MT242, Cours n° 17, Lundi 17 Avril 2000.

Rappel : diagonalisation des matrices hermitiennes. On dit que A est hermitienne si A est une matrice carrée de taille $n \times n$ à coefficients complexes telle que $\mathrm{A}_{j,i} = \overline{\mathrm{A}_{i,j}}$ pour tous $i, j = 1, \ldots, n$.

Théorème. *Si* A *est hermitienne, ses valeurs propres sont réelles et il existe une base* $\mathbb{C}$*-orthonormée de* $\mathbb{C}^n$ *formée de vecteurs propres de* A*.*

Rappel : endomorphisme symétrique, matrices symétriques. Soient E un espace euclidien de dimension finie et a un endomorphisme de E ; on dit que a est un *endomorphisme symétrique* si

$$\forall v, w \in \mathrm{E}, \quad a(v) \,.\, w = v \,.\, a(w).$$

La matrice de a dans toute base orthonormée de E est alors symétrique. Inversement, si la matrice de a dans *une* base orthonormée est symétrique, l'endomorphisme a est symétrique.

Lemme 4.2.1. *Si a est symétrique sur un espace euclidien* E *de dimension finie* > 0*, il existe au moins un vecteur propre pour a : il existe* $v \in \mathrm{E}$, $v \neq 0_{\mathrm{E}}$ *et* $a(v) = \lambda v$ *pour un* $\lambda \in \mathbb{R}$*.*

Démonstration. Soit $\mathbf{e}$ une base orthonormée de E et soit A la matrice de a dans cette base. Le polynôme caractéristique de a est le polynôme caractéristique de A, qui est une matrice symétrique réelle, donc hermitienne. Ce polynôme est de degré $n = \dim \mathrm{E} > 0$, donc il a des racines, qui sont réelles d'après les rappels ci-dessus. Soit $\lambda \in \mathbb{R}$ une telle racine. Alors $\det(a - \lambda \mathrm{I}d_{\mathrm{E}}) = 0$, donc $a - \lambda \mathrm{I}d_{\mathrm{E}}$ n'est pas injectif, donc il existe un vecteur $v \in \mathrm{E}$ non nul tel que $(a - \lambda \mathrm{I}d_{\mathrm{E}})(v) = 0$.

Théorème 4.2.2. Diagonalisation des endomorphismes symétriques. *Soit* E *un espace euclidien de dimension finie* > 0 *; si* $a \in \mathcal{L}(\mathrm{E})$ *est symétrique, les racines du polynôme caractéristique de a sont réelles et on peut trouver une base orthonormée de* E *formée de vecteurs propres de a.*

Démonstration. On raisonne par récurrence sur la dimension $n = \dim \mathrm{E}$. Le résultat est évident quand $n = 1$. On suppose le résultat vrai pour la dimension $n-1$ et on considère un endomorphisme symétrique a de E, avec $\dim \mathrm{E} = n$. D'après le lemme précédent, on peut trouver un vecteur propre f_0 de a, et on vérifie que $f_0^\perp$ est stable par a ; en effet, si w est orthogonal à f_0, on a

$$a(w) \,.\, f_0 = w \,.\, a(f_0) = \lambda \, w \,.\, f_0 = 0$$

ce qui montre que $w \in f_0^\perp$. Le sous-espace $\mathrm{E}' = f_0^\perp$ est de dimension $n-1$, et la restriction a' de a à E′ est un endomorphisme symétrique de E′. D'après l'hypothèse de récurrence, il existe une base orthonormée $(f_1', \ldots, f_{n-1}')$ de E′ formée de vecteurs propres de a', c'est à dire de vecteurs propres de a. Le système de vecteurs $(f_0, f_1', \ldots, f_{n-1}')$ est alors une base orthonormée de E formée de vecteurs propres de a.

