

Pierre Février; Lycée Pasteur; Neuilly.

Partie I

1. a) Soit donc L un sous-groupe de E .

S'il est discret, 0 (qui appartient à L) est isolé (dans L) par définition.

Réciproquement, supposons 0 isolé: il existe un voisinage V de 0 dans E tel que $V \cap L = \{0\}$.

Soit x dans L : d'une part, $x + V$ est voisinage de x par structure d'espace vectoriel normé; d'autre part, $x + L = L$ par structure de groupe; donc:

$$(x + V) \cap L = (x + V) \cap (x + L) = x + (V \cap L) = x + \{0\} = \{x\}$$

x est ainsi isolé dans L et L est discret.

Un sous-groupe L de E est discret si et seulement si 0 est isolé

b) Soit donc L un sous-groupe discret de E et soit $x \in \bar{L}$: x est limite d'une suite (x_k) de L .

Cette suite est de Cauchy: pour $\varepsilon > 0$ donné, il existe N tel que $k \geq l \geq N$ assure $\|x_k - x_l\| < \varepsilon$.

Comme 0 est isolé dans L , on peut choisir ε tel que $L \cap B(0, \varepsilon)$ se réduise à $\{0\}$. Les éléments $x_k - x_l$ précédents (qui sont bien dans L) sont alors nuls; la suite (x_k) est stationnaire à partir du rang N et $x = x_N$ est dans L .

Tout sous-groupe discret de E est fermé

c) D'abord, les sous-ensembles de la forme $a\mathbb{Z}$ sont des sous-groupes de \mathbb{R} et ils sont discrets, 0 étant isolé.

Réciproquement, soit L un sous-groupe discret de \mathbb{R} .

S'il est réduit à $\{0\}$, $a = 0$ convient.

Sinon, il contient nécessairement des éléments strictement positifs. Soit a la borne inférieure de $L \cap \mathbb{R}_+^*$. $a > 0$ car 0 est isolé. Montrons par double inclusion que $L = a\mathbb{Z}$:

Si a n'était pas dans L , il existerait, par définition d'une borne inférieure, $x \in L$ tel que $a < x < 2a$, puis $y \in L$ tel que $a < y < x < 2a$. On aurait alors $x - y \in L$ tel que $0 < x - y < a$ ce qui contredirait le choix de a . Donc $a \in L$ et donc aussi $a\mathbb{Z} \subset L$.

Inversement, soit $x \in L$ et soit n la partie entière de x/a : $na \leq x < (n+1)a$. L'élément $x-na$ de L vérifie donc $0 \leq x-na < a$. Par définition de a , cela impose $x-na = 0$ donc $x \in a\mathbb{Z}$. Par double inclusion, $L = a\mathbb{Z}$ et on a prouvé:

Les sous-groupes discrets de \mathbb{R} sont les sous-ensembles $a\mathbb{Z}$

2. Si L est discret, il est de la forme $a\mathbb{Z}$ et ici $a > 0$. Comme 1 et α sont dans L , il existe en particulier des entiers p et q tels que $1 = qa$ et $\alpha = pa$. Il apparaît que $\alpha = p/q$, rationnel.

Inversement, si $\alpha = p/q$ ($p > 0, q > 0$), tous les réels $m + n\alpha$ sont dans $q^{-1}\mathbb{Z}$. L est donc un sous-groupe de ce groupe discret et il est donc lui-même discret (évident par exemple par 1a.)

L est discret si et seulement si α est rationnel

3. Identifiant \mathbb{R}^2 avec \mathbb{C} , on prend pour L l'ensemble des complexes $m+nj$ où $m, n \in \mathbb{Z}$.

C'est un sous-groupe discret, car le carré de la norme de tout élément est un entier (c'est $m^2 + n^2 - mn$), donc seul 0 se trouve dans la boule unité ouverte.

Sa première projection sur \mathbb{R} est le sous-groupe formé des $m + n\sqrt{3}/2$, non discret puisque $\sqrt{3}/2$ est irrationnel.

$\mathbb{Z} + \mathbb{Z}j$ répond à la question

4. Remarquons que (a_1, \dots, a_m) existe bien puisque L est partie génératrice de F et que nécessairement $m \leq n$.

a) Si P n'était pas fini, on pourrait considérer dans P une suite (x_k) dont les éléments seraient deux à deux distincts. P est borné; on peut donc appliquer Bolzano-Weierstrass et, quitte à extraire, supposer que la suite converge dans E . Sa limite x est dans L puisque celui-ci est fermé. Mais alors, si V est un voisinage de x , $V \cap L$ ne peut se réduire à x car il contient tous les x_k à partir d'un certain rang.

