Sous-groupes fermés de $\mathbb{R}^n$

On munit $\mathbb{R}^n$ de sa structure euclidienne canonique. Une partie est dite discrète lorsque chacun de ses points est isolé (dans $\mathbb{R}^n$). On sait qu'une partie compacte et discrète de $\mathbb{R}^n$ est finie.

Sous-groupes fermés

On dit qu'un groupe G est somme directe de deux sous-groupes H_1 et H_2, et on note $G = H_1 \oplus H_2$, lorsque tout $g \in G$ s'écrit de manière unique sous la forme $g = h_1 + h_2$ avec $(h_1, h_2) \in H_1 \times H_2$. Si G est un sous-groupe de $\mathbb{R}^n$, on note $\mathrm{rg}(G) = \dim \mathrm{Vect}_{\mathbb{R}}(G)$. C'est le rang de G.

Proposition : Si G est un sous-groupe de $\mathbb{R}^n$, $\mathrm{Adh}(G)$ est aussi un sous-groupe de $\mathbb{R}^n$.

$\square$ *On a $0 \in G \subset \mathrm{Adh}(G)$. Si $x, y \in \mathrm{Adh}(G)$, il existe des suites (x_n) et (y_n) de points de G qui convergent vers x et y. Comme $(x_n - y_n)$ est à valeurs dans G, on obtient $x - y \in \mathrm{Adh}(G)$.*

$\square$

Proposition : Un sous-groupe G de $\mathbb{R}^n$ est discret si et seulement si 0 est isolé dans G.

$\square$ *Si G est discret, 0 est isolé dans G. Réciproquement, supposons 0 isolé dans G. Il existe alors $r > 0$ tel que $B(0,r) \cap G = \{0\}$. Soit $x \in G$. Comme G contient les $y - x$ pour $y \in G$, on a $y - x \notin B(0,r)$ pour tout $y \in G \setminus \{x\}$. On en déduit que $B(x, r) \cap G = \{x\}$, donc G est discret.*

$\square$

Proposition : Tout sous-groupe discret de $\mathbb{R}^n$ est fermé.

$\square$ *Soit G un sous-groupe discret de $\mathbb{R}^n$. Soit (x_n) une suite d'éléments de G qui converge vers $x \in \mathbb{R}^n$. La suite $(x_{n+1} - x_n)$ est à valeurs dans G et converge vers 0. Elle est donc nulle à partir d'un certain rang, c'est-à-dire que (x_n) est stationnaire. Ainsi, $x \in G$.*

$\square$

Théorème (Structure des sous-groupes fermés de $\mathbb{R}^n$) : Soit G une partie de $\mathbb{R}^n$. G est un sous-groupe fermé de E si et seulement si il existe deux sous-espaces vectoriels supplémentaires F et S, et un sous-groupe discret D de S, tels que $G = F \oplus D$.

$\square$ • *Considérons d'abord le cas où G n'est pas discret. Dans ce cas, existe une suite $(x_p)_{p \in \mathbb{N}^*}$ d'éléments de $G \setminus \{0\}$ qui converge vers 0. On va en déduire que G contient une droite vectorielle. La suite $\left(\dfrac{x_p}{\|x_p\|} \right)$ est à valeurs dans la sphère unité, qui est compacte. On dispose donc d'une extractrice et d'un vecteur unitaire x tels que $\dfrac{x_{\varphi(p)}}{\|x_{\varphi(p)}\|} \underset{p \to +\infty}{\longrightarrow} x$.*

Montrons que $\mathrm{Vect}(x) \subset G$. *Fixons* $\lambda \in \mathbb{R}^*$. *On a* $\lambda x = \lim_{p\to+\infty} \frac{\lambda}{\|x_{\varphi(p)}\|} x_{\varphi(p)} = \lim_{p\to+\infty} \left\lfloor \frac{\lambda}{\|x_{\varphi(p)}\|} \right\rfloor x_{\varphi(p)}$ *puisque* $\left[\frac{\lambda}{\|x_{\varphi(p)}\|} - \left\lfloor \frac{\lambda}{\|x_{\varphi(p)}\|} \right\rfloor \right] x_{\varphi(p)} \underset{p\to+\infty}{\longrightarrow} 0$ *(la suite* (x_p) *tend vers* 0*). Comme* $\left\lfloor \frac{\lambda}{\|x_{\varphi(p)}\|} \right\rfloor x_{\varphi(p)}$ *est un élément de* G *(pour tout* p*), et comme* G *est fermé, on obtient* $\lambda x \in G$*. Finalement,* $\mathrm{Vect}(x) \subset G$.

