Ecole Polytechnique 2001 MP - Sujet 2 - Corrigé

Cette correction a été rédigée par Frédéric Bayart et est disponible à l'adresse suivante : http://mathweb.free.fr
Si vous avez des remarques à faire, ou pour signaler des erreurs, n'hésitez pas à écrire à : mathweb@free.fr

Mots-clés : groupe topologique, sous-groupe de $\mathbb{R}^n$, groupe linéaire, groupe orthogonal, groupe opérant sur un ensemble

Commentaires : Ce problème mélange l'algèbre pure (groupe) et la topologie. Par certains aspects, il est très classique et pourra être étudié avec profit par les candidats à l'agrégation.

Partie I.

1.a. Si L est discret, tout élément est isolé, donc en particulier 0 l'est. Réciproquement, si L n'est pas discret, il existe un point x de L qui n'est pas isolé, et donc une suite (x_n) de points de L avec $x_n \neq x$ pour tout n, et $x_n \to x$. Alors $x - x_n$ est une suite de points de L, tous distincts de 0, et qui tend vers 0. Donc 0 n'est pas isolé.

1.b. Soit (x_n) une suite de points de L qui converge vers x. Si x n'est pas élément de L, on peut toujours supposer que les (x_n) sont distincts. Alors la suite $(x_n - x_{n+1})$ est une suite d'éléments de L, distincts de 0, et qui converge vers 0. Donc 0 ne peut être isolé, ce qui n'est pas le cas puisque L est discret. Donc x est élément de L, et L est fermé.

1.c. C'est une question classique, qu'il faut savoir résoudre rapidement! Remarquons d'abord que les $a\mathbb{Z}$, avec $a > 0$, sont des sous-groupes discrets de $\mathbb{R}$. Réciproquement, si $L = \{0\}$, le résultat est trivialement vérifié. Si $L \neq \{0\}$, on pose $H = \mathbb{R}_+^* \cap L$, et on considère $a = \inf H$. Comme 0 est isolé, $a > 0$. Comme L est fermé, $a \in L$, et donc $a\mathbb{Z} \subset L$. Si l'inclusion est stricte, on considère $x \in L - a\mathbb{Z}$. On encadre ce x par $ka < x < (k+1)a$, où k est un entier. Mais alors, $x - ka$ est un élément de L, qui vérifie $x - ka > 0$ et $x - ka < a$. Ceci contredit la définition de a.

2. D'abord, si $\alpha = \frac{p}{q}$ est un rationnel, avec $p \wedge q = 1$, un élément de L s'écrit :

$$m + n\frac{p}{q} = (mq + np)\,\frac{1}{q},$$

et donc $L \subset \frac{1}{q}\mathbb{Z}$, ce qui prouve que L est discret.
Réciproquement, si L est discret, soit $a > 0$ tel que $L = a\mathbb{Z}$. Pour $m = 0$, $n = 1$, on trouve $\alpha = ka \implies a = \alpha/k$. Pour $m = 1$, $n = 1$, on obtient $1 + \alpha = k'a = k'\alpha/k$, où k et k' sont des entiers. Ceci prouve que α est rationnel.

3. Voici un bon contre-exemple en topologie! Soit $e_1 = (1,0)$ et $e_2 = (1,1)$. On pose :

$$G = \left\{ne_1 + m\sqrt{2}e_2;\ (n,m) \in \mathbb{Z}\right\}.$$

Si on note p la première projection, un calcul aisé montre que $p(G) = \{n + m\sqrt{2}\}$, qui n'est pas discret d'après la question précédente. D'autre part, G est discret dans $\mathbb{R}^2$ car si $x \in G$, $x \neq 0$, on remarque que $\|x\| \geq 1$ (faire le calcul suivant que m est nul ou non), et donc 0 est isolé, et G est discret.

4.a. Il est bien connu que l'intersection d'un ensemble discret et d'un ensemble borné dans $\mathbb{R}^n$ est fini (si elle ne l'était pas, on construirait une suite injective d'éléments dans l'intersection, puis l'extraction d'une suite convergente nierait le fait que L est discret). Il est en outre clair que $\{\sum_{i=1}^m \lambda_i a_i |\ \lambda_i \in [0,1[\}$ est un ensemble borné.

