ÉCOLE POLYTECHNIQUE **FILIÈRE** MP

CONCOURS D'ADMISSION 2001

DEUXIÈME COMPOSITION DE MATHÉMATIQUES

Corrigé de M. Quercia (michel.quercia@prepas.org)

Première partie

1a. Si L est discret alors $0 \in L$ est isolé. Si 0 est isolé, soit V un voisinage de 0 tel que $V \cap L = \{0\}$ et $x \in L$: alors $V + x$ est un voisinage de x et $(V + x) \cap L = (V + x) \cap (L + x) = (V \cap L) + x = \{x\}$ donc x est isolé.

1b. Soit L un sous-groupe discret et (x_k) une suite d'éléments de L convergeant vers $x \in E$. Alors $(x_{k+1} - x_k)$ est une suite d'éléments de L convergeant vers 0, donc puisque 0 est isolé on a $x_{k+1} - x_k = 0$ à partir d'un certain rang, soit $k \geqslant K$, et la suite $(x_k)_{k \geqslant K}$ est constante donc $x = x_K \in L$.

1c. $a\mathbb{Z}$ est bien un sous-groupe de $\mathbb{R}$ et il est discret car 0 est isolé : $]-a, a[\cap a\mathbb{Z} = \{0\}$ si $a > 0$ et $]-1, 1[\cap 0\mathbb{Z} = \{0\}$.

Réciproquement, soit L un sous-groupe discret de $\mathbb{R}$. Si $L = \{0\}$ alors $L = 0\mathbb{Z}$; sinon soit $r > 0$ tel que $]-r, r[\cap L = \{0\}$ et $a = \min(L \cap [r, +\infty[)$. a existe car $L \cap [r, +\infty[$ est non vide (sinon $L \subset \mathbb{R}^-$ et $L = -L$ donc $L = \{0\}$), fermé et minoré. On a $a \in L$ par construction donc $a\mathbb{Z} \subset L$ et $a = \min(L \cap \mathbb{R}^{+*})$. Soit alors $x \in L$: il existe $q \in \mathbb{Z}$ unique tel que $qa \leqslant x < (q+1)a$ d'où $y = x - qa \in L$ et $0 \leqslant y < a$ ce qui implique $y = 0$ par définition de a d'où $x = qa \in a\mathbb{Z}$. Ceci prouve que $L = a\mathbb{Z}$.

2. L est bien un sous-groupe de $\mathbb{R}$, c'est le sous-groupe engendré par 1 et α. Supposons L discret, soit $L = a\mathbb{Z}$ pour un certain $a \in [0, +\infty[$. Alors il existe $p, q \in \mathbb{Z}$ tels que $1 = qa$ et $\alpha = pa$ d'où $q \neq 0$ et $\alpha = p/q$ est rationnel.

Réciproquement, si α est rationnel, $\alpha = p/q$ avec $p, q \in \mathbb{Z}$, alors $L \subset (1/q)\mathbb{Z}$ qui est discret donc L est lui aussi discret.

3. On prend $L = \{(m + n\pi, m),\ m, n \in \mathbb{Z}\}$, le groupe engendré par $(1, 1)$ et $(\pi, 0)$. La première projection de L est $L_1 = \{m + n\pi,\ m, n \in \mathbb{Z}\}$ non discret car π est irrationnel. Par contre L est discret car $(0, 0)$ est isolé : $L \cap]-1, 1[^2 = \{(0, 0)\}$.

4a. Supposons P infini : il existe alors une suite (x_k) d'éléments de P deux à deux distincts, et P est borné donc cette suite admet une sous-suite $(x_{\varphi(k)})$ convergente dans E.
On a alors $x_{\varphi(k+1)} - x_{\varphi(k)} \in L \setminus \{0\}$ et $x_{\varphi(k+1)} - x_{\varphi(k)} \xrightarrow[k \to \infty]{} 0$ ce qui contredit le fait que 0 est isolé.

4b. Comme $x \in L \subset F$, x admet une décomposition : $x = \sum_{i=1}^{m} \lambda_i a_i$ avec $\lambda_i \in \mathbb{R}$. Alors $(y, z) = (\sum_{i=1}^{m} \lfloor \lambda_i \rfloor a_i, \sum_{i=1}^{m} \{\lambda_i\} a_i)$ convient.

Soit (y', z') un autre couple de $L' \times P$ tel que $x = y' + z'$, et $y' = \sum_{i=1}^{m} \mu_i a_i$, $z' = \sum_{i=1}^{m} \nu_i a_i$ avec $\mu_i \in \mathbb{Z}$ et $\nu_i \in [0, 1[$.
On a $x = \sum_{i=1}^{m} \lambda_i a_i = y' + z' = \sum_{i=1}^{m} (\mu_i + \nu_i) a_i$ soit $\mu_i + \nu_i = \lambda_i$ par indépendance linéaire des a_i ce qui implique $\mu_i = \lfloor \lambda_i \rfloor$ et $\nu_i = \{\lambda_i\}$ puisque $\mu_i \in \mathbb{Z}$ et $0 \leqslant \nu_i < 1$, d'où $y' = y$ et $z' = z$.