• *Revenons au cas général. Si* G *contient au moins une droite vectorielle, on note* V_G *la réunion des droites vectorielles contenues dans* G*. Sinon, on convient que* $V_G = \{0\}$*. Cet ensemble contient* 0 *et est stable par homothétie. De plus, si* $x, y \in V_G$*, on a :* $\forall \lambda \in \mathbb{R}$, $\lambda(x+y) = \lambda x + \lambda y \in G$*, ce qui signifie que* $x + y \in V_G$*. Donc* V_G *est un sous-espace vectoriel de* $\mathbb{R}^n$ *contenu dans* G*. Si* W *est un sous-espace vectoriel de* $\mathbb{R}^n$ *contenu dans* G*, on a :* $\forall \lambda \in \mathbb{R}$, $\forall x \in W$, $\lambda x \in W \subset G$ *d'où* $x \in V_G$*. On en déduit que* V_G *est le plus grand sous-espace contenu dans* G*.*

Soit S *un supplémentaire de* V_G *dans* $\mathbb{R}^n$*. Montrons que* $G = V_G + (G \cap S)$ *et que* $G \cap S$ *est discret. Comme* G *contient* V_G *et* $S \cap G$*, on a bien* $V_G + (G \cap S) \subset G$*. Réciproquement, soit* $g \in G$*. On écrit* $g = v + s$ *avec* $(v, s) \in V_G \times S$*. On a* $s = g - v \in G$*, d'où* $g \in V_G + (G \cap S)$*. Par conséquent,* $G = V_G + (G \cap S)$*. La définition de* V_G *entraîne que* $S \cap G$ *est un sous-groupe de* G *ne contenant aucune droite vectorielle, donc discret d'après le • précédent. Ainsi, si* G *est un sous-groupe fermé de* $\mathbb{R}^n$*, il se décompose comme somme directe d'un sous-espace vectoriel et d'un sous-groupe discret de* $\mathbb{R}^n$*.*

• *Réciproquement, considérons* F *et* S *deux sous-espaces supplémentaires de* $\mathbb{R}^n$ *et un sous-groupe discret* D *de* S*. L'ensemble* $G = F + D$ *est un sous-groupe de* $\mathbb{R}^n$*.*

Reste à montrer que G *est fermé dans* $\mathbb{R}^n$*. Considérons une suite* (g_n) *d'éléments de* G *qui converge vers* $g \in \mathbb{R}^n$*. On écrit* $g_n = f_n + d_n$ *avec* $(f_n, d_n) \in F \times D$*. Notons* π *la projection de* $\mathbb{R}^n$ *sur* F *parallèlement à* S*. Cette application est continue, donc* $(f_n) = (\pi(g_n))$ *converge vers* $\pi(g)$*. Comme* F *est fermé, on obtient que* $\pi(g) \in F$*. Alors* $d_n = g_n - f_n \underset{n\to+\infty}{\longrightarrow} g - \pi(g)$ *et comme* D *est fermé dans* $\mathbb{R}^n$*, on a* $g - \pi(g) \in D$*. D'où* $g = \pi(g) + (g - \pi(g)) \in F + D = G$*.*

□

Dans la décomposition d'un sous-groupe fermé de $\mathbb{R}^n$, le supplémentaire S peut être choisi arbitrairement. On prendra souvent l'orthogonal de F. On note $\mathbf{d}(G) = \dim V_G$.
On est ainsi ramené à classer les sous-groupes discrets de $\mathbb{R}^n$.

Sous-groupes discrets

Exemple : On note $p(x, y) = x$ la projection sur la première coordonnée. Il existe des sous-groupes discrets de $\mathbb{R}^2$ tels que $p(\mathbb{R})$ ne soit pas une partie discrète de $\mathbb{R}$. En effet, si $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, le groupe $G = \mathbb{Z}(1{,}1) \oplus \mathbb{Z}(\alpha{,}0)$ a pour projection $\mathbb{Z} + \mathbb{Z}\alpha$, qui est dense dans $\mathbb{R}$. Pourtant, G est discret : pour $(x, y) \in \mathbb{Z}^2\backslash\{(0{,}0)\}$, on a $\|(x + y\alpha, x)\|^2 = (x + y\alpha)^2 + x^2$. Cette quantité est supérieure à 1 si $x \neq 0$, à α^2 sinon. Cela montre que $(0{,}0)$ est isolé dans G, donc que G est discret.

Pour un sous-groupe de la forme $G = \mathbb{Z}g_1 \oplus \ldots \oplus \mathbb{Z}g_r$ où $(g_1, \ldots, g_r)$ est une famille libre, on appelle cellule fondamentale associée à G l'ensemble $P = \left\{ \sum_{i=1}^{r} \lambda_i g_i : \forall i \in [\![1,n]\!],\ \lambda_i \in [0{,}1] \right\}$.

Théorème (Structure des sous-groupes discrets de $\mathbb{R}^n$) : Les sous-groupes de $\mathbb{R}^n$ de rang r sont les $\mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_r$ où $(a_1, \ldots, a_r)$ est une famille libre de vecteurs de E.