Cette contradiction assure que P est fini.

b) Soit donc $x \in L$. A fortiori, $x \in F = \text{Vect}(L)$ dont (a_1, \dots, a_m) est une base. Il existe donc des réels μ_1, \dots, μ_m (uniques) tels que $x = \sum_{i=1}^m \mu_i a_i$. Posons $k_i = E(\mu_i)$ et $\lambda_i = \mu_i - k_i$, et aussi $y = \sum_{i=1}^m k_i a_i$ et $z = \sum_{i=1}^m \lambda_i a_i$: $y \in L'$ car les k_i sont entiers; $x = y + z$ est évident; $z \in L$ car $z = x - y$ avec $x \in L$ et $y \in L' \subset L$; $z \in P$ car de plus les λ_i sont dans $[0, 1[$: le couple (y, z) convient.

Ce couple est unique car si $y' = \sum_{i=1}^m k'_i a_i$ et $z' = \sum_{i=1}^m \lambda'_i a_i$ conviennent aussi, l'indépendance de (a_1, \dots, a_m) exige $\mu_i = k'_i + \lambda'_i$ et donc $k'_i = E(\mu_i) = k_i$, puis $\lambda'_i = \lambda_i$:

$(y, z) \in L' \times P$ tel que $x = y + z$ existe et est unique.

c) Pour tout $k \in \mathbb{N}$, kx est encore dans L et le résultat du b. s'applique donc à kx : $kx = y_k + z_k$ avec $y_k \in L'$ et $z_k \in P$.

Puisque P est fini, les z_k ne peuvent être deux à deux distincts: il existe $k < l$ tels que $z_k = z_l$. Alors, $(l - k)x = y_l - y_k \in L'$ et $d = l - k > 0$ convient:

Il existe un entier d tel que $dx \in L'$.

d) Notons p_1, \dots, p_r les éléments de P ($r \geq 1$ car $0 \in P$). On applique la question c. à chaque p_i : il existe un entier $d_i > 0$ tel que $d_i p_i \in L'$. Soit d le ppcm des d_i : a fortiori $dp_i \in L'$ pour tout i .

Or, d'après b., tout $x \in L$ s'écrit $x = y + p_i$ pour une valeur de i . Donc $dx \in L'$. Ainsi $L \subset d^{-1}L'$ et L est un sous-groupe de $d^{-1}L'$.

Mais $d^{-1}L'$ est l'ensemble des éléments qui s'écrivent $\sum_{i=1}^m k_i d^{-1}a_i$ avec $k_i \in \mathbb{Z}$, écriture unique car $(d^{-1}a_1, \dots, d^{-1}a_m)$ est libre; donc $d^{-1}L'$ est isomorphe à \mathbb{Z}^m et:

L est isomorphe à un sous-groupe de \mathbb{Z}^m .

Rappelons que $m \leq n$ puisque (a_1, \dots, a_m) est libre dans \mathbb{R}^n .

5. a) π est un morphisme de groupes de L dans \mathbb{Z} . Donc $\pi(L)$ est un sous-groupe de \mathbb{Z} , c'est à dire un ensemble de la forme $k\mathbb{Z}$, $k \in \mathbb{N}$: $\pi(L) = k\mathbb{Z}$.

k lui-même est un élément de $\pi(L)$ et s'écrit donc $\pi(x^0)$ avec x^0 dans L .

$\pi(L) = k\mathbb{Z} = \pi(x^0)\mathbb{Z}$.

b) Soit $x \in L$. $\pi(x) \in \pi(L) = \pi(x^0)\mathbb{Z}$: il existe donc $p \in \mathbb{Z}$ tel que $\pi(x) = p\pi(x^0) = \pi(px^0)$. En posant $\tilde{x} = x - px^0$ (qui est bien dans L), on a donc $\pi(\tilde{x}) = 0$. $x = px^0 + \tilde{x}$ est une décomposition de la forme voulue.

Si $x = qx^0 + x'$ convient aussi, alors $\pi(x) = q\pi(x^0)$, c'est à dire $p\pi(x^0) = q\pi(x^0)$. Comme on suppose dans cette question $\pi(x^0) \neq 0$, on en déduit $p = q$ puis $x' = \tilde{x}$: la décomposition est unique.