4c. La suite (z_k) est à valeurs dans P fini, donc il existe $k < k'$ tels que $z_k = z_{k'}$ soit $(k' - k)x = y_{k'} - y_k \in L'$.

4d. On note $P = \{x_1, \ldots, x_p\}$, $d_i \in \mathbb{N}^*$ tel que $d_i x_i \in L'$ et $d = \text{ppcm}(d_1, \ldots, d_p)$. Alors pour tout $x \in P$ on a $dx \in L'$ d'où $P \subset (1/d)L'$ et $L = L' + P \subset (1/d)L'$. Soit alors :

$$\varphi : \begin{cases} \mathbb{Z}^m & \longrightarrow & (1/d)L' \\ (\lambda_1, \ldots, \lambda_m) & \longmapsto & (\lambda_1 a_1 + \ldots + \lambda_m a_m)/d. \end{cases}$$

φ est un morphisme de groupes, injectif car les a_i sont linéairement indépendants, et surjectif par définition de L'. L'image réciproque, $\varphi^{-1}(L)$, est un sous groupe de $\mathbb{Z}^m$ isomorphe à L.

5a. Remarquons déjà que π est un morphisme de groupes. $\pi(L)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $k\mathbb{Z}$ avec $k \in \mathbb{N}$. On choisit $x^0 \in L$ tel que $\pi(x^0) = k$.

5b. $\pi(x) \in \pi(x^0)L$ donc il existe $p \in \mathbb{Z}$ tel que $\pi(x) = p\pi(x^0)$. Alors $x = px^0 + (x - px^0) = px^0 + \tilde{x}$ et par construction : $\tilde{x} \in L$, $\tilde{x}_m = \pi(\tilde{x}) = 0$. Unicité de $(p, \tilde{x})$: si $x = qx^0 + y$ avec $q \in \mathbb{Z}$, $y \in L$ et $y_m = 0$ alors $\pi(x) = p\pi(x^0) = q\pi(x^0)$ d'où $q = p$ car $\pi(x^0) \neq 0$, puis $y = x - qx^0 = x - px^0 = \tilde{x}$.

5c. On montre par récurrence sur m que si L est un sous-groupe de $\mathbb{Z}^m$ alors il existe $r \in \mathbb{N}$ tel que L est isomorphe à $\mathbb{Z}^r$. Ceci suffira à conclure puisque tout sous-groupe discret de E est isomorphe à un sous-groupe d'un groupe $\mathbb{Z}^m$.

Pour $m = 0$ l'énoncé est trivial, et pour $m = 1$ c'est un fait connu (les sous-groupes de $\mathbb{Z}$ sont monogènes). Supposons $m \geqslant 2$ et soit L un sous groupe de $\mathbb{Z}^m$. Si $\pi(L) = \{0\}$ alors $L \subset \mathbb{Z}^{m-1} \times \{0\}$ donc l'application $(x_1, \ldots, x_m) \longmapsto (x_1, \ldots, x_{m-1})$ induit un isomorphisme de L sur un sous-groupe L' de $\mathbb{Z}^{m-1}$. L' est isomorphe à un groupe $\mathbb{Z}^r$ par hypothèse de récurrence et L est aussi isomorphe à $\mathbb{Z}^r$.
Si $\pi(L) \neq \{0\}$ soit $x^0 \in L$ tel que $\pi(L) = \pi(x^0)\mathbb{Z}$ et $L' = L \cap (\mathbb{Z}^{m-1} \times \{0\})$. L' est un sous-groupe de $\mathbb{Z}^{m-1} \times \{0\}$ donc est isomorphe à un $\mathbb{Z}^r$ et $L = \mathbb{Z}x_0 \oplus L'$ (question précédente) est isomorphe à $\mathbb{Z}^{r+1}$.

6. Soient A, A' ces aires, $\mathcal{B}$ une base orthonormale de E et P la matrice de passage de (u_1, u_2) à (v_1, v_2). On a :

$$A' = |\det_{\mathcal{B}}(v_1, v_2)| = |\det_{\mathcal{B}}(u_1, u_2) \det P| = A|\det P|.$$

Les coefficients de P sont les coordonnées de v_1 et v_2 dans (u_1, u_2), ce sont des entiers donc $\det P \in \mathbb{Z}$. De même, P^{-1}, matrice de passage de (v_1, v_2) à (u_1, u_2), est à coefficietns entiers d'où $\det(P^{-1}) = \frac{1}{\det P} \in \mathbb{Z}$ ce qui entraîne $\det P \in \{-1, 1\}$ et $A = A'$.

Deuxième partie

7a. $L(GB)$ est le groupe engendré par les colonnes des matrices de G et $L(B)$ est l'ensemble des vecteurs à coordonnées entières donc $d = \text{ppcm}\{\text{dénominateurs des coefficients des éléments de } G\}$ convient.