$\square$ • *Soit G un sous-groupe discret non nul, de rang r. Il existe $g_1, \dots, g_r \in G$ tels que $(g_1, \dots, g_r)$ soit une base de* $\mathrm{Vect}(G)$*.*
Si $x \in \mathrm{Vect}(G)$, on note $\ell(x)$ la dernière coordonnée de x sur cette base.
On considère la cellule $P = \left\{ \sum_{i=1}^{r} \lambda_i g_i : \forall i \in [\![1,n]\!],\ \lambda_i \in [0,1] \right\}$. L'ensemble $P \cap G$ est fini. En effet, c'est un compact (c'est l'image de $[0,1]^r$ par l'application continue $(\lambda_1, \dots, \lambda_r) \longmapsto \displaystyle\sum_{i=1}^{r} \lambda_i g_i$), et on sait qu'un compact discret est nécessairement fini.
On en déduit qu'il existe $h \in P \cap G$ tel que $\ell(h) > 0$ et : $\forall g \in G,\ \ell(g) > 0 \Longrightarrow \ell(g) \geqslant \ell(h)$. En effet, l'ensemble $P \cap G \cap \ell^{-1}(\mathbb{R}_+^*)$ est fini et non vide (il contient g_r). La restriction à cet ensemble de l'application ℓ atteint donc son minimum en un point h. Reste à voir que, pour $g \in G$ tel que $\ell(g) > 0$, on a aussi $\ell(g) \geqslant \ell(h)$. On décompose g en $g = \displaystyle\sum_{i=1}^{r} \lambda_i g_i$ où $\lambda_r = \ell(g)$. On considère l'élément $g' = g - \displaystyle\sum_{i=1}^{r} \lfloor \lambda_i \rfloor g_i = \sum_{i=1}^{r} (\lambda_i - \lfloor \lambda_i \rfloor) g_i$ de $G \cap P$. Si $\ell(g') \neq 0$, $\ell(g) \geqslant \ell(g') \geqslant \ell(h)$. Sinon, $\ell(g)$ est un entier strictement positif, donc supérieur ou égal à $1 = \ell(g_r) \geqslant \ell(h)$.
Soit $g \in G$. Montrons qu'il existe $\alpha \in \mathbb{Z}$ tel que $g - \alpha h \in \mathrm{Vect}(g_1, \dots, g_{r-1}) \cap G$. L'image de G par la forme linéaire ℓ est un sous-groupe de $\mathbb{R}$. Ce qui précède montre que $\ell(G) \cap]-\ell(h), \ell(h)[= \{0\}$ de sorte que 0 est isolé dans $\ell(G)$. Ainsi, $\ell(G)$ est monogène, engendré par son plus petit élément strictement positif, à savoir $\ell(h)$. Donc, pour tout $g \in G$, il existe $\alpha \in \mathbb{Z}$ tel que $\ell(g) = \alpha \ell(h)$ i.e. $g - \alpha h \in \mathrm{Vect}(g_1, \dots, g_{r-1})$.
• *Soit $(a_1, \dots, a_r)$ une famille libre de $\mathbb{R}^n$. On la complète en une base $(a_1, \dots, a_n)$. On note $(a_1^*, \dots, a_n^*)$ la base duale. Pour $x \in \mathbb{R}^n$, on note $N(x) = \displaystyle\max_{i \in [\![1,n]\!]} |a_i^*(x)|$, ce qui définit une norme (infinie) sur $\mathbb{R}^n$. Si $G = \mathbb{Z}a_1 \oplus \dots \oplus \mathbb{Z}a_r$, on a : $\forall g \in G \backslash \{0\},\ N(g) \geqslant 1$. L'équivalence de N avec la norme euclidienne canonique entraîne que 0 est isolé dans G. Ainsi, G est un sous-groupe discret.*
• *On va conclure par récurrence sur r. Notons $\mathscr{P}_r$: « tout sous-groupe discret de rang r de $\mathbb{R}^n$ est de la forme $\mathbb{Z}a_1 \oplus \dots \oplus \mathbb{Z}a_r$ où $(a_1, \dots, a_r)$ est une famille libre de $\mathbb{R}^n$ ».*
L'assertion $\mathscr{P}_1$ découle de la structure des sous-groupes discrets de $\mathbb{R}$. En effet, si G est un sous-groupe discret de rang 1 de $\mathbb{R}^n$, on choisit un vecteur directeur e de $\mathrm{Vect}(G)$ et on a que $\{\lambda \in \mathbb{R} : \lambda e \in G\}$ est un sous-groupe discret de $\mathbb{R}$, donc de la forme $a\mathbb{Z}$ avec $a > 0$. Ainsi, $G = \mathbb{Z}(ae)$. Supposons $\mathscr{P}_{r-1}$ vraie. On considère $g_1, \dots, g_r, \ell, h$ comme précédemment. On a vu que $G = \mathbb{Z}h \oplus (\mathrm{Vect}(g_1, \dots, g_{r-1}) \cap G)$. Or $\mathrm{Vect}(g_1, \dots, g_{r-1}) \cap G$ est un sous-groupe discret de rang $r-1$ de $\mathbb{R}^n$. On dispose donc d'une famille libre $(a_2, \dots, a_r)$ telle que $\mathrm{Vect}(g_1, \dots, g_{r-1}) \cap G = \mathbb{Z}a_2 \oplus \dots \oplus \mathbb{Z}a_r$. En posant $a_1 = h$, la famille $(a_1, \dots, a_r)$ est libre et $G = \mathbb{Z}a_1 \oplus \dots \oplus \mathbb{Z}a_r$, ce qui prouve $\mathscr{P}_r$.

