\det(A)| = |\det(B)|$, i.e. les aires de ces deux parallélogrammes sont égales.

Partie II

7. a) Soit g dans G. On dispose de d dans $\mathbf{N}^*$ tel que la matrice de dg relativement à la base B soit à coordonnées entières et donc, pour x dans B, $d(g(x)) \in L(B)$. Par finitude de G et puisque $L(B)$ est un groupe et est ainsi stable par multiplication par un entier, quitte à prendre un ppcm, on peut supposer $dg(x) \in L(B)$ pour tout (g, x) dans $G \times B$. Comme $L(B)$ est un groupe et donc stable par combinaisons linéaires à coefficients entiers, il en va de même pour toute telle combinaison d'éléments de la forme $g(x)$ avec $g \in G$ et $x \in B$, i.e. $dL(GB) \subset L(B)$.

b) Puisque G est un groupe, donc stable par composition, tout élément de G stabilise GB, et en fait le laisse invariant car tous les éléments de G sont inversibles. Puisque ce sont aussi des applications linéaires, ils laissent donc stable $L(GB)$. Par définition $L(B)$ admet B comme $\mathbf{Z}$-base, donc est isomorphe à $\mathbf{Z}^n$. L'homothétie de rapport d induit un isomorphisme de groupe entre $L(GB)$ et son image, et cette dernière est donc un sous-groupe d'un groupe isomorphe à $\mathbf{Z}^n$. Il résulte de la question 5c et de sa démonstration que $L(GB)$ est isomorphe à $\mathbf{Z}^r$ avec $r \leq n$. On dispose alors de B' une $\mathbf{Z}$-base de $L(GB)$. Le sous-espace vectoriel engendré par GB admet B' comme base, et il contient B car G contient e, de sorte que B' est une base de E. Alors pour g dans G et b dans B' on a

$g(b) \in L(GB)$ donc $g(b)$ est une combinaison linéaire à coefficients entiers des éléments de B', i.e. $\boxed{\text{la matrice de } g \text{ dans } B' \text{ est à coefficients entiers.}}$

8. a) Soit u l'endomorphisme de E canoniquement associé à A et G le sous-groupe multiplicatif de $\mathrm{GL}(E)$ monogène engendré par u, i.e. $G = \left\{u^k \;\middle|\; 0 \leq k < r\right\}$. C'est un groupe fini et, puisque $\mathbf{Q}$ est un corps, les matrices dans la base canonique des éléments de G sont à coefficients rationnels. D'après la question 7, on dispose alors d'une base B' de E dans laquelle les matrices des éléments de G sont à coefficients entiers. En particulier A est semblable à une matrice à coefficients entiers. Comme le déterminant, et donc aussi le polynôme caractéristique, est invariant par changement de base, $\boxed{\chi_A \text{ est à coefficients entiers.}}$

b) On factorise χ_A sur $\mathbf{C}$ sous la forme $\chi_A = (X-\lambda)(X-\mu)$. Si λ et μ sont distincts, et puisque A est dans $\mathscr{M}_2(\mathbf{C})$, on dispose de U et V non nuls dans $\mathscr{M}_{2,1}(\mathbf{C})$ tel que $AU = \lambda U$ et $AV = \mu V$ respectivement, i.e. de vecteurs propres pour A associés à λ et μ. De tels vecteurs propres étant indépendants, on en déduit que A est semblable à la matrice diagonale $\mathrm{diag}(\lambda, \mu)$ via la matrice de passage de la base canonique à la base (U, V), i.e. $A = P^{-1}\mathrm{diag}(\lambda, \mu)P$ avec P inversible. On a alors pour tout k dans $\mathbf{N}^*$, $A^k = P^{-1}\mathrm{diag}(\lambda^k, \mu^k)P$ et donc $A^k = I_2 \iff \lambda^k = \mu^k = 1$. Comme A est à coefficients réels, χ_A l'est aussi et donc soit λ et μ sont réels tous les deux, et $\lambda = -\mu = \pm 1$, soit ils sont complexes conjugués. Dans ce dernier cas on peut écrire $\lambda = e^{i\theta}$ et il vient $\chi_A = X^2 - 2\cos(\theta)X + 1$ et donc, puisque χ_A est à coefficients entiers et que cos est à valeurs dans $[\,-1; 1\,]$, $\cos(\theta) \in \left\{0; \pm\frac{1}{2}; \pm 1\right\}$. Dans le premier cas on a $r = 2$, dans le second on peut choisir $\lambda \in \{-j; i; j\}$ et $r \in \{6; 4; 3\}$. Si maintenant $\chi_A = (X-\lambda)^2$, comme χ_A est à coefficients entiers, λ est réel. Et on dispose encore d'un vecteur propre associé U à λ. On complète U en une base (U, V), de sorte que A est semblable à une matrice triangulaire T : $T = \begin{pmatrix} \lambda & x \\ 0 & \mu \end{pmatrix}$. Par invariance du polynôme caractéristique par changement de base, il vient $\mu = \lambda$ et on montre par récurrence qu'on a $T^r = \begin{pmatrix} \lambda^r & r\lambda^{r-1}x \\ 0 & \lambda^r \end{pmatrix}$. Comme T^r est semblable donc égal à I_2, il vient $x = 0$ et $\lambda = \pm 1$, donc $r \in \{1; 2\}$. On en déduit $\boxed{r \in \{1; 2; 3; 4; 6\}.}$

Exemples. On remarque dans le cas où χ_A est simplement scindé, A est semblable à une matrice diagonale et l'ordre de A est donné par celui des racines de χ_A. De plus si $A = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$, alors $\chi_A = X^2 + aX + b$. On en déduit les exemples suivants,