Point de vue matriciel ; changement de base orthonormée

Soient $\mathbf{e}$ et $\mathbf{f}$ deux bases orthonormées d'un espace euclidien E de dimension finie $n > 0$. La matrice de passage P de la base $\mathbf{e}$ à la base $\mathbf{f}$ est formée en plaçant en colonne les coordonnées des "nouveaux" vecteurs f_j par rapport à "l'ancienne" base $\mathbf{e}$. La $j$ème colonne de P contient donc les coordonnées du vecteur f_j dans la base $\mathbf{e}$, c'est à dire les nombres $f_j \,.\, e_i$, pour $i = 1, \ldots, n$. On a donc

$$\mathrm{P}_{i,j} = f_j \,.\, e_i$$

pour $i, j = 1, \ldots, n$. La matrice inverse $\mathrm{Q} = \mathrm{P}^{-1}$ est la matrice de passage de la base $\mathbf{f}$ à la base $\mathbf{e}$; en appliquant le même raisonnement, en échangeant simplement les rôles de $\mathbf{e}$ et $\mathbf{f}$, on voit que $\mathrm{Q}_{i,j} = e_j \,.\, f_i = \mathrm{P}_{j,i}$. Donc :

si P *est une matrice de changement de base orthonormée, on a* $\mathrm{P}^{-1} = {}^t\mathrm{P}$.

Définition 4.2.4. On dit qu'une matrice carrée réelle U est *orthogonale* si elle est inversible et si $\mathrm{U}^{-1} = {}^t\mathrm{U}$.

Si U est de taille $n \times n$, il suffit de savoir que ${}^t\mathrm{U}\,\mathrm{U} = \mathrm{I}_n$, ou bien que $\mathrm{U}\,{}^t\mathrm{U} = \mathrm{I}_n$. On peut voir directement par le calcul que U est une matrice orthogonale si et seulement si les colonnes de la matrice U forment une base orthonormée de $\mathbb{R}^n$.

Exemple. Rotation dans $\mathbb{R}^2$: la matrice

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$$

est orthogonale pour tout θ.

Le théorème de diagonalisation se traduit ainsi :

Théorème 4.2.3. Diagonalisation des matrices réelles symétriques. *Soit* A *une matrice réelle symétrique de taille* $n \times n$, $n > 0$ *; il existe une matrice orthogonale* U *et une matrice diagonale réelle* Δ *telles que*

$$\mathrm{A} = {}^t\mathrm{U}\,\Delta\,\mathrm{U}.$$

Endomorphismes symétriques et formes quadratiques

Soit a un endomorphisme symétrique d'un espace euclidien E ; on définit à partir de a une forme bilinéaire symétrique β sur $\mathrm{E} \times \mathrm{E}$ en posant

$$\beta(v, w) = a(v) \,.\, w = v \,.\, a(w) = \beta(w, v)$$

pour tous $v, w \in \mathrm{E}$. On pose ensuite $\mathrm{Q}(v) = \beta(v, v)$ pour tout $v \in \mathrm{E}$. Si $\mathbf{e}$ est une base orthonormée de E, la matrice A de a dans $\mathbf{e}$ est aussi la matrice de la forme quadratique Q dans la base $\mathbf{e}$.

Inversement, si Q est une forme quadratique sur un espace euclidien E de dimension finie, il existe un endomorphisme symétrique $a \in \mathcal{L}(\mathrm{E})$ tel que $\mathrm{Q}(v) = a(v) \,.\, v$ pour tout $v \in \mathrm{E}$ (non détaillé à l'amphi ; il suffit de prendre l'endomorphisme a dont la matrice dans une base orthonormée de E est la matrice de Q dans cette même base).

Proposition 4.2.1. *Soit* Q *une forme quadratique sur un espace euclidien de dimension finie* $n > 0$. *Il existe une base orthonormée* $(e_1, \ldots, e_n)$ *de* E *et des nombres réels* (λ_i) *tels que*

$$\mathrm{Q}(v) = \sum_{i=1}^{n} \lambda_i \,(v \,.\, e_i)^2 \quad \textit{soit encore} \quad \mathrm{Q} = \sum_{i=1}^{n} \lambda_i \,(e_i^*)^2.$$

Démonstration. Soit a l'endomorphisme symétrique tel que $Q(v) = a(v) . v$ pour tout $v \in E$; on peut trouver une base orthonormée $(e_1, \ldots, e_n)$ de E telle que $a(e_i) = \lambda_i e_i$ pour $i = 1, \ldots, n$. Si $v = \sum_{i=1}^n x_i e_i$, on voit que $a(v) = \sum_{i=1}^n \lambda_i x_i e_i$, donc

$$Q(v) = a(v) . v = \sum_{i=1}^n \lambda_i x_i^2 = \sum_{i=1}^n \lambda_i (v . e_i)^2.$$