7b. On a $G(GB) = \{g(x),\ g \in G,\ x \in GB\} = \{g \circ h(y),\ g \in G,\ h \in G,\ y \in B\} = GB$ donc $L(GB)$ est stable par toutes les applications $g \in G$. De plus c'est un sous groupe de $(1/d)L(B) = (1/d)\mathbb{Z}^n$ donc il est isomorphe à un $\mathbb{Z}^r$ et $r \leqslant n$ (ceci se démontre par récurrence en reprenant la question **5c**). Soit $(e_1, \ldots, e_r)$ une $\mathbb{Z}$-base de $L(GB)$: le sous-espace vectoriel engendré par GB est le sous-espace engendré par $(e_1, \ldots, e_r)$ donc est de dimension au plus r et $B = \text{id}.B \subset GB$ donc il contient le sous-espace engendré par B c'est-à-dire E. On en déduit $r \geqslant n$ puis $r = n$ et $B' = (e_1, \ldots, e_n)$ est une base de E. Alors pour $g \in G$ on a $g(e_i) \in L(GB)$ donc $g(e_i)$ est une combinaison linéaire à coefficients entiers des e_j ce qui prouve que la matrice de g dans B' est à coefficients entiers.

8a. Soit a l'endomorphisme de E de matrice A dans la base canonique de E et G le sous-groupe de $GL(E)$ engendré par a. $G = \{a^k,\ 0 \leqslant k < r\}$ est fini et les matrices dans B des éléments de G sont à coefficients rationnels donc il existe 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 et son polynôme caractéristique est à coefficients entiers.

8b. A annule le polynôme $X^r - 1$ qui est scindé à racines simples dans $\mathbb{C}$, donc A est $\mathbb{C}$-diagonalisable et ses valeurs propres, λ, μ, sont des racines d'ordre r de 1. Distinguons plusieurs cas :

i) $\lambda = \mu = 1$. Alors $A = I$ et $r = 1$.
ii) $\lambda = -1$, $\mu = \pm 1$. Alors $A \neq I$ et $A^2 = I$, $r = 2$.
iii) $\lambda = e^{i\theta}$, $\mu = e^{-i\theta}$ avec $0 < \theta < \pi$. Alors $\text{tr}(A) = 2\cos\theta$ est un entier compris strictement entre -2 et 2, d'où $\theta \in \{\pi/3, \pi/2, 2\pi/3\}$ et $r \in \{6, 4, 3\}$.

Il n'y a pas d'autre cas car λ et μ sont soit tous deux réels soit tous deux non réels conjugués.

Exemples. $r = 1$: I. $r = 2$: $-I$. $r = 3$: $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. $r = 4$: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. $r = 6$: $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

Troisième partie

9. C'est un fermé borné de $\mathcal{L}(E)$, ev de dimension finie.

10a. $(u, a) \circ (v, b) = (u \circ v, a + u(b))$ donc $AO(E)$ est stable par composition. La loi $\circ$ est associative, $(e, 0)$ est élément neutre et $(u, a) \circ (u^{-1}, -u^{-1}(a)) = (u^{-1}, -u^{-1}(a)) \circ (u, a) = (e, 0)$ donc (u, a) admet pour symétrique $(u, a)^{-1} = (u^{-1}, -u^{-1}(a))$.

10b. $(u, a)(e, b)(u, a)^{-1} = (e, u(b))$.

11a. Si $u(L)+a=L$ alors $a=u(0)+a\in L$ d'où $L+a=L$ et $u(L)=L-a=L$ c'est-à-dire $(e,a)\in G$ et $(u,0)\in G$.

11b. Soit $(e_1,\dots,e_n)$ une $\mathbb{Z}$-base de L et $M=\max(\|e_1\|,\dots,\|e_n\|)$. L'ensemble $K=\{x\in L,\ \|x\|\leqslant M\}$ est fini car L est discret et si $(u,a)\in G$ alors $(u,0)\in G$ donc $u(e_i)\in K$ pour tout i. Ainsi la restriction de u à $(e_1,\dots,e_n)$ ne peut prendre d'un nombre fini de valeurs et cette restriction détermine u par linéarité, donc l'ensemble des u est fini.

11c. L admet $(2e_1,e_2)=((2,0),(0,1))$ pour $\mathbb{Z}$-base, $M=2$ et :

$$K=\{(\pm2,0),(0,\pm2),(0,\pm1),(0,0)\}.$$

Considérons $(u,0)\in G$. On a $u(2e_1)\in\{(\pm2,0),(0,\pm2)\}$ et $u(e_2)\in\{(0,\pm1)\}$ par conservation de la norme et $u(e_1)\perp u(e_2)$ ce qui donne quatre matrices éventuelles pour u dans la base orthonormale (e_1,e_2) :

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\qquad\begin{pmatrix}-1&0\\0&1\end{pmatrix},\qquad\begin{pmatrix}1&0\\0&-1\end{pmatrix},\qquad\begin{pmatrix}-1&0\\0&-1\end{pmatrix}.$$

Ces quatre matrices sont effectivement orthogonales et en composant avec une translation (e,a) avec $a\in L$ arbitraire on obtient quatre familles de transformations éléments de G :

$$(x,y)\longrightarrow(\pm x+2\alpha,\pm y+\beta),\qquad\alpha,\beta\in\mathbb{Z}.$$

* *
*