4.b. Si $x \in L$, x est en particulier élément de F et on peut décomposer $x = \sum_{i=1}^m \mu_i a_i$. Nous écrivons alors :

$$x = \sum_{i=1}^m [\mu_i] a_i + \sum_{i=1}^m (\mu_i - [\mu_i]) a_i.$$

On conclut car $\sum_{i=1}^m [\mu_i] a_i$ est élément de L' et $\sum_{i=1}^m (\mu_i - [\mu_i]) a_i$ est élément de P.
Prouvons désormais l'unicité. Si $y + z = y' + z'$, on écrit $y - y' = z' - z = \sum \lambda_i a_i$, où d'une part $\lambda_i \in \mathbb{Z}$, car $y - y' \in L'$ et $\lambda_i \in]-1,1[$, car $z,z' \in P$. Donc $\lambda_i = 0$, et $y = y'$, $z = z'$.

4.c. Pour k allant de 1 à $card(P)$, on écrit la décomposition $kx = y_k + z_k$. Comme P est fini, il existe k et l éléments de $\{1,\dots,card(P)\}$ tels que $z_k = z_l$. En particulier, $(k-l)x = y_k - y_l$ est élément de L'.

4.d. En fait, dans la question précédente, on peut choisir le même d pour tous les x de L. En effet, la démonstration effectuée prouve que l'on peut choisir $d \leq card(P)$. En posant q la factorielle de $card(P)$, pour tout x de L', alors $qx \in L'$. L'application de $L \to L'$, définie par $x \mapsto qx$, est injective, donc L est isomorphe à sous-groupe de L', qui est lui-même isomorphe à $\mathbb{Z}^m$.

5.a. $\pi(L)$ est inclus dans $\mathbb{Z}$ et en est un sous-groupe. Donc $\pi(L) = k\mathbb{Z}$. On choisit pour x^0 un élément de $\pi^{-1}(k)$.

5.b. Soit p un entier tel que $\pi(x) = p\pi(x^0)$. On pose $\tilde{x} = x - px^0$. Alors $\tilde{x} \in L$, et $\pi(x - px^0) = 0$ et donc $\tilde{x}_m = 0$. L'unicité de la décomposition se prouve facilement en appliquant la projection π à deux décompositions éventuelles.

5.c. D'après la question 4., il suffit de prouver que tout sous-groupe de $\mathbb{Z}^m$ est isomorphe à un groupe $\mathbb{Z}^r$. On démontre ceci par récurrence sur m. Si $m = 1$, le résultat est réalisé. Soit maintenant L un sous-groupe de $\mathbb{Z}^m$, avec $m \geq 2$.

- Si $\pi(L) = \{0\}$, L peut en fait être vu comme un sous-groupe de $\mathbb{Z}^{m-1}$, et on a le résultat.
- Si $\pi(L) \neq \{0\}$, on utilise les notations de la question b. Soit f l'application de L dans $\mathbb{Z}^{m-1}$ définie par $x \mapsto \tilde{x}$. On vérifie que f est un morphisme de groupes : si $x = px^0 + \tilde{x}$ et $x' = qx^0 + \tilde{x'}$ on écrit $x + x' = (p+q)x^0 + \tilde{x} + \tilde{x'}$, et donc $f(x+x') = \tilde{x} + \tilde{x'} = f(x) + f(x')$. Soit $L' = f(L)$. Par hypothèse de récurrence, L' est isomorphe à un groupe $\mathbb{Z}^r$. En particulier, soit $x^1,\dots,x^r$ une $\mathbb{Z}$-base de L'. Alors en appliquant les résultats de la question précédente, $x^0,x^1,\dots,x^r$ est une $\mathbb{Z}-$base de L, et L est donc isomorphe à $\mathbb{Z}^{r+1}$.

6. Soit A une matrice 2×2 à coefficients dans $\mathbb{Z}$, telle que $(u_1,u_2) = A(v_1,v_2)$. Comme $(v_1,v_2) = A^{-1}(u_1,u_2)$, et que A^{-1} est aussi à coefficients dans $\mathbb{Z}$, le calcul de l'inverse d'une matrice 2×2 prouve que nécessairement $|\det A| = 1$. Le déterminant des deux vecteurs (u_1,u_2) vaut donc celui des deux vecteurs (v_1,v_2), et donc les deux parallélogrammes ont la même aire.