Différence avec la méthode de Gauss ordinaire : on vient d'exprimer Q comme combinaison linéaire de carrés de formes linéaires indépendantes, mais le résultat obtenu ici est plus particulier que la décomposition de Gauss ordinaire, parce que la base qui est Q-orthogonale est *en même temps* orthogonale pour le produit scalaire usuel. De plus, le résultat obtenu ici demande des méthodes différentes. Pour pouvoir diagonaliser, il faut trouver des racines pour le polynôme caractéristique de a. On ne sait pas en général trouver explicitement les racines d'un polynôme de degré ≥ 5. En revanche la méthode de Gauss ordinaire donne des résultats explicites, qui ne demandent que des opérations élémentaires d'addition, multiplication et division.

Exemple. Considérons le sous-ensemble de $\mathbb{R}^2$ d'équation $(x + y)^2 + (2x + y)^2 = 1$. Il s'agit d'une ellipse. L'expression donnée dans l'équation est déjà une décomposition de Gauss pour la forme quadratique $Q(x, y) = (x + y)^2 + (2x + y)^2$, mais la décomposition orthogonale donnerait une information supplémentaire qui ne se voit pas directement sur l'équation précédente : elle donnerait les *axes* de l'ellipse, qui sont les deux droites orthogonales correspondant respectivement à la plus grande et à la plus petite section de l'ellipse par les droites passant par $(0, 0)$.

Encadrement de $Q(v)$

Soit a l'endomorphisme symétrique tel que $Q(v) = a(v) . v$ pour tout $v \in E$. Rangeons les valeurs propres de a en une suite croissante $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$. On obtient alors à partir de la proposition précédente l'encadrement

$$\lambda_1 \|v\|^2 \leq Q(v) \leq \lambda_n \|v\|^2$$

pour tout $v \in E$.

Il en résulte que $Q(v) \geq 0$ pour tout $v \in E$ si et seulement si toutes les valeurs propres de a sont ≥ 0. On peut aussi vérifier que la forme quadratique Q est définie positive sur l'espace E si et seulement si toutes les valeurs propres de a sont > 0.

4.3. Isométries d'un espace euclidien

Soit T une application (qu'on ne suppose pas linéaire *a priori*) d'un espace euclidien E dans un autre espace euclidien F ; on dit que T *conserve les distances* si

$$d(T(A), T(B)) = d(A, B)$$

pour tous "points" A, B de E (les éléments de E sont aussi des vecteurs, et on peut écrire la conservation de la distance sous la forme $\|T(B) - T(A)\| = \|B - A\|$ pour tous $A, B \in E$).

Proposition 4.3.1. *Soient* E *et* F *deux espaces euclidiens ; si* $T : E \to F$ *conserve les distances, c'est la composition d'une application linéaire isométrique de* E *dans* F *et d'une translation dans* F.

Démonstration. En composant T avec la translation dans F de vecteur $-\mathrm{T}(0_{\mathrm{E}})$ on se ramène au cas $\mathrm{T}(0_{\mathrm{E}}) = 0_{\mathrm{F}}$. On se donne $s \in]0,1[$. On montrera plus loin que

$$(*) \qquad s\, d^2(\mathrm{M},\mathrm{A}) + (1-s)\, d^2(\mathrm{M},\mathrm{B}) - s(1-s)\, d^2(\mathrm{A},\mathrm{B}) = d^2\big(\mathrm{M}, s\mathrm{A} + (1-s)\mathrm{B}\big)$$

pour tout triplet A, B, M de points d'un espace euclidien. En appliquant cette relation aux images, et en utilisant la conservation de la distance, on aura

$$d^2\big(\mathrm{T}(\mathrm{M}), s\mathrm{T}(\mathrm{A}) + (1-s)\mathrm{T}(\mathrm{B})\big) =$$

$$s\, d^2(\mathrm{T}(\mathrm{M}),\mathrm{T}(\mathrm{A})) + (1-s)\, d^2(\mathrm{T}(\mathrm{M}),\mathrm{T}(\mathrm{B})) - s(1-s)\, d^2(\mathrm{T}(\mathrm{A}),\mathrm{T}(\mathrm{B})) =$$

$$s\, d^2(\mathrm{M},\mathrm{A}) + (1-s)\, d^2(\mathrm{M},\mathrm{B}) - s(1-s)\, d^2(\mathrm{A},\mathrm{B}) = d^2\big(\mathrm{M}, s\mathrm{A} + (1-s)\mathrm{B}\big).$$

