Exemple.
$n=1$
$G=\mathbb{Z}$
$f_1=2$
$2\mathbb{Z}\subset G$

Question :

G sous-groupe discret de $\mathbb{R}^n$

$\overset{?}{\Rightarrow}$ G libre de type fini

$f_1, \dots, f_t \in G$, linéairement indépendants sur $\mathbb{R}$, t maximal

$t = \dim_{\mathbb{R}}$ s/e. de $\mathbb{R}^n$ engendré par G.

$H = \mathbb{Z} f_1 + \dots + \underbrace{\mathbb{Z} f_t \subset G}_{\text{indice fini } m} \overset{?}{\subset} \frac{1}{m}(\mathbb{Z} f_1 + \dots + \mathbb{Z} f_t)$ $\quad \exists m \geq 1$

G/H fini

$\forall x \in G$ classe de mx modulo H est $0 \Leftrightarrow mx \in H$

$L \xrightarrow{\sigma_i} N \qquad 1 \leq i \leq n$

$$\left.\begin{array}{c} L \\ \Big| {\scriptstyle n/d} \\ K(\alpha) \\ \Big| {\scriptstyle d} \\ K \end{array}\right) n$$

$(\sigma_i(\alpha))_{1\leq i \leq n}$

$=$ (à l'ordre près) où

$(\underbrace{\alpha_1, \dots, \alpha_d}, \underbrace{\alpha_1, \dots, \alpha_d}, \dots, \underbrace{\alpha_1, \dots, \alpha_d})$ $\quad \frac{n}{d}$ fois

$$\prod_{i=1}^{n} (X - \sigma_i(\alpha)) = \prod_{j=1}^{d} (X - \alpha_j)^{n/d}.$$

Sous-groupes de $\mathbb{R}^n$ (suite).

Sous-groupes discrets :

$G \subset \mathbb{R}^n$ discret $\Rightarrow \exists e_1, \dots, e_t \in G$, linéairement indépendants sur $\mathbb{R}$, tels que $G = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_t$.

Veut dire : pour $0 \leq t \leq n$,

$\mathbb{Z}^t \times \{0\}^{n-t} = \{(a_1, \dots, a_t, 0, \dots, 0) ; a_i \in \mathbb{Z}\}$ est un sous-groupe discret de $\mathbb{R}^n$, on obtient ainsi tous les sous-groupes discrets de $\mathbb{R}^n$ après changement de base de $\mathbb{R}^n$.

Dans un sous-groupe discret de $\mathbb{R}^n$, des éléments sont linéairement indépendants sur $\mathbb{Z}$ ssi ils sont linéairement indépendants sur $\mathbb{R}$.

$G = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_t \subset \mathbb{R}^n \qquad e_i \quad \mathbb{R}$-l.i

$t = \operatorname{rang}_{\mathbb{Z}} G \qquad 0 \leq t \leq n$

V espace vectoriel sur $\mathbb{R}$ de dim. n.

Définition. Réseau (lattice) de $\mathbb{R}^n$ = sous-groupe discret de V de rang n.

Structure des sous-groupes de $\mathbb{R}^n$

G sous-groupe de $\mathbb{R}^n$ $\quad \rho > 0$

V_ρ = sous-espace vectoriel de $\mathbb{R}^n$ engendré par $G \cap B(0,\rho)$

$\rho_1 \leq \rho_2 \Rightarrow V_{\rho_1} \subseteq V_{\rho_2}$.

$$]0,\infty[= \mathbb{R}_{>0} \longrightarrow \mathbb{Z}_{\geq 0}$$
$$\rho \longmapsto \dim V_\rho$$

$V = \bigcap_{\rho>0} V_\rho$

$\dim V_\rho = \dim V_{\rho_0}$

$V = V_{\rho_0} = V_\rho \quad \forall \rho \leq \rho_0 \qquad \rho_0 > 0$

$G' = G \cap V$ est un sous-groupe dense de V.

W le sous-espace de $\mathbb{R}^n$ engendré par G.

$V \subset W$ On choisit V' un supplémentaire de V dans W $\quad W = V \oplus V' \xrightarrow{p} V'$

$\ker p = V \qquad p|_{V'} = id_{V'}$.