$(p, \tilde{x}) \in \mathbb{Z} \times L$ tel que $\tilde{x} = 0$ et $x = px^0 + \tilde{x}$ existe et est unique.

c) Grâce à la question 4., il suffit de montrer: tout sous-groupe de \mathbb{Z}^m est isomorphe à un \mathbb{Z}^r (en convenant que $\mathbb{Z}^0 = \{0\}$).

Montrons cette propriété par récurrence sur m .

Pour $m = 0$, c'est évident et pour $m = 1$, c'est un résultat connu: tout sous-groupe de \mathbb{Z} est de la forme $a\mathbb{Z}$ et est donc isomorphe à \mathbb{Z} ou à $\{0\}$.

Supposons le résultat acquis pour l'entier $m - 1$, $m \geq 2$, et soit L un sous-groupe de \mathbb{Z}^m .

Remarquons que l'ensemble H des éléments de la forme $(x_1, \dots, x_{m-1}, 0) \in \mathbb{Z}^m$ s'identifie à \mathbb{Z}^{m-1} .

Introduisons alors $\pi(L)$ et distinguons deux cas:

Si $\pi(L) = \{0\}$, c'est que L est un sous-groupe de H et le résultat découle de la remarque précédente et de l'hypothèse de récurrence.

Si $\pi(L) \neq \{0\}$, on se trouve dans la situation du b): tout $x \in L$ s'écrit de manière unique $x = px^0 + \tilde{x}$ avec $p \in \mathbb{Z}$ et $\tilde{x} \in \ker \pi$. $\ker \pi$ est un sous-groupe de H (c'est $H \cap L$) et est donc isomorphe à un \mathbb{Z}^s par l'hypothèse de récurrence. On peut encore distinguer deux cas:

Si $s = 0$, c'est à dire $\ker \pi = \{0\}$, alors $L = x^0 \mathbb{Z}$, isomorphe à \mathbb{Z} et le résultat est acquis.

Si $s \neq 0$, $\ker \pi$ contient une famille (e_1, \dots, e_s) telle que tout élément de $\ker \pi$ s'écrit de manière unique $\sum_{i=1}^s k_i e_i$, $k_i \in \mathbb{Z}$. Alors L contient la famille (x^0, e_1, \dots, e_s) et tout élément de L s'écrit de manière unique $x = px^0 + \sum_{i=1}^s k_i e_i$, $p \in \mathbb{Z}$, $k_i \in \mathbb{Z}$. L est isomorphe à \mathbb{Z}^{s+1} et le résultat est acquis:

Tout sous-groupe discret de E est isomorphe à un \mathbb{Z}^r .

Remarque: Il résulte du raisonnement que $r \leq m$, donc, avec la remarque du 4., $r \leq n$. Plus précisément, si L est, comme en 4., un sous-groupe discret de E engendrant un sous-espace vectoriel de dimension m , il ne peut en exister une \mathbb{Z} -base ayant moins de m éléments, et L est donc isomorphe à \mathbb{Z}^m .

6. L'aire du parallélogramme construit sur (u_1, u_2) est $|\det(u_1, u_2)|$ où le déterminant est pris dans la base canonique.

Par définition d'une \mathbb{Z} -base, v_1 et v_2 s'écrivent $v_1 = au_1 + bu_2$ et $v_2 = cu_1 + du_2$, a, b, c, d entiers. Il en résulte $|\det(v_1, v_2)| = |ad - bc| |\det(u_1, u_2)|$ et l'aire du parallélogramme construit sur (v_1, v_2) est donc un multiple entier de l'aire du parallélogramme construit sur (u_1, u_2) .

Mais les rôles peuvent être échangés et donc:

Les deux aires sont nécessairement égales.

Partie II

7. a) Les éléments $g(x)$, $g \in G$, $x \in B$, sont en nombre fini et leurs coefficients sur la base B sont, par hypothèse, rationnels. Si $d > 0$ est le dénominateur commun à tous ces rationnels, $dg(x)$ est à coordonnées entières dans B pour tout $x \in B$ et tout $g \in G$. Autrement dit, $dGB \subset L(B)$.