Si on applique à $\mathrm{M} = s\mathrm{A} + (1-s)\mathrm{B}$, on en déduit que T préserve les barycentres,

$$\mathrm{T}(s\mathrm{A} + (1-s)\mathrm{B}) = s\mathrm{T}(\mathrm{A}) + (1-s)\mathrm{T}(\mathrm{B}).$$

Ensuite si $v = \overrightarrow{0_{\mathrm{E}}\mathrm{M}}$, la relation $\mathrm{T}((1-s)0_{\mathrm{E}} + s\mathrm{M}) = (1-s)\mathrm{T}(0_{\mathrm{E}}) + s\mathrm{T}(\mathrm{M})$ donne l'homogénéité $\mathrm{T}(sv) = s\mathrm{T}(v)$ pour $0 < s < 1$; des petites manipulations donnent ensuite $\mathrm{T}(sv) = s\mathrm{T}(v)$ pour $s \geq 1$, puis pour $s < 0$, donc $\mathrm{T}(sv) = s\mathrm{T}(v)$ pour tout $s \in \mathbb{R}$. Enfin

$$\mathrm{T}(v+w) = 2\,\mathrm{T}\Big(\frac{1}{2}(v+w)\Big) = 2\Big(\frac{\mathrm{T}(v) + \mathrm{T}(w)}{2}\Big) = \mathrm{T}(v) + \mathrm{T}(w)$$

permet de conclure que T est linéaire.

On a fait de la démonstration de la relation $(*)$ un prétexte pour un exercice de calcul différentiel. On traduit la relation $(*)$ en notations vectorielles : si on pose $f(v) = s\|v-a\|^2 + (1-s)\|v-b\|^2 - \|v-(sa+(1-s)b)\|^2$, il faut voir que $f(v) = s(1-s)\|b-a\|^2$; on montre que la fonction f a un gradient nul en tout point $v \in \mathrm{E}$. Elle est donc constante. On trouve la valeur de la constante en prenant par exemple $v = b$.

Cours n° 18, Mercredi 19 Avril 2000.

Isométries linéaires

Définition 4.3.1. Soient E un espace euclidien de dimension finie et u un endomorphisme de E ; on dit que u est un *endomorphisme orthogonal*, ou bien une *isométrie* si

$$\|u(v)\| = \|v\|$$

pour tout $v \in \mathrm{E}$.

Puisque u est linéaire, il en résulte que pour tous $v, w \in \mathrm{E}$,

$$d(u(v), u(w)) = \|u(v) - u(w)\| = \|u(v-w)\| = \|v-w\| = d(v,w),$$

donc u conserve les distances. La relation $\|u(v)\| = \|v\|$ pour tout $v \in \mathrm{E}$ signifie que $v \,.\, v = u(v) \,.\, u(v)$ pour tout $v \in \mathrm{E}$. On obtient alors par polarisation

$$w \,.\, v = u(w) \,.\, u(v)$$

pour tous $v, w \in \mathrm{E}$, ce qui montre la propriété importante suivante : toute application isométrique conserve le produit scalaire. En particulier, des vecteurs orthogonaux ont des images orthogonales.

Toute isométrie u est injective : si $u \neq 0_{\mathrm{E}}$, alors $\|u\| > 0$ et $\|u(v)\| = \|v\| > 0$ montre que $u(v) \neq 0_{\mathrm{E}}$. Il en résulte que u est bijective, puisque E est de dimension finie. L'application identique Id_{E} est un exemple évident d'isométrie de E.

