ÉCOLE POLYTECHNIQUE **FILIÈRE MP**

CONCOURS D'ADMISSION 2001

DEUXIÈME COMPOSITION DE MATHÉMATIQUES

(Durée : 4 heures)

L'utilisation des calculatrices n'est pas autorisée pour cette épreuve.

⋆⋆⋆

On attachera la plus grande importance à la clarté, à la précision et à la concision de la rédaction.

⋆⋆⋆

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 $(\ |\ )$ son produit scalaire usuel et par $\|\ \|$ 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 **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 $k_i \in \mathbf{Z}$.

Première partie

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 $a \in [0, +\infty[$.

2. On désigne par α un nombre réel > 0 et par L le sous-groupe de $\mathbf{R}$, ensemble des réels $m + n\alpha$ où $n, m \in \mathbf{Z}$. 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. On se propose ici de démontrer que tout sous-groupe discret L de E est isomorphe à un sous-groupe d'un groupe $\mathbf{Z}^m$. 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

$$P = L \cap \left\{ \sum_{i=1}^{m} \lambda_i a_i \,|\, \lambda_i \in [0,1[\right\} .$$

a) Vérifier que P est un ensemble fini.

b) Etant donné un élément x de L, construire un couple $(y,z) \in L' \times P$ tel que l'on ait $x = y + z$, et démontrer son unicité.

c) Soit encore x un élément de L ; écrivant $kx = y_k + z_k$ (pour k entier > 0), montrer qu'il existe un entier $d > 0$ tel que l'on ait $dx \in L'$.

d) Conclure.

5. Dans cette question, L est un sous-groupe de $\mathbf{Z}^m$; ses éléments seront notés $x = (x_1, \ldots, x_m)$; on posera $\pi(x) = x_m$.

a) Montrer qu'il existe un entier $k \geqslant 0$ et un élément x° de L tel que l'on ait

$$\pi(L) = k\mathbf{Z} = \pi(x^\circ)\mathbf{Z} .$$

b) On suppose ici $\pi(L)$ non réduit à $\{0\}$; étant donné un élément x de L, construire un couple $(p, \widetilde{x}) \in \mathbf{Z} \times L$ tel que l'on ait $\widetilde{x}_m = 0$ et $x = px^\circ + \widetilde{x}$; démontrer son unicité.

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

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).

Deuxième partie

7. Dans cette question, on désigne par B la base canonique de E et par $GL(E)$ 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 $GL(E)$ 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) Montrer qu'il existe un entier $d > 0$ 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 $A^r = I$ et que r est le plus petit entier > 0 ayant cette propriété).

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

b) On suppose ici $n = 2$. Montrer 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.

Troisième partie

On désigne par $O(E)$ le groupe des automorphismes linéaires orthogonaux de E (ensemble des u de $GL(E)$ tels que $\|u(x)\| = \|x\|$ pour tout x de E), et par $AO(E)$ l'ensemble des transformations de E de la forme

$$x \mapsto g(x) = u(x) + a \quad \text{où} \quad u \in O(E) \quad \text{et} \quad a \in E \;;$$

on écrit alors $g = (u, a)$. On note e l'élément neutre de $O(E)$.

9. Montrer que $O(E)$ 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 $AO(E) \to O(E)$ 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) Montrer 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) de E tels que $x_1 \in 2\mathbf{Z},\ x_2 \in \mathbf{Z}$.

* *
*

Rapport de M^{me} Hélène AIRAULT et M. Paul GÉRARDIN, correcteurs.

Le problème traitait de propriétés de sous-groupes discrets de l'espace euclidien R^n. De tels sous-groupes apparaissent en particulier si on considère les périodes d'une fonction périodique de variable complexe.

Approximativement un quart des candidats a bien compris le problème. Les notes se répartissent de la manière suivante (*on donne le pourcentage de candidats ayant obtenu une note N dans un intervalle donné*) :

$0 \leq \mathrm{N} < 4$	7%
$4 \leq \mathrm{N} < 8$	24%
$8 \leq \mathrm{N} < 12$	31%
$12 \leq \mathrm{N} \leq 16$	25%
$16 \leq \mathrm{N} \leq 20$	13%

On a attribué 43 notes inférieures ou égales à 2/20, sur 1295 copies corrigées.

Première partie

1.a) Il faut montrer l'équivalence de deux propriétés. Lorsque L est discret, alors par la définition, le point 0 est isolé. Ceci a été fait par presque tous les candidats.

Seulement la moitié des candidats établit la réciproque. Une translation de vecteur x permettait de transporter un voisinage de 0 en un voisinage de x. Beaucoup de candidats se sont embrouillés dans leurs notations.