$\square$

Si $(a_1, \dots, a_r)$ est libre et si $G = \mathbb{Z}a_1 \oplus \dots \oplus \mathbb{Z}a_r$, on dit que $(a_1, \dots, a_r)$ est une $\mathbb{Z}$-base de G.
On appelle réseau de $\mathbb{R}^n$ tout sous-groupe discret de rang n.

La caractérisation précédente revient à identifier les sous-groupes discrets de $\mathbb{R}^n$ aux groupes $\mathbb{Z}^m$:

Proposition : Un groupe abélien G est isomorphe à $\mathbb{Z}^m$ si et seulement si il existe une famille $(g_1, \dots, g_m)$ de G telle que $G = \mathbb{Z}g_1 \oplus \dots \oplus \mathbb{Z}g_m$.

$\square$ *Si G admet une $\mathbb{Z}$-base $(g_1, \dots, g_m)$, $\varphi : \begin{cases} G & \longrightarrow & \mathbb{Z}^m \\ g = \sum_{i=1}^{m} k_i g_i & \longmapsto & (k_1, \dots, k_m) \end{cases}$ est un isomorphisme.*

Réciproquement, supposons qu'il existe un isomorphisme $\varphi : \mathbb{Z}^m \longmapsto G$. Pour $i \in [\![1,m]\!]$, posons $e_i = \varphi((0,\dots,0,1,0,\dots,0))$ où le 1 est i-ème position. Soit $x \in G$. Notons $\varphi^{-1}(g) = (k_1, \dots, k_m)$. On a $g = \varphi\left(\sum_{k=1}^{m} k_i (0,\dots,0,1,0,\dots,0)\right) = \displaystyle\sum_{k=1}^{m} k_i e_i$

où le 1 *est i-ème position. De plus, si* g *admet deux décompositions* $g = \sum_{k=1}^{m} k_i e_i = \sum_{k=1}^{m} p_i e_i$*, alors en appliquant* φ^{-1}*, on peut identifier coordonnée par coordonnée, ce qui fournit* $k_i = p_i$ *pour tout i.*

$\square$

Un sous-groupe G fermé de $\mathbb{R}^n$ est uniquement déterminé (à isomorphisme près) par la donnée d'un couple (d, r) d'entiers tels que $0 \leqslant d \leqslant r \leqslant n$: on a $G \cong \mathbb{R}^d \times \mathbb{Z}^{r-d}$. En effet, en notant $G = \bigoplus_{i=1}^{d} \mathbb{R} e_i \oplus \bigoplus_{i=d+1}^{r} \mathbb{Z}\varepsilon_i$, l'application $\begin{cases} G & \longrightarrow \quad \mathbb{R}^d \times \mathbb{Z}^{r-d} \\ \sum_{i=1}^{d} t_i e_i + \sum_{j=d+1}^{r} m_j \varepsilon_j & \longmapsto \quad (t_1, \ldots, t_d, m_{d+1}, \ldots, m_r) \end{cases}$ est $\mathbb{Z}$-linéaire et bijective.

Proposition : Soient G un réseau de E, $(a_1, \ldots, a_n)$ une $\mathbb{Z}$-base de G et $(b_1, \ldots, b_n)$ une famille de vecteurs de $\mathbb{R}^n$. Pour $i \in [\![1,n]\!]$, on décompose b_i en $b_i = \sum_{j=1}^{n} p_{ij} a_j$. La famille $(b_1, \ldots, b_n)$ est une $\mathbb{Z}$-base de G si et seulement si $P = (p_{ij})_{i,j \in [\![1,n]\!]} \in \mathscr{GL}_n(\mathbb{Z}) = \{M \in \mathscr{M}_n(\mathbb{Z}) : \det M \in \{-1,1\}\}$.