Soient E un espace euclidien de dimension finie et u une isométrie de E ; on vient de dire que u est un isomorphisme. Il est clair que l'application u^{-1} est aussi une isométrie. Si v est une autre isométrie, il est immédiat que la composition $v \circ u$ est une isométrie. Il résulte de ces remarques que l'ensemble des isométries de E, muni de l'opération de composition des applications, est un groupe. On le note O(E), et on l'appelle le *groupe orthogonal* de l'espace euclidien E.

Proposition 4.3.2. *Soit* E *un espace euclidien de dimension finie* > 0 *;*

si u *est une isométrie de* E *et si* $\mathbf{e}$ *est une base orthonormée de* E*, la matrice* U *de* u *dans la base* $\mathbf{e}$ *est une matrice orthogonale ;*

si $u \in \mathcal{L}(\mathrm{E})$*, si* $\mathbf{e}$ *est une base orthonormée de* E *et si la matrice* U *de* u *dans la base* $\mathbf{e}$ *est orthogonale, alors* u *est une isométrie.*

Démonstration. Commençons par le deuxième point. On suppose U orthogonale. Soient v un vecteur de E et X la matrice colonne de ses coordonnées dans la base $\mathbf{e}$; alors UX est la matrice colonne des coordonnées de $u(v)$ dans $\mathbf{e}$. On a vu que les carrés scalaires peuvent s'exprimer matriciellement (par la formule $v \,.\, v = {}^t\mathrm{X}\,\mathrm{X}$), donc

$$u(v) \,.\, u(v) = {}^t(\mathrm{UX})\mathrm{UX} = {}^t\mathrm{X}\,{}^t\mathrm{U}\mathrm{U}\mathrm{X} = {}^t\mathrm{X}\,\mathrm{X} = v \,.\, v$$

pour tout $v \in \mathrm{E}$, ce qui montre que u est isométrique.

Inversement, si u est une isométrie, si $n = \dim \mathrm{E}$, si X, Y sont deux vecteurs colonne quelconques de $\mathbb{R}^n$, soient v, w les vecteurs de E qui ont pour coordonnées respectives dans la base orthonormée $\mathbf{e}$ les vecteurs colonne X et Y ; on peut traduire la relation $v \,.\, w = u(v) \,.\, u(w)$ par

$${}^t\mathrm{X}\,\mathrm{Y} = {}^t(\mathrm{UX})\,\mathrm{UY} = {}^t\mathrm{X}({}^t\mathrm{U}\,\mathrm{U})\mathrm{Y}.$$

Ceci étant vrai pour tous les vecteurs colonne X et Y, on en déduit que ${}^t\mathrm{U}\,\mathrm{U} = \mathrm{I}_n$ (prendre pour X et Y les vecteurs de la base canonique de $\mathbb{R}^n$).

Déterminant, valeurs propres des isométries

La matrice $\mathrm{U} = \mathrm{mat}_{\mathbf{e}}(u)$ d'un endomorphisme orthogonal u dans une base orthonormée $\mathbf{e}$ quelconque de E est une matrice orthogonale, on aura donc

$$\det u = \det \mathrm{U} = \pm 1$$

parce que $(\det \mathrm{U})^2 = \det({}^t\mathrm{U}\mathrm{U}) = \det \mathrm{I}_n = 1$. Soit maintenant λ une valeur propre du polynôme caractéristique de u (qui est égal au polynôme caractéristique de U) ; il existe un vecteur colonne complexe non nul Z tel que $\mathrm{UZ} = \lambda \mathrm{Z}$. On a alors

$$\lambda\overline{\lambda}\langle \mathrm{Z}, \mathrm{Z}\rangle = \langle \mathrm{UZ}, \mathrm{UZ}\rangle = {}^t(\mathrm{UZ})\overline{(\mathrm{UZ})} = {}^t\mathrm{Z}\,{}^t\mathrm{U}\mathrm{U}\overline{\mathrm{Z}} = {}^t\mathrm{Z}\overline{\mathrm{Z}} = \langle \mathrm{Z}, \mathrm{Z}\rangle$$

ce qui montre que $\lambda\overline{\lambda} = 1$ puisque $\langle \mathrm{Z}, \mathrm{Z}\rangle \neq 0$. Il en résulte que les racines du polynôme caractéristique de U sont toutes de module 1. En particulier, les seules possibilités pour les valeurs propres d'un endomorphisme orthogonal u sont ± 1.