1.b) Souvent, pour montrer que L est fermé dans l'espace E, les copies utilisent seulement l'hypothèse que la partie est discrète dans E : cette hypothèse ne suffit pas puisque la partie discrète $\{1/n | n \in N^*\}$ de R n'est pas fermée dans R. La condition pour L d'être un sous-groupe est essentielle. On peut procéder de plusieurs manières. Quelques candidats ont montré directement que le complémentaire de L est ouvert en remarquant qu'il existe $\alpha > 0$ tel que $x, y \in L$ et $x \neq 0 \Rightarrow |y - x| > \alpha$. La plupart des candidats ont préféré utiliser les suites. Il fallait montrer qu'une suite de points de L qui converge dans E est stationnaire et déduire que la limite de cette suite est dans L. Certains ont escamoté les étapes du raisonnement : ils ne démontrent pas que la suite est stationnaire. Dans certaines mauvaises copies, on trouve que L est fermé car c'est « une réunion de fermés », toute partie de E serait fermée comme réunion de points !

1.c) Beaucoup de candidats ont omis de montrer que aZ est discret. La plupart oublient le cas où a est nul. Pour la réciproque, les démonstrations claires n'étaient pas très nombreuses. Beaucoup de copies faisaient référence à « la division euclidienne » sans bien connaître le sens de ce concept. Certains candidats ont montré qu'ils avaient étudié la théorie des sous-groupes denses dans R, ce qui n'était pas nécessaire. Le minimum a des nombres réels positifs appartenant à L est dans L car l'ensemble L est fermé. La condition $\lim_{n\to\infty} |\frac{p_n}{q_n} - \alpha| = 0$ n'implique pas que la suite $(p_n - \alpha q_n)_n$ tende vers zéro quand $n \to \infty$.

2) Si $\alpha > 0$ est rationnel, il s'écrit sous la forme irréductible $\alpha = \frac{p}{q}$, avec $p > 0$, $q > 0$ et dans ce cas, $L = \frac{1}{q}Z$. Seulement quelques candidats ont donné une démonstration succincte, alors que la plupart ont perdu du temps dans une rédaction non convaincante.

Pour la réciproque, si 1 et α sont multiples entiers d'un même nombre, alors α est un nombre rationnel comme quotient de ces deux multiples. Autrement, si $L = Z + \alpha Z$ est discret, il est de la forme aZ avec $a > 0$. L'élément 1 appartient à L, donc 1 s'écrit comme multiple de a. L'élément a est donc rationnel et comme α est un multiple de a, on déduit que α est rationnel.

3) Certains candidats ont donné des exemples de sous-ensembles de R^2 qui ne sont pas des sous-groupes. On pouvait pivoter d'un tiers de tour le sous-groupe Z^2 de R^2.

4.a) La rédaction de la solution donnée par de nombreux candidats est très imprécise. Les candidats font appel au théorème de Bolzano-Weierstrass et on peut lire les mots « extraction » « suite extraite », ou bien « R est archimédien »....mais sans rapport clair avec la démonstration recherchée. L'ensemble $\{\sum_{i=1}^{m} \lambda_i a_i | \lambda_i \in [0, 1[\}$ est borné, donc contenu dans un compact. L'ensemble P discret et contenu dans un ensemble compact est fini.

4.b) Il y a beaucoup d'erreurs dans la démonstration de l'unicité. Les conditions $z \in P$, $z' \in P$ n'entraînent pas que $z - z'$ appartienne à P.

Pour l'existence de la décomposition, beaucoup de candidats ont considéré la « partie entière » sans prendre en compte le cas où les composantes de x dans la base $(a_i)_{1\leq i\leq n}$ sont négatives. Soit α_i la composante suivant a_i, alors $\alpha_i = n_i + z_i$ avec $n_i \in Z$ et il faut bien préciser la condition $0 \leq z_i < 1$.

4.c) Seulement la moitié des candidats a résolu cette question. D'après la question **a)**, l'ensemble P est fini. Pour $x \in L$, il existe deux entiers distincts k_1 et k_2 tels que $k_1 x = y_{k_1} + z_{k_1}$ et $k_2 x = y_{k_2} + z_{k_2}$ avec $z_{k_1} = z_{k_2}$. On suppose $k_1 > k_2$ et on prend $d = k_1 - k_2$, qui dépend a priori du point x.

4.d) Très peu de bonnes solutions ont été données pour cette question.