Partie II.

7.a. $GB = \{y_1,\dots,y_r\}$ est un ensemble fini. Pour chaque y_i élément de GB, nous écrivons que

$$y_i = \sum_{j=1}^n \frac{p_{i,j}}{q_{i,j}} e_j,$$

où les $p_{i,j}$ et $q_{i,j}$ sont des entiers naturels (nous savons que nous avons une telle décomposition car les coefficients des éléments de G sont des rationnels). Soit d un multiple commun des $q_{i,j}$. Alors, chaque dy_i est élément de $L(B)$, et par combinaisons linéaires, chaque x qui est élément de $dL(GB)$, et qui donc s'écrit $x = a_1 dy_1 + \cdots + a_r dy_r$, est élément de $L(B)$.

7.b. L'inclusion précédente prouve en particulier que $dL(GB)$ est un ensemble discret, puisque $L(B)$ l'est. D'après la première partie, $L(GB)$ est donc isomorphe à un groupe $\mathbb{Z}^r$, où $r \leq n$. En fait, on a même $r = n$, car l'espace vectoriel engendré par $L(GB)$ est E. Soit $(f_1, \ldots, f_n)$ une $\mathbb{Z}-$base de $L(GB)$. En particulier, $(f_1, \ldots, f_n)$ est une base de E. Pour chaque i, nous écrivons que f_i est élément de $L(GB)$:

$$f_i = \sum_{j,k} a_{i,j,k} g_j(e_k),$$

avec $a_{i,j,k}$ entier, et g_j élément de G. Si $g \in G$, alors

$$g(f_i) = \sum_{j,k} a_{i,j,k} g \circ g_j(e_k).$$

Mais $g \circ g_j(e_k)$ est élément de $L(GB)$, et s'écrit donc comme combinaison linéaire à coefficients entiers des $(f_1, \ldots, f_n)$. C'est aussi le cas des $g(f_i)$. Nous avons alors prouvé que dans la base $(f_1, \ldots, f_n)$, les matrices des éléments de G sont à coefficients entiers.

8.a. Nous appliquons le résultat de la question précédente au groupe $G = \{A^k;\ k \in \mathbb{N}\}$, qui est fini car A est d'ordre fini. Dans une base de E, A est à coefficients entiers. Le calcul du polynôme caractéristique de A dans cette base montre que ce polynôme est à coefficients entiers.

8.b. On sait que A est semblable sur $\mathbb{C}$ à une matrice du type $\begin{pmatrix} \lambda_1 & \mu \\ 0 & \lambda_2 \end{pmatrix}$. Comme $A^r = I$, et que $\begin{pmatrix} \lambda_1 & \mu \\ 0 & \lambda_2 \end{pmatrix}^r = \begin{pmatrix} \lambda_1^r & r\mu \\ 0 & \lambda_2^r \end{pmatrix}$, on a nécessairement $\mu = 0$. En outre, $|\lambda_1| = |\lambda_2| = 1$, et le polynôme caractéristique de A est $X^2 - (\lambda_1 + \lambda_2)X + \lambda_1\lambda_2$. Mais comme nous savons qu'il est à coefficients entiers, cela ne peut-être que $X^2 + aX + b$, où $a = 0,1,2,-1,-2$, et $b = \pm 1$. Reste donc à envisager ces différents cas.