$\square$ *On sait que* $\mathscr{GL}_n(\mathbb{Z})$ *est l'ensemble des inversibles de* $\mathscr{M}_n(\mathbb{Z})$*. Comme les* b_j *sont dans G et comme* $(a_1, \ldots, a_n)$ *est une* $\mathbb{Z}$ *-base de G, les* p_{ij} *sont dans* $\mathbb{Z}$*. De plus,* $(b_1, \ldots, b_n)$ *est une* $\mathbb{Z}$*-base de G si et seulement si, pour tout* $i \in [\![1,n]\!]$*, on peut écrire* $a_i = \sum_{j=1}^{n} q_{ij} b_j$ *où les* q_{ij} *sont dans* $\mathbb{Z}$*, i.e. s'il existe une matrice* $Q = (q_{ij})_{i,j \in [\![1,n]\!]} \in \mathscr{M}_n(\mathbb{Z})$ *telle que* $PQ = I_n$*. On en déduit le résultat.*

$\square$

$\det(a_1, \ldots, a_n)$ est le volume orienté de la cellule fondamentale. La proposition précédente affirme que deux cellules fondamentales définies par deux $\mathbb{Z}$-bases de G ont même volume (non orienté).

Proposition : On munit l'ensemble des sous-groupes fermés de $\mathbb{R}^n$ de la relation d'équivalence définie par : $G_1 \sim G_2$ si et seulement s'il existe f un automorphisme continu de réciproque continue du groupe $(\mathbb{R}^n, +, \|\cdot\|)$ tel que $f(G_1) = G_2$. Il y a $\dfrac{(n+1)(n+2)}{2}$ classes d'équivalence : elles sont constituées des groupes qui ont le même rang et le même $\mathbf{d}$.

$\square$ *On sait que les endomorphismes continus de* $\mathbb{R}^n$ *sont les éléments de* $\mathscr{L}(\mathbb{R}^n)$*. Soit G un sous-groupe fermé de* $\mathbb{R}^n$*. On a* $G = \mathbb{Z}a_1 \oplus \ldots \oplus \mathbb{Z}a_m \oplus \mathbb{R}b_1 \oplus \ldots \oplus \mathbb{R}b_d$ *où* $(a_1, \ldots, a_m, b_1, \ldots, b_n)$ *est une famille libre de vecteurs de* $\mathbb{R}^n$*. Alors* $\mathrm{rg}(G) = m + d$ *et* $\mathbf{d}(G) = d$*. Considérons* f *un automorphisme continu de* $\mathbb{R}^n$ *i.e. un élément de* $\mathscr{GL}(\mathbb{R}^n)$*. La famille* $f(a_1, \ldots, a_m, b_1, \ldots, b_n)$ *est libre et on a* $f(G) = \mathbb{Z}f(a_1) \oplus \ldots \oplus \mathbb{Z}f(a_m) \oplus \mathbb{R}f(b_1) \oplus \ldots \oplus \mathbb{R}f(b_d)$*. On a donc* $\mathrm{rg}(f(G)) = \mathrm{rg}(G)$ *et* $\mathbf{d}(f(G)) = \mathbf{d}(G)$*.*

Réciproquement, soient G et G′ deux sous groupes fermés de $\mathbb{R}^n$ *tels que* $\mathrm{rg}(G') = \mathrm{rg}(G) = r$ *et* $\mathbf{d}(G') = \mathbf{d}(G) = d$*. Notons* $m = r - d$*. On dispose de deux familles libres* $(a_1, \ldots, a_m, b_1, \ldots, b_d)$ *et* $(a'_1, \ldots, a'_m, b'_1, \ldots, b'_d)$*. On les complète en des bases de* $\mathbb{R}^n$*,* $(a_1, \ldots, a_m, b_1, \ldots, b_d, c_1, \ldots, c_s)$ *et* $(a'_1, \ldots, a'_m, b'_1, \ldots, b'_d, c'_1, \ldots, c'_s)$*. Il existe un unique automorphisme linéaire f envoyant la première base sur la seconde. On a* $f(G) = G'$*. Ainsi,* $G \sim G' \iff (\mathrm{rg}(G), \mathbf{d}(G)) = (\mathrm{rg}(G'), \mathbf{d}(G'))$*.*

L'ensemble des classes d'équivalence est équipotent à l'ensemble des couples (r, d) de $\mathbb{N}^2$ tels que $0 \leqslant d \leqslant r \leqslant n$. Il est fini et de cardinal. $\displaystyle\sum_{r=0}^{n}(r+1) = \frac{(n+1)(n+2)}{2}$.

□

Proposition : Soit $e = (e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$. Soit G un sous-groupe fini de $\mathscr{GL}(\mathbb{R}^n)$ tel que les matrices des éléments de G dans e soient à coefficients rationnels. Il existe une base de $\mathbb{R}^n$ dans laquelle toutes les matrices des éléments de G sont à coefficients entiers.