Comme tout élément de $L(GB)$ est combinaison linéaire à coefficients dans \mathbb{Z} des éléments de GB , on a aussi $dL(GB) \subset L(B)$:

Il existe un entier $d > 0$ tel que $dL(GB) \subset L(B)$.

b) $L(B)$ est un sous-groupe discret de E (c'est l'ensemble des points à coordonnées entières, 0 est isolé). $d^{-1}L(B)$ aussi; donc son sous-groupe $L(GB)$ aussi (0 y est, a fortiori, isolé).

D'après la partie I, $L(GB)$ admet donc une \mathbb{Z} -base (e_1, \dots, e_r) avec $r \leq n$ (d'après les remarques). Mais comme les éléments de G sont inversibles, GB contient une base de E . Par conséquent, $L(GB)$ engendre E ; (e_1, \dots, e_r) aussi et donc $r = n$. Ainsi (e_1, \dots, e_n) , génératrice de E à n éléments, est une base de E .

Vérifions qu'elle répond à la question:

GB est stable par G puisque $g'(g(x)) = (g'g)(x)$. $L(GB)$, formé des combinaisons linéaires à coefficients entiers des éléments de GB , est donc aussi stable par G . En particulier, pour tout j et tout $g \in G$, $g(e_j) \in L(GB)$ et est donc combinaison linéaire à coefficients entiers de (e_1, \dots, e_n) . Cela signifie exactement:

Les matrices dans (e_1, \dots, e_n) des éléments de G sont à coefficients entiers.

8. a) A est inversible, puisque $A^r = I$, $r > 0$, et représente dans la base canonique de E un endomorphisme $u \in GL(E)$ tel que $u^r = Id$. Le sous-groupe G de $GL(E)$ engendré par u est fini, cyclique d'ordre r , constitué de Id, u, \dots, u^{r-1} , dont les matrices dans B sont I, A, \dots, A^{r-1} , à coefficients rationnels.

La question 7. s'applique et signifie notamment l'existence d'une matrice A' , semblable à A et à coefficients entiers.

Le polynôme caractéristique de A , égal à celui de A' , est donc à coefficients entiers.

b) Le raisonnement du a. montre que l'on peut supposer A à coefficients entiers.

D'autre part, $A^r = I$ assure que A est diagonalisable en tant que matrice complexe ($X^r - 1$ polynôme annulateur scindé à racines simples). De plus, les deux valeurs propres λ et μ (distinctes ou non) de A sont racines r -èmes de l'unité; en particulier $|\lambda| = |\mu| = 1$. Enfin, la trace et le déterminant de A sont entiers, donc $\lambda + \mu \in \mathbb{Z}$ et $\lambda\mu \in \mathbb{Z}$.

Supposons d'abord λ et μ réelles. Elles valent alors 1 ou -1 et A est égale à I_2 ou $-I_2$ ou semblable à $S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Pour I_2 , $r = 1$; pour $-I_2$ et S , $r = 2$ et nous avons là des exemples à coefficients entiers.

Supposons à présent λ et μ non réelles, donc complexes conjuguées: $\mu = \bar{\lambda} \neq \lambda$, de module 1. Ici, $\det A = \bar{\lambda}\lambda = 1$ et $Tr A = \bar{\lambda} + \lambda$ vérifie

$TrA \in \mathbb{Z}$ et $|TrA| \leq 2$. Mais $TrA = \pm 2$ exigerait $\bar{\lambda} = \lambda = \pm 1$, exclu ici. Donc $TrA \in \{-1, 0, 1\}$ et il y a trois possibilités pour le polynôme caractéristique χ_A :

$\chi_A = X^2 - X + 1$; $\lambda = e^{i\pi/3}$, $\mu = e^{-i\pi/3}$, racines primitives 6-èmes de l'unité; $r = 6$;

exemple: $A = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$.

$\chi_A = X^2 + 1$; $\lambda = i$, $\mu = -i$, racines primitives 4-èmes de l'unité; $r = 4$;

exemple: $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

$\chi_A = X^2 + X + 1$; $\lambda = j$, $\mu = j^2$, racines primitives 3-èmes de l'unité; $r = 3$;

exemple: $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

Les seules valeurs effectivement prises par r sont 1, 2, 3, 4 et 6.

Partie III

9. Résultat usuel:

Le groupe orthogonal $O(E)$ est compact.

10. a) $AO(E)$ est constitué de bijections de E sur lui-même et c'est un sous-groupe du groupe des bijections de E :

Il est non vide: l'identité e lui appartient et s'écrit aussi $(e, 0)$ avec les notations de l'énoncé.