- $X^2 - 1 = (X-1)(X+1)$: A est semblable à $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, et est donc d'ordre 2.
- $X^2 + 1 = (X-i)(X+i)$: A est semblable à $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, et est donc d'ordre 4. C'est par exemple le cas de la matrice $\begin{pmatrix} 1 & 1 \\ -2 & -1 \end{pmatrix}$.
- $X^2 + X + 1$: A est semblable à $\begin{pmatrix} e^{i2\pi/3} & 0 \\ 0 & e^{-i2\pi/3} \end{pmatrix}$, et est donc d'ordre 3. C'est par exemple le cas de la matrice $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.
- $X^2 - X + 1$: A est semblable à $\begin{pmatrix} e^{i\pi/3} & 0 \\ 0 & e^{-i\pi/3} \end{pmatrix}$, et est donc d'ordre 6. C'est par exemple le cas de la matrice $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.
- $X^2 + 2X + 1$, A est la matrice $-I$, et est donc d'ordre 2.
- $X^2 - 2X + 1$, A est la matrice I, et est donc d'ordre 1.
- Dans les autres cas ($X^2 \pm 2X - 1$, $X^2 \pm X - 1$), les racines du polynôme caractéristique ne sont pas de module 1, et donc ne conduisent pas à des matrices qui seront d'ordre fini.

Partie III.

9. $O(E)$ étant une partie d'un espace vectoriel normé de dimension finie, il suffit de montrer que $O(E)$ est une partie fermée bornée. Or, tout élément de $O(E)$ est de norme 1, puisqu'il s'agit d'une isométrie. D'autre part, on sait aussi que $O(E) = \{u \in GL(E); u^*u = e\}$, où u^* désigne l'adjoint

de u. Or l'application ψ qui à une application linéaire sur E associe l'application linéaire u^*u est continue, et $O(E) = \psi^{-1}(e)$. Comme le singleton $\{e\}$ est fermé, $O(E)$ l'est aussi.

10.a. Soit $g = (u,a)$, et $g' = (u',a')$. Alors :

$$\begin{array}{rcl} g \circ g'(x) & = & u(u'(x) + a') + a \\ & = & u \circ u'(x) + u(a') + a \end{array}$$

$AO(E)$ est un groupe pour la loi :

$$(u,a).(u',a') = (u \circ u',u(a') + a).$$

L'élément neutre de ce groupe est $(e,0)$:

$$(u,a).(e,0) = (u,a) = (e,0).(u,a).$$

L'inverse d'un élément (u,a) est $(u^{-1}, -u^{-1}(a))$:

$$(u,a).(u^{-1}, -u^{-1}(a)) = (e,a - a) = (e,0) = (u^{-1}, -u^{-1}(a)).(u,a).$$

10.b. Avec la règle de calcul précédemment énoncée, on trouve facilement :

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

11.a. Si $(u,a) \in G$, alors pour tout x de L, on a : $u(x) + a \in L$. En particulier, pour $x = 0$, $a \in L$. Comme une translation est un isomorphisme dans un groupe, on a bien $(e,a) \in G$. En outre, pour tout x de L, $u(x) \in L$. En outre, comme $(u,a)^{-1}$ est aussi élément de G (qui est un sous-groupe de $AO(E)$), pour tout x de L, $u^{-1}(x)$ appartient à L. Ceci achève de prouver que $(u,0) \in G$.

11.b. Soit $\{e_1,\dots,e_n\}$ une $\mathbb{Z}$-base de L, qui est aussi une base de E. Soit $u \in \rho(G)$, et $S_1 = \{x \in L;\ \|x\| = \|e_1\|\}$. S_1 est fini, et $u(e_1) \in S_1$. Donc il n'y a qu'un nombre fini de choix pour $u(e_1)$. C'est bien sûr la même chose pour chaque $u(e_k)$. Comme u est entièrement déterminé par l'image de $(e_1,\dots,e_n)$, il n'y a qu'un nombre fini de choix possibles pour u.

11.c. Il s'agit de déterminer $\rho(G)$, les élément a possibles d'un couple (u,a) étant tous les éléments de G. Nous copions le raisonnement de la question précédente, avec $e_1 = (0,1)$ et $e_2 = (2,0)$. Comme dans $O(E)$, les éléments sont des rotations ou des symétries axiales, les seules possibilités pour envoyer e_1 sur un élément de norme 1 et e_2 sur un élément de norme 2 sont :

- $u_1 = e$,
- $u_2 = -e$,
- u_3 est la symétrie d'axe (Ox),
- u_4 est la symétrie d'axe (Oy).

On a alors :

$$G = \big\{(u_i,a);\ i \in \{1,\dots,4\},\ a \in L\big\}.$$