On va montrer que $p(G)$ est un sous-groupe discret de V'. Soit $z \in p(G)$, $|z| < \varepsilon$

$\varepsilon = \rho_0/2$. But : $z = 0$.

$z \in p(G) \qquad |z| < \varepsilon = \rho_0/2$.

$p : W = V \oplus V' \to V'$

$z = p(w) \qquad w \in G$.

$u = z - w \qquad p(u) = p(z) - p(w) = z - z = 0$

$u \in V \qquad G' = G \cap V$ dense dans V

$\exists w' \in G', \quad |w' + u| < \varepsilon$.

$$|w - w'| \leq |\underset{\overset{\|}{z}}{w+u}| + |u + w'| < 2\varepsilon = \rho_0$$

$w, w' \in G \qquad w - w' \in G$. $\quad |w - w'| < \rho_0 \Rightarrow$

$w - w' \in V \cap G = G'$

$p(w - w') = 0 = p(w) = z \qquad \Rightarrow z = 0$

Donc $p(G)$ est un sous-groupe discret de V' $\quad \exists y_1, \dots, y_t \in V'$, linéairement indépendants sur $\mathbb{R}$, tels que $p(G) = \mathbb{Z}y_1 + \dots + \mathbb{Z}y_t$.

$y_j = p(z_j) \qquad z_j \in G. \qquad 1 \leq j \leq t$.

$G'' = \mathbb{Z}z_1 + \dots + \mathbb{Z}z_t \subset G$

$z_1, \dots, z_t$ $\mathbb{R}$-l-i $\quad \Rightarrow G''$ discret dans $\mathbb{R}^n$

$$\underset{\underset{G}{\cup}}{W} = V \oplus V' \qquad G = G' \oplus G''.$$

V est le plus grand sous-espace vectoriel de $\mathbb{R}^n$ contenu dans l'adhérence de G

$V \subset \overline{G}$ adh. de G. ($G \cap V$ est dense dans V)

$\mathbb{R}t \subset \overline{G} \overset{?}{\Longrightarrow} t \in V$

$G = G' \oplus G''$ $\quad p(\mathbb{R}t) \subset G'' \subset \mathbb{R}^n$

$\cup$

$\mathbb{R}t$

$\underbrace{}_{\text{discret}}$

$p(\mathbb{R}t) = 0 \Rightarrow \mathbb{R}t \subset V$

Proposition. G sous-groupe de $\mathbb{R}^n$. Il existe un sous-espace vectoriel V de $\mathbb{R}^n$ maximal contenu dans l'adhérence $\overline{G}$ de G. Alors $G' = G \cap V$ est dense dans V et il existe un sous-groupe G'' de G, discret dans $\mathbb{R}^n$, tel que $G = G' \oplus G''$.

Cas particulier où G est fermé $\overline{G} = G$, $G' = V$

$G = V \oplus G''$, V sous-espace vectoriel de $\mathbb{R}^n$ G'' discret dans $\mathbb{R}^n$.

Exercice. $G = \mathbb{Z}^2 + \mathbb{Z}(\sqrt{2}, \sqrt{3})$ est dense dans $\mathbb{R}^2$

$G = \{ (a_1 + b\sqrt{2}, a_2 + b\sqrt{3}) ; (a_1, a_2, b) \in \mathbb{Z}^3 \}$

rang 3. $\quad G \simeq \mathbb{Z}^3$

$\forall \ (x_1, x_2) \in \mathbb{R}^2, \ \forall \varepsilon > 0 \ \exists \ a_1, a_2, b \in \mathbb{Z}$

$|x_1 - a_1 - b\sqrt{2}| < \varepsilon$ et $|x_2 - a_2 - b\sqrt{3}| < \varepsilon$.

$1, \sqrt{2}, \sqrt{3}$ sont linéairement indépendants sur $\mathbb{Q}$.