Il est stable par composition: si $g = (u, a)$ et $g' = (u', a')$, $g'g(x) = u'(g(x)) + a' = u'u(x) + u'(a) + a'$. gg' est l'élément $(u'u, u'(a) + a')$ de $AO(E)$.

Il est stable par passage à l'inverse, puisqu'il découle du calcul précédent que $g = (u, a)$ admet $g' = (u^{-1}, -u^{-1}(a)) \in AO(E)$ pour inverse.

$AO(E)$ est un groupe.

Remarque: On reconnaît dans $AO(E)$ le groupe des isométries affines de E .

b) L'application du a. donne aussitôt:

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

11. a) Soit donc $(u, a) \in G$.

Remarquons d'abord que (e, b) est la translation de vecteur b , de sorte que (e, b) est dans G si et seulement si b est dans L .

Soit donc $b \in L$. Par structure de groupe, $(u, a)(e, b)(u, a)^{-1} \in G$, c'est à dire $(e, u(b)) \in G$ et donc $u(b) \in L$. Cela établit que $u(L) \subset L$.

Mais on a aussi $(u, a)^{-1} \in G$, c'est à dire $(u^{-1}, -u^{-1}(a)) \in G$. Par le même raisonnement, on en déduit $u^{-1}(L) \subset L$, donc $L \subset u(L)$.

Finalement, $u(L) = L$, c'est à dire $(u, 0) \in G$.

Comme, enfin, $(u, a) = (e, a)(u, 0)$, l'élément $(e, a) = (u, a)(u, 0)^{-1} \in G$ aussi.

$$\boxed{(u, a) \in G \text{ si et seulement si } (u, 0) \in G \text{ et } (e, a) \in G.}$$

b) Puisque u n'est autre que $(u, 0)$, il résulte du a) que $\rho(G)$ est constitué des $u \in O(E)$ tels que $u(L) = L$, autrement dit $\rho(G) = G \cap O(E)$.

L admet une \mathbb{Z} -base (e_1, \dots, e_r) avec $r \leq n$, mais puisque L engendre E , on a aussi $r \geq n$, donc $r = n$ et (e_1, \dots, e_n) , génératrice à n éléments, est une base de E .

Or L ne possède qu'un nombre fini de points sur toute sphère de centre 0 (même argument qu'au 4.a pour prouver que P est fini. En fait, pour tout compact K de E , $L \cap K$ est fini). Cela entraîne que par $u \in G \cap O(E)$, chaque e_i n'a qu'un nombre fini d'images possibles: les $x \in L$ tels que $\|x\| = \|e_i\|$. Comme u est entièrement défini par les images des e_i , il n'existe qu'un nombre fini de possibilités pour u :

$$\boxed{\rho(G) \text{ est fini.}}$$

c) D'après a), les éléments de G sont les composés d'un élément de $\rho(G)$ et d'une translation de vecteur $a \in L$.

Déterminons $\rho(G)$. $L = 2\mathbb{Z}e_1 + \mathbb{Z}e_2$, (e_1, e_2) base canonique de \mathbb{R}^2 . Une \mathbb{Z} -base de L est donc $(2e_1, e_2)$. Si $u \in \rho(G)$, $u(e_2)$ est un élément de L de norme 1; il n'en existe que deux: e_2 et $-e_2$: $u(e_2) = \pm e_2$. Comme $u \in O(E)$, $u(e_1)$ est orthogonal à e_2 et de norme 1; c'est donc $\pm e_1$.

Il n'existe donc que 4 possibilités pour $u \in \rho(G)$ données par $u(e_i) = \varepsilon_i e_i$, $\varepsilon_i = \pm 1$. Or il s'agit bien d'éléments de $O(E)$ qui conservent L (Id , $-Id$, les réflexions d'axes $\mathbb{R}e_1$ et $\mathbb{R}e_2$): $\rho(G)$ est constitué de ces 4 éléments (c'est le groupe du rectangle).

En composant avec les translations de vecteur $a \in L$, on obtient tous les éléments de G :

$u = Id$: (u, a) est la translation de vecteur a .

$u = -Id$: (u, a) est la symétrie centrale par rapport à $a/2$.

$u = s_{e_i}$: (u, a) est la réflexion d'axe $a/2 + \mathbb{R}e_i$.

($a/2$ décrit le sous-groupe discret $L/2$).

G est constitué des éléments ainsi énumérés.