5.a) Beaucoup de candidats n'ont pas vu que l'image $\pi(L)$ est un sous-groupe de Z et par suite de la forme kZ avec $k \in N$. Souvent ils ont étudié $\inf \pi(L)$, ce qui n'était pas utile. Peu de candidats ont remarqué que l'entier k appartient à $\pi(L)$. Il existe alors x_0 tel que $k = \pi(x_0)$. Il ne s'agissait pas de répéter le cours sur les sous-groupes de Z.

5.b) Une bonne partie des candidats a réussi à déterminer le couple $(p, \widetilde{x})$. Soit $x = (x_1, x_2, \cdots, kp) \in L$ avec $p \in Z$ et soit $x^0 = (x_1^0, x_2^0, \cdots, \pi(x_0))$, certains candidats n'ont pas su relier k et $\pi(x_0)$ et calculer $x - px_0$.

Les candidats qui ont traité le problème de l'unicité ont souvent omis de préciser que $\pi(x_0) \neq 0$.

5.c) Une bonne partie des candidats a abordé cette question. En général les rédactions données sont assez longues et embrouillées. D'après certains candidats, un sous-groupe de Z^m serait la somme directe de ses projections. Le sous-groupes $Z(1,1)$ de R^2 n'est pas égal à la somme $Z(1,0) + Z(0,1)$. Pour démontrer le résultat demandé, on pouvait faire un raisonnement par récurrence en utilisant **5.b)**.

6) La majorité des candidats a omis de traiter cette question et parmi ceux qui l'ont traitée, très peu ont donné une réponse correcte. Celle-ci utilisait la relation entre l'aire d'un parallélogramme construit sur deux vecteurs et le déterminant de ces deux vecteurs, puis la modification du déterminant par changement de base, et enfin le déterminant de la matrice de changement de base en jeu qui ici est égal à 1 ou -1.

Deuxième partie

7.a) Toute notation (comme « $\wedge$ » ou « $\vee$ ») doit être définie. D'autre part, certains candidats confondent le plus petit commun multiple, le maximum et le pgcd. Les démonstrations étaient souvent assez confuses.

7.b) Cette question difficile ne fut résolue que par une dizaine de candidats, bien que de nombreuses copies prétendent en donner une solution. En général, il est faux qu'une matrice à coefficients rationnels puisse être ramenée par un changement de base à une matrice à coefficients entiers, par exemple, la matrice scalaire $\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$.

8.a) Cette question a été traitée par la majorité des candidats. D'après **7.a)**, il existe une base de R^n par rapport à laquelle toutes les matrices des éléments de G ont des coefficients entiers. Une partie des candidats a omis de mentionner que le polynôme caractéristique ne dépend pas de la base choisie.

8.b) Un petit nombre de copies a donné des exemples corrects pour tous les cas, $r = 1, 2, 3, 4, 6$. Dans certaines copies, on trouve comme exemples des matrices à coefficients non entiers. Le fait que ces valeurs soient les seules valeurs possibles pour r n'a été démontré que par quelques candidats.

Troisième partie

9) Comme dans la question **4.a)**, on peut lire dans les copies des expressions comme « fermé borné », on ne sait ni de quel « fermé » il s'agit, ni par quoi il est borné. Il n'y a pas de logique entre les phrases successives. Il est écrit que « $O(E)$ est fermé », mais on ne sait pas dans quel espace. Pour certains candidats, le groupe linéaire $GL(E)$ est un espace vectoriel.

10.a) Beaucoup de candidats n'ont pas compris que la loi de groupe était celle de la composition des applications $(u_1, a_1) \circ (u_2, a_2) = (u_1 \circ u_2, u_1(a_2) + a_1)$. L'erreur la plus répandue était d'écrire $(u_1 \circ u_2, a_1 + a_2)$.

10.b) Les erreurs de **10.a)** se répercutaient sur **10.b)**.

11.a) Approximativement, la moitié des candidats a résolu cette question. Les candidats devaient montrer que a appartient à l'ensemble L. La justification donnée pour cela est souvent fausse, par exemple, on peut lire : « $a \in L$ » car L engendre E.

11.b) Il fallait démontrer que pour toute base de L sur Z, les matrices de $\rho(G)$ sont à coefficients entiers ; comme elles restent dans un compact, ces coefficients sont bornés et il n'y a qu'un nombre fini de possibilités. Moins de la moitié des candidats a abordé cette question.

11.c) Cette question fut résolue seulement dans quelques copies.

Pour la rédaction, on a remarqué un effort d'une partie des candidats. Toutefois, l'orthographe de « inclus » et « exclu » continue d'être une source de difficultés.