□ *Notons $G(e) = \{g(e_i) : g \in G,\ e_i \in e\}$. L'ensemble $\mathrm{gr}(G(e))$ est le sous-groupe de $\mathbb{R}^n$ engendré par les colonnes des matrices des éléments de G. On a $\mathrm{gr}(e) = \mathbb{Z}e_1 \oplus \dots \oplus \mathbb{Z}e_n$. Notons d le PPCM des dénominateurs des coefficients des éléments de G (qui sont en nombre fini). On a $d\,\mathrm{gr}(G(e)) \subset \mathrm{gr}(e)$.*
De plus, on a $G(G(e)) = \{g(x) : g \in G,\ x \in G(e)\} = \{gg'(y) : g, g' \in G,\ y \in e\} = G(e)$. Donc $\mathrm{gr}(G(e))$ est stable par tous les éléments de G. De plus, c'est un sous-groupe de $\dfrac{1}{d}\mathrm{gr}(e)$, donc il est isomorphe à un $\mathbb{Z}^r$ où $r \leqslant n$. Fixons $(x_1, \dots, x_r)$ une $\mathbb{Z}$-base de $\mathrm{gr}(G(e))$.
Le sous-espace engendré par $G(e)$ est $\mathrm{Vect}(x_1, \dots, x_r)$. Il est de dimension au plus r. On a $e \subset G(e)$, donc $\mathrm{Vect}(G(e)) = \mathbb{R}^n$. On en déduit que $r = n$. Ainsi, $(x_1, \dots, x_r)$ est une base de $\mathbb{R}^n$. Pour tout $g \in G$, on a $g(x_i) \in \mathrm{gr}(G(e))$, donc $g(x_i)$ est une combinaison linéaire à coefficients entiers des x_j. On en conclut que $\mathrm{Mat}_{(x_1,\dots,x_n)}(g) \in \mathscr{M}_n(\mathbb{Z})$.

□

Proposition : Soit $M \in \mathscr{M}_n(\mathbb{Q})$ une matrice d'ordre fini. On a $\chi_M \in \mathbb{Z}[X]$.

□ *Notons d l'ordre de M. On a $M^{-1} = M^{d-1}$. Notons u l'endomorphisme de $\mathbb{R}^n$ canoniquement associé à M, et G le sous-groupe de $\mathscr{GL}(\mathbb{R}^n)$ engendré par u. On a $G = \{u^k,\ k \in [\![0, d[\![\}$. C'est un ensemble fini. Les matrices dans e des éléments de G sont à coefficients rationnels, donc il existe une base de $\mathbb{R}^n$ dans laquelle les matrices des éléments de G sont à coefficients entiers. En particulier, M est semblable à une matrice à coefficients entiers, donc son polynôme caractéristique est à coefficients entiers.*

□

Dualité sur les sous-groupes de $\mathbb{R}^n$

Si G est un sous-groupe de $\mathbb{R}^n$, on note $G^\circ = \{y \in E : \forall x \in G,\ \langle x, y\rangle \in \mathbb{Z}\}$ l'associé de G.

Proposition : G° est un sous-groupe fermé de $\mathbb{R}^n$.

□ *Pour $x \in \mathbb{R}^n$, l'application $\varphi_x : y \in \mathbb{R}^n \longmapsto \langle x, y\rangle$ est un morphisme de groupes continu. Ainsi, l'image réciproque du sous-groupe fermé $\mathbb{Z}$ de $\mathbb{R}$ est un sous-groupe fermé de $\mathbb{R}^n$. Donc $G^\circ = \displaystyle\bigcap_{x \in G} \varphi_x^{-1}(\mathbb{Z})$ est un sous-groupe fermé de $\mathbb{R}^n$.*

□

Si F est un sous-espace vectoriel de E, on a $F^\circ = F^\perp$. En effet, on a immédiatement $F^\perp \subset F^\circ$. Réciproquement, si $x \in F^\circ$, l'application $\varphi_x|_F$ est une forme linéaire à valeurs dans $\mathbb{Z}$. Elle n'est pas surjective, donc nécessairement nulle. On en déduit que $x \in F^\perp$.

Proposition : G est dense dans $\mathbb{R}^n$ si et seulement si $G^\circ = \{0\}$.