$\boxed{\begin{array}{l} r = 1 \text{ et } A = I_2,\ r = 2 \text{ et } A = -I_2,\ r = 3 \text{ et } A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ r = 4 \text{ et } A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \\ r = 6 \text{ et } A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}. \end{array}}$

Partie III

9. L'espace $\mathscr{L}(E)$ est un espace vectoriel normé de dimension finie. Toutes les normes y sont équivalentes et on dispose du théorème de Heine-Borel. Par définition de la norme sur $\mathscr{L}(E)$, $\mathscr{O}(E)$ est inclus dans la sphère unité fermée, qui est compacte. Sa compacité équivaut donc à son caractère fermé. Or si (u_n) est une suite convergente d'éléments de $\mathscr{O}(E)$, convergeant vers u dans $\mathscr{L}(E)$, par continuité de l'évaluation en un vecteur, pour tout x dans E, on a $u(x) = \lim u_n(x)$ et en particulier, par continuité de la norme, $\|u(x)\| = \lim \|u_n(x)\| = \|x\|$. Donc $u \in \mathscr{O}(E)$ et $\mathscr{O}(E)$ est fermé, donc $\boxed{\mathscr{O}(E) \text{ est compact.}}$

10. a) Puisque les isométries sont bijectives tout comme les translations, $AO(E)$ est inclus dans le groupe des bijections de E dans E. On a $\mathrm{Id}_E = (e, 0)$ et donc $AO(E)$ contient l'élément neutre de S_E. De plus pour u et v dans $\mathscr{O}(E)$ et a et b dans E, on a $(u, a) \circ (v, b) = (u \circ v, a + u(b))$, de sorte que $AO(E)$ est stable par composition et (u, a) admet $(u^{-1}, -u^{-1}(a))$ comme inverse. Il en résulte que

$\boxed{AO(E) \text{ est un groupe, d'élément neutre } (e, 0), \text{ de loi donnée par } (u, a) \circ (v, b) = (u \circ v, a + u(b)) \text{ et de symétrique donné par } (u, a)^{-1} = (u^{-1}, -u^{-1}(a)).}$

b) Les formules précédentes donnent directement $\boxed{(u, a)(e, b)(u, a)^{-1} = (e, u(b)).}$

11. a) On vérifie que G est un sous-groupe de $AO(E)$ puisqu'il contient Id_E et que, pour g et h dans G, on a $g(h(L)) = g(L) = L$ et $L = g^{-1}(g(L)) = g^{-1}(L)$, i.e. $gh \in G$ et $g^{-1} \in G$. Soit g dans G avec $g = (u, a) \in AO(E)$. En particulier $a = g(0) \in L$ et donc, puisque L est un groupe, $(e, a) \in G$. Il en va donc de même de $(e, a)^{-1} \circ (u, a)$, i.e. de $(u, 0)$: $\boxed{(e, a) \in G \text{ et } (u, 0) \in G.}$

b) Soit $(e_1, \ldots, e_n)$ une $\mathbf{Z}$-base de L et g dans G. D'après ce qui précède $\rho(g) \in G$. On note $u = \rho(g)$ et K une boule fermée centrée en 0 contenant $(e_1, \ldots, e_n)$. Par théorème de Heine-Borel, K est compact. Si $K \cap L$ était infini, on disposerait d'une suite injective à valeurs dans $K \cap L$. Par compacité on peut la supposer convergente dans K et donc ses accroissements forment une suite à valeurs dans L, tendant vers 0, mais ne prenant pas la valeur 0. C'est incompatible avec le caractère discret de L, donc $K \cap L$ est fini. Or, pour tout i dans $[\![1; n]\!]$, $u(e_i)$ est de même norme que e_i, donc appartient à K et par suite, puisque u appartient à $\rho(G)$, $u(e_i) \in K \cap L$. Ainsi les familles $(u(e_i))_{1 \leq i \leq n}$ pour u dans $\rho(G)$ sont en nombre fini. Or l'application $u \mapsto (u(e_i))_{1 \leq i \leq n}$ est injective, par linéarité de u, donc $\boxed{\rho(G) \text{ est fini.}}$

c) En reprenant les notations de la question précédente on peut poser $e_1 = (2, 0)$ et $e_2 = (0, 1)$, de sorte que (e_1, e_2) est une $\mathbf{Z}$-base de L. Pour u dans $\rho(G)$, on a donc $\|\rho(e_1)\| = 2$ et $\|\rho(e_2)\| = 1$. Or pour (a, b) dans L, on a $\|(a, b)\|^2 = a^2 + b^2$ avec $4 \mid a^2$. On en déduit $u(e_2) = \pm e_2$ et $u(e_1) \in \{\pm e_1, \pm 2e_2\}$. Comme u est orthogonale, on a nécessairement $u(e_1) = \pm e_1$, de sorte que u est soit $\pm\mathrm{Id}_E$, soit une symétrie par rapport à $\mathbf{R}e_1$ ou $\mathbf{R}e_2$. Réciproquement ces quatre applications sont orthogonales et préservent L. Comme les translations de vecteurs dans L sont aussi dans G, leurs composées avec les quatre endomorphismes précédents sont dans G. Ainsi $\boxed{G = \left\{(x_1, x_2) \mapsto (\varepsilon_1 x_1 + 2a_1, \varepsilon_2 x_2 + a_2) \;\middle|\; (\varepsilon_1, \varepsilon_2) \in \{\pm 1\}^2, (a_1, a_2) \in \mathbf{Z}^2\right\}.}$