Lemme. V un sous-espace vectoriel de $\mathbb{R}^n$, G un sous-groupe discret de $\mathbb{R}^n$ contenu dans V. Alors G est un réseau de V (G engendre V comme $\mathbb{R}$-espace vectoriel) $\Longleftrightarrow$ $\exists B \subset V$, borné, tel que

$$V = \bigcup_{g \in G} (g + B).$$

$V = \mathbb{R}^n$

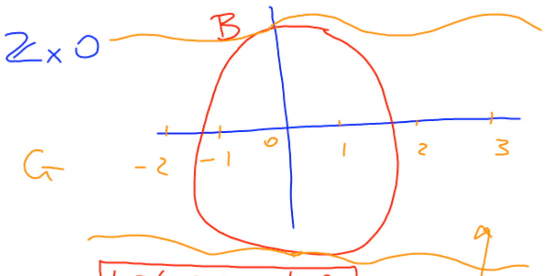
$G = \mathbb{Z}^t \times (0)^{n-t}$

$t = n \Leftrightarrow$

$B = [0,1]^n \quad g = (a_1, \dots, a_t, 0, \dots, 0) \in G$

$g + B = \mathbb{R}^t \times [0,1]^{n-t} \ . = \mathbb{R}^n \Longleftrightarrow n = t.$

$n = 2 \qquad G = \mathbb{Z} \times 0$



$g + B$

$t = t_1 e_1 + \dots + t_d e_d$
$t_i \in \mathbb{R}$
$g = [t_1] e_1 + \dots + [t_d] e_d$
$t - g \in B$

$\bigcup_{g \in G} g + B$

Démonstration.

Si G engendre V

$e_1, \dots, e_d$ base de V, $e_i \in G$.

$$B = \{ x_1 e_1 + \dots + x_d e_d \; ; \; x_i \in \mathbb{R}, \; 0 \leq x_i < 1, \; 1 \leq i \leq d \}$$

Alors $V = \bigcup_{g \in G} (g + B)$

Inversement si $G \subset V' \subsetneq V$

W un supplémentaire $\quad p : V \longrightarrow W$

pour $g \in G$,

$p(g + B) \subset p(B)$ borné

$$p\Big(\bigcup_{g \in G} g + B \Big) \subset p(B) \neq W.$$

alors que $p(V) = W$.

Géométrie des nombres de Minkowski.

G réseau de $\mathbb{R}^n$.

$\exists \, e_1, \dots, e_n$ base de $\mathbb{R}^n$,

$G = \mathbb{Z} e_1 + \dots + \mathbb{Z} e_n$.

changement de base : matrice coeff. $\in \mathbb{Z}$ dét. ± 1.

$\underline{\underline{e}} = (\underline{e_1}, \dots, \underline{e_n})$ base de $\mathbb{R}^n$

$\underline{e_i} \in G \subset \mathbb{R}^n$

$$P_{\underline{\underline{e}}} = \{ x_1 e_1 + \dots + x_n e_n \in \mathbb{R}^n \; ; \; x_1, \dots, x_n \in \mathbb{R}, \; 0 \leq x_i < 1 \}$$

domaine fondamental.

bijection $\mathbb{R}^n / G \longrightarrow P_{\underline{\underline{e}}}$

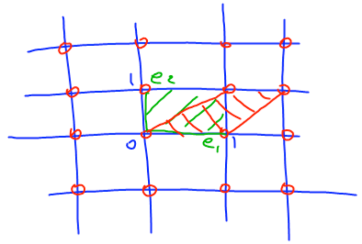
$$\mathbb{R}^n \longrightarrow P_{\underline{\underline{e}}}$$

$$t_1 e_1 + \dots + t_n e_n \longmapsto \sum_{i=1}^{n} \{t_i\} e_i$$

$t_i = [t_i] + \{t_i\}$, $\quad [t_i] \in \mathbb{Z}$, $\quad \{t_i\} \in [0, 1)$

$\mathbb{R}^n = \bigcup_{g \in G} (g + P_{\underline{\underline{e}}})$ partition réunion disjointe.

$G = \mathbb{Z}^2 \subset \mathbb{R}^2$



$e_1 = (1, 0)$
$e_2 = (0, 1)$

$f_1 = (1, 0)$
$f_2 = (1, 1)$

Si $\underline{e}$ et $\underline{\underline{f}}$ sont deux bases de G

$$\mu(P_{\underline{\underline{e}}}) = \mu(P_{\underline{\underline{f}}}) := \text{volume de } G = v(G).$$

μ mesure de Lebesgue.