□ *Supposons G dense dans $\mathbb{R}^n$. Soit $x \in G^\circ$. Par continuité de φ_x, $\varphi_x(G)$ est dense dans $\varphi_x(\mathbb{R}^n)$. Si x était non nul, $\varphi_x(G)$ serait dense dans $\mathbb{R} = \varphi_x(\mathbb{R}^n)$, alors que $\varphi_x(G) \subset \mathbb{Z}$. On a donc nécessairement $x = 0$ puis $G^\circ = \{0\}$.*
Réciproquement, supposons G non dense dans $\mathbb{R}^n$ et montrons que $G^\circ \neq \{0\}$. L'ensemble $\mathrm{Adh}(G)$ est un sous-groupe strict de $\mathbb{R}^n$. On a donc $(\mathrm{rg}(\mathrm{Adh}(G)), \mathbf{d}(\mathrm{Adh}(G))) \neq (n, n)$.
Si $\mathrm{rg}(\mathrm{Adh}(G)) \neq n$, alors $\mathrm{Adh}(G)$ est contenu dans un sous-espace strict de $\mathbb{R}^n$. L'orthogonal de ce sous-espace est non nul et contenu dans $\mathrm{Adh}(G)^\circ \subset G^\circ$. En particulier, on a $G^\circ \neq \{0\}$.
Supposons désormais $\mathrm{rg}(\mathrm{Adh}(G)) = n$ et $\mathbf{d}(\mathrm{Adh}(G)) < n$. Il existe une base $(a_1, \dots, a_n)$ de $\mathbb{R}^n$ telle que $\mathrm{Adh}(G) = \mathbb{R}a_1 \oplus \dots \oplus \mathbb{R}a_d \oplus \mathbb{Z}a_{d+1} \oplus \dots \oplus \mathbb{Z}a_n$. On considère la forme linéaire ℓ qui à un vecteur associe sa dernière coordonnée sur $(a_1, \dots, a_n)$. La restriction de ℓ à $\mathrm{Adh}(G)$ est à valeurs dans $\mathbb{Z}$. Le théorème de Riesz assure que ℓ s'écrit φ_x pour un certain $x \in \mathbb{R}^n \backslash \{0\}$. Ainsi, on a $x \in \mathrm{Adh}(G)^\circ \subset G^\circ$, d'où $G^\circ \neq \{0\}$.

□

Théorème : Soit $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$.
Le sous-groupe $\mathbb{Z}^n + \mathbb{R}\alpha$ est dense dans $\mathbb{R}^n$ si et seulement si α est $\mathbb{Q}$-libre.
Le sous-groupe $\mathbb{Z}^n + \mathbb{Z}\alpha$ est dense dans $\mathbb{R}^n$ si et seulement si $(1, \alpha_1, \dots, \alpha_n)$ est $\mathbb{Q}$-libre.

□ *Notons $G = \mathbb{Z}^n + \mathbb{R}\alpha$. On a $x = (x_1, \dots, x_n) \in G^\circ \iff \begin{cases} \forall y \in \mathbb{Z}^n,\ \langle x, y\rangle \in \mathbb{Z} \\ \forall \lambda \in \mathbb{R},\ \lambda\langle x, \alpha\rangle \in \mathbb{Z} \end{cases}$. La première condition est satisfaite si et seulement si $x \in \mathbb{Z}^n$ (prendre pour y les vecteurs de la base canonique). La seconde condition est satisfaite si et seulement si $\langle x, \alpha\rangle = 0$. On a donc $G^\circ = \{0\}$ si et seulement si le seul élément $(x_1, \dots, x_n)$ de $\mathbb{Z}^n$ tel que $x_1\alpha_1 + \dots + x_n\alpha_n = 0$ est $(0,\dots,0)$, ou encore si $(\alpha_1, \dots, \alpha_n)$ est $\mathbb{Q}$-libre. La proposition précédente permet de conclure.*
Notons maintenant $G = \mathbb{Z}^n + \mathbb{Z}\alpha$. Le vecteur x est dans G° si et seulement si il est dans $\mathbb{Z}^n$ et $\langle x, \alpha\rangle \in \mathbb{Z}$. On a donc $G^\circ = \{0\}$ si et seulement si le seul $(n+1)$-uplet $(x_0, \dots, x_n)$ de $\mathbb{Z}^{n+1}$ tel que $x_0 1 + x_1\alpha_1 + \dots + x_n\alpha_n = 0$ est $(0,\dots,0)$, ou encore si $(1, \alpha_1, \dots, \alpha_n)$ est $\mathbb{Q}$-libre.

□

Exemple : Pour $(a_1, \dots, a_n) \in \mathbb{R}_+^n$ et $(\varphi_1, \dots, \varphi_n) \in \mathbb{R}^n$, calculons $\sup\limits_{t \in \mathbb{R}} \sum\limits_{i=1}^{n} a_i \cos(\alpha_i t + \varphi_i)$ où la condition du théorème précédent est vérifiée. On a $f(t) := \sum\limits_{i=1}^{n} a_i \cos(\alpha_i t + \varphi_i) \leqslant \sum\limits_{i=1}^{n} a_i$.

