Titre : **Générateurs de $O(E)$ et $SO(E)$**
Recasages : 106, 108, 160, 161
Thème : Algèbre linéaire, théorie des groupes, produit scalaire.
Références : Perrin, cours d'algèbre (p. 187-188)

On fixe $(E, (.,.))$ un $\mathbb{K}$-espace vectoriel euclidien de dimension n finie, on note $\|.\|$ la norme associée au produit scalaire.

Théorème 1. *Le groupe orthogonal $O(E)$ est engendré par les réflexions. Plus précisément, tout élément de $O(E)$ est produit d'au plus n réflexions.*

Soit $u \in O(E)$, on considère $F_u := \text{Ker }(u - Id)$ et $p_u := n - \dim F_u$. On prouve par récurrence sur p_u que u est un produit d'au plus p_u réflexions.
Le cas $p_u = 0$ est clair : on a alors $F_u = E$ et $u = Id$ soit un produit de 0 réflexions.
Pour $p_u > 0$, notre hypothèse de récurrence est :

$$\forall a \in O(E) \mid p_a < p_u, a \text{ est produit d'au plus } p_a \text{ réflexions}$$

Comme $p_u > 0$, on peut choisir $x \in F_u^{\perp} \setminus \{0\}$, on pose $y = u(x)$. Comme F_u est stable par u (c'est un espace propre) et $u \in O(E)$, son orthogonal $F_u^{\perp}$ est aussi stable par u, donc $y \in F_u^{\perp}$. Comme $u \in O(E)$, on a $\|y\| = \|x\|$, donc

$$(x - y, x + y) = (x, x) - (y, x) + (x, y) - (y, y) = \|x\|^2 - \|y\|^2 = 0$$

On considère τ la réflexion qui fixe $E^+ := \langle x - y \rangle^{\perp}$ et retourne $E^- := \langle x - y \rangle$, ceci est bien défini car $y \neq x$ (en effet, $x \in F_u^{\perp} \setminus \{0\}$ entraîne $x \notin F_u$). De plus, comme $x + y \in \langle x - y \rangle^{\perp}$, on a

$$\begin{cases} \tau(x - y) = y - x = \tau(x) - \tau(y) \\ \tau(x + y) = x + y = \tau(x) + \tau(y) \end{cases}$$

Donc $\tau(y) = \tau(u(x)) = x$ et $x \in F_{\tau u}$. Comme $x - y \in F_u^{\perp}$, on a $E^- \subset F_u^{\perp}$ et en passant à l'orthogonal, $F_u \subset E^+$, donc $\tau_{|F_u} = Id_{F_u}$: donc pour $z \in F_u$, on a $\tau(z) = z$ et $z \in F_{\tau u}$. Ainsi, $F_u \subset F_{\tau u}$ mais cette inclusion est stricte car $x \in F_{\tau u} \cap F_u^{\perp}$. Donc $p_{\tau u} < p_u$, donc τu est un produit d'au plus $p_{\tau u}$ réflexions. Ainsi, u est un produit d'au plus $p_{\tau u} + 1 \leqslant p_u$ réflexions.

Théorème 2. *Le groupe spécial orthogonal $SO(E)$ est engendré par les renversements pour $n \geqslant 3$.*

On prouve le lemme suivant

Lemme 3. *Pour $n \geqslant 3$, si τ_1 et τ_2 sont deux réflexions, il existe σ_1 et σ_2 des renversements tels que*

$$\tau_1 \tau_2 = \sigma_1 \sigma_2$$

Démonstration. Si $n = 3$, alors $-\tau_1$ et $-\tau_2$ sont des renversements : dans une bonne base, la matrice d'une réflexion s'écrit

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

et donc celle de $-\tau_1$ s'écrit

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

qui est bien la matrice d'un renversement et $\sigma_1 = -\tau_1$ et $\sigma_2 = -\tau_2$ conviennent.
Si $n > 3$, notons H_1 et H_2 les hyperplans fixés par τ_1 et τ_2 (respectivement), comme $n > 3$, il existe $V \subset H_1 \cap H_2$ de dimension $n-3 \geqslant 1$. Donc $(\tau_1\tau_2)_{|V} = Id_V$. Comme $\tau_1\tau_2$ est un élément de $O(E)$, $V^\perp$ est stable par $\tau_1\tau_2$. Ainsi, $V^\perp$ est de dimension 3 et on retrouve le premier cas : il existe $\sigma_1, \sigma_2 \in O(V^\perp)$ des renversements tels que $\sigma_1\sigma_2 = (\tau_1\tau_2)_{|V^\perp}$. On pose $\widetilde{\sigma_1} = Id_V \oplus \sigma_1$ et $\widetilde{\sigma_2} = Id_V \oplus \sigma_2$, ce sont des renversements de $O(E)$ et on retrouve $\widetilde{\sigma_1}\widetilde{\sigma_2} = \tau_1\tau_2$, soit le résultat voulu. $\square$

Soit $u \in SO(E)$, par le théorème précédent, u s'écrit comme un produit $\tau_1 \cdots \tau_k$ de réflexions. Comme $\det(\tau_i) = -1$, on obtient $1 = \det(u) = (-1)^k$ et k est pair, le lemme appliqué aux produits successifs $\tau_i\tau_{i+1}$ donne alors le résultat.