Les matrices orthogonales de taille $n \times n$ forment un groupe pour la multiplication des matrices. On le note $\mathrm{O}(n)$, et on l'appelle le *groupe orthogonal*. Les matrices $\mathrm{U} \in \mathrm{O}(n)$ telles que $\det \mathrm{U} = 1$ forment un sous-groupe de $\mathrm{O}(n)$, appelé le *groupe spécial orthogonal*, et noté $\mathrm{SO}(n)$.

Exemples.

1. Rotations de $\mathbb{R}^2$. L'application r_θ de rotation d'angle θ dans $\mathbb{R}^2$ admet pour matrice dans la base canonique

$$\mathrm{R}_\theta = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}.$$

Le déterminant est égal à 1. Les racines du polynôme caractéristique sont $\mathrm{e}^{i\theta}$ et $\mathrm{e}^{-i\theta}$. En particulier, la rotation dans $\mathbb{R}^2$ n'a pas de vecteur propre lorsque $\mathrm{e}^{i\theta}$ n'est pas réel, c'est à dire lorsque $\sin(\theta) \neq 0$. On remarque que la matrice étant réelle, le polynôme caractéristique est à coefficients réels, et les racines non réelles viennent par paires conjuguées.

2. Symétries orthogonales. On considère un sous-espace vectoriel F de E. Pour tout vecteur $v \in \mathrm{E}$, on écrit la décomposition en deux vecteurs orthogonaux

$$v = \mathrm{P}_\mathrm{F} v + \mathrm{P}_{\mathrm{F}^\perp} v,$$

puis on considère le vecteur obtenu en changeant le signe de la composante sur $\mathrm{F}^\perp$,

$$s_\mathrm{F} v = \mathrm{P}_\mathrm{F} v - \mathrm{P}_{\mathrm{F}^\perp} v$$

(à l'amphi, j'ai noté S_F ; finalement j'aime mieux s_F, en réservant les majuscules pour les matrices). L'application ainsi obtenue est linéaire puisque $s_\mathrm{F} = \mathrm{P}_\mathrm{F} - \mathrm{P}_{\mathrm{F}^\perp}$. En utilisant la relation $\mathrm{P}_\mathrm{F} + \mathrm{P}_{\mathrm{F}^\perp} = \mathrm{I}d_\mathrm{E}$ on peut écrire aussi

$$s_\mathrm{F} = \mathrm{P}_\mathrm{F} - \mathrm{P}_{\mathrm{F}^\perp} = 2\mathrm{P}_\mathrm{F} - \mathrm{I}d_\mathrm{E} = \mathrm{I}d_\mathrm{E} - 2\mathrm{P}_{\mathrm{F}^\perp}.$$

Selon les cas, l'une ou l'autre formule est plus pratique pour calculer s_F. L'application s_F est une isométrie, puisqu'en utilisant l'orthogonalité des deux composantes, on a

$$\|s_\mathrm{F} v\|^2 = \|\mathrm{P}_\mathrm{F} v\|^2 + \|\mathrm{P}_{\mathrm{F}^\perp} v\|^2 = \|\mathrm{P}_\mathrm{F} v + \mathrm{P}_{\mathrm{F}^\perp} v\|^2 = \|v\|^2.$$

Par ailleurs il est clair que $s_\mathrm{F}^2 = \mathrm{I}d_\mathrm{E}$, c'est à dire que $s_\mathrm{F}^{-1} = s_\mathrm{F}$. Si on considère la matrice S_F de s_F dans une base orthonormée de E, on aura donc $\mathrm{S}_\mathrm{F}^{-1} = \mathrm{S}_\mathrm{F} = {}^t\mathrm{S}_\mathrm{F}$, donc S_F est à la fois orthogonale et symétrique.

Exercice proposé, non traité. Montrer que si a est un endomorphisme de E qui est à la fois symétrique et isométrique, alors $a = s_\mathrm{F}$ pour un certain sous-espace F (en admettant les deux cas dégénérés $\mathrm{F} = \mathrm{E}$ et $\mathrm{F} = \{0\}$).

3. Réflexions. Il s'agit du cas particulier de la symétrie orthogonale par rapport à un hyperplan. Soit $w \in \mathrm{E}$ un vecteur non nul, et soit $\mathrm{F} = (\mathbb{R}w)^\perp$. Si $n = \dim \mathrm{E}$, on a $\dim \mathrm{F} = n - 1$ puisque w n'est pas nul, et $\mathrm{F}^\perp = \mathbb{R}w$. Ici il est plus simple de calculer $\mathrm{P}_{\mathrm{F}^\perp}$: en posant $w_1 = \|w\|^{-1} w$ on obtient une base orthonormée de $\mathrm{F}^\perp = \mathbb{R}w$, et

$$\mathrm{P}_{\mathrm{F}^\perp} v = (v \,.\, w_1)\, w_1$$

pour tout vecteur $v \in \mathrm{E}$, ce qui donnera en posant $r_w = s_\mathrm{F}$ (à l'amphi, j'ai noté R_w ; même remarque que précédemment)

$$r_w(v) = v - 2\,\frac{v \,.\, w}{\|w\|^2}\, w = v - 2\,\frac{v \,.\, w}{w \,.\, w}\, w.$$

On notera les deux propriétés caractéristiques suivantes : tout vecteur v orthogonal à w reste fixe pour r_w, c'est à dire $r_w(v) = v$, et $r_w(w) = -w$.

Matrice dans la base canonique. Si $w = (w_1, \ldots, w_n) \in \mathbb{R}^n$, la matrice R_w par rapport à la base canonique de la réflexion r_w correspondant au vecteur w a pour coefficients

$$\mathrm{R}_{i,j} = \delta_{i,j} - 2\,\frac{w_i w_j}{\|w\|^2}.$$

Par exemple, si $w = (1, 1, 1) \in \mathbb{R}^3$ on aura

$$\mathrm{R} = \begin{pmatrix} 1/3 & -2/3 & -2/3 \\ -2/3 & 1/3 & -2/3 \\ -2/3 & -2/3 & 1/3 \end{pmatrix}.$$

Isométries de $\mathbb{R}^2$ et de $\mathbb{R}^3$

Le cas de dimension 1 : dans ce cas les seules isométries sont $v \to v$ et $v \to -v$, c'est à dire Id et $-$Id. Le groupe $\mathrm{O}(1)$ est donc le groupe à deux éléments $\{-1, 1\}$, et $\mathrm{SO}(1) = \{1\}$ est le groupe à un seul élément.

Considérons un espace euclidien E de dimension 2 et u une isométrie de E. On sait que le déterminant de u est égal à 1 ou à -1. Etudions d'abord le cas où $\det u = -1$. Le polynôme caractéristique de u est réel de degré deux. Si le produit des racines est -1, il y a deux racines réelles. Les racines réelles sont des valeurs propres, nécessairement égales à 1 ou à -1. Si le produit est égal à -1, il y a une racine 1 et une racine -1, donc u est diagonalisable. Il existe donc une base de vecteurs propres (f_1, f_2) de E telle que

$$u(f_1) = f_1, \quad u(f_2) = -f_2.$$

On voit que les vecteurs f_1 et f_2 sont orthogonaux puisque $-f_1 \,.\, f_2 = u(f_1) \,.\, u(f_2) = f_1 \,.\, f_2$. L'application u est la symétrie orthogonale par rapport à la droite $\mathbb{R} f_1$, c'est à dire la réflexion r_{f_2}.

Supposons maintenant que $\det u = 1$. L'image du vecteur $(1, 0)$ est un vecteur de norme 1, qu'on peut écrire $(\cos\theta, \sin\theta)$. L'image de $(0, 1)$ est un vecteur de norme 1 orthogonal au précédent, donc égal à $\pm(-\sin\theta, \cos\theta)$. Puisque le déterminant est égal à 1 on a nécessairement ici la matrice de la rotation d'angle θ,

$$\mathrm{U} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Le groupe $\mathrm{SO}(2)$ est donc le groupe des rotations de $\mathbb{R}^2$. Il est isomorphe (en tant que groupe bien sûr) au groupe des nombres complexes de module 1, muni de la multiplication.

Le cas de $\mathbb{R}^3$. Soit u une isométrie de $\mathbb{R