La famille $(\alpha_i/2\pi)_{i \in [\![1,n]\!]}$ est $\mathbb{Q}$-libre. Le théorème précédent assure l'existence d'une suite réelle $(t_k)_{k \in \mathbb{N}^*}$ et d'une suite $(n_k)_{k \in \mathbb{N}^*}$ d'entiers telles que, pour tout i, $\dfrac{t_k}{2\pi}\alpha_i + n_k \underset{k \to +\infty}{\longrightarrow} -\dfrac{\varphi_i}{2\pi}$ ou encore $t_k\alpha_i + 2\pi n_k \underset{k \to +\infty}{\longrightarrow} -\varphi_i$. On a alors : $\forall i \in [\![1,n]\!],\ \cos(\alpha_i t_k + \varphi_i) \underset{k \to +\infty}{\longrightarrow} 1$ puis $f(t_k) \underset{k \to +\infty}{\longrightarrow} \sum\limits_{i=1}^{n} a_i$.

Exemple : $H = \left\{ \left(a + c\sqrt{2},\, b + c\sqrt{3}\right),\, (a,b,c) \in \mathbb{Z}^3 \right\}$ est un sous-groupe dense de $\mathbb{R}^2$. Pour le vérifier, il suffit de montrer que $\left(1,\sqrt{2},\sqrt{3}\right)$ est $\mathbb{Q}$-libre. Soient $a,b,c \in \mathbb{Q}$ tels que $a + b\sqrt{2} + c\sqrt{3} = 0$. On a $a^2 - 2b^2 - 3c^2 = 2bc\sqrt{6}$. Comme $\sqrt{6}$ est irrationnel, on a nécessairement $bc = 0$. Supposons $c = 0$. Si b était non nul, $\sqrt{2}$ serait rationnel. Donc $b = c = 0$ puis $a = 0$. On procède de même si $c = 0$.

Proposition : Soit G un sous-groupe fermé de $\mathbb{R}^n$. On a $\mathbf{d}(G^\circ) = n - \mathrm{rg}(G)$ et $\mathrm{rg}(G^\circ) = n - \mathbf{d}(G)$.

☐ *Soit $(a_1, \dots, a_n)$ une base de $\mathbb{R}^n$ telle que $G = \mathbb{R}a_1 \oplus \dots \oplus \mathbb{R}a_d \oplus \mathbb{Z}a_{d+1} \oplus \dots \oplus \mathbb{Z}a_r$. On considère la base antéduale $(a'_1, \dots, a'_n)$, qui vérifie $\langle a_i, a'_j \rangle = \delta_{i,j}$. Soit $x \in E$. On écrit $x = \sum_{i=1}^{n} x_i a'_i$. On a $x \in G^\circ$ si et seulement si : $\forall i \in [\![1,d]\!],\ \langle a_i, x\rangle = 0$ et $\forall i \in [\![d+1,r]\!],\ \langle a_i, x\rangle \in \mathbb{Z}$.*
Cela revient à dire que : $\forall i \in [\![1,d]\!],\ x_i = 0$ et $\forall i \in [\![d+1,r]\!],\ x_i \in \mathbb{Z}$.
Ainsi, $G^\circ = \mathbb{Z}a'_{d+1} \oplus \dots \oplus \mathbb{Z}a'_r \oplus \mathbb{R}a'_{r+1} \oplus \dots \oplus \mathbb{R}a'_n$. D'où $\mathrm{rg}(G^\circ) = n - \mathbf{d}(G)$ et $\mathbf{d}(G^\circ) = n - \mathrm{rg}(G)$.

☐

Proposition : Si G est un sous-groupe de $\mathbb{R}^n$, on a $(G^\circ)^\circ = G$.

☐ *Supposons d'abord G fermé. On reprend les notations précédentes. On a déjà $G \subset (G^\circ)^\circ$. Fixons $x \in \mathbb{R}^n$. On écrit $x = \sum_{i=1}^{n} x_i a_i$. La description de G° montre que x est dans $(G^\circ)^\circ$ si et seulement si : $\forall i \in [\![d+1,r]\!],\ x_i \in \mathbb{Z}$ et $\forall i \in [\![r+1,n]\!],\ x_i = 0$. Ainsi, $(G^\circ)^\circ = \mathbb{R}a_1 \oplus \dots \oplus \mathbb{R}a_d \oplus \mathbb{Z}a_{d+1} \oplus \dots \oplus \mathbb{Z}a_r = G$.*
Revenons au cas général. Il suffit de montrer que $\mathrm{Adh}(G)^\circ = G^\circ$ pour conclure en utilisant le cas précédent. Comme $G \subset \mathrm{Adh}(G)$, on a $\mathrm{Adh}(G)^\circ \subset G^\circ$. Considérons $x \in G^\circ$. Pour tout $g \in G$, on a $\langle x, g\rangle \in \mathbb{Z}$. La continuité de φ_x et le fait que $\mathbb{Z}$ soit fermé dans $\mathbb{R}$ assurent que l'on a encore $\langle x, h\rangle \in \mathbb{Z}$ pour $h \in \mathrm{Adh}(G)$. D'où $\mathrm{Adh}(G)^\circ = G^\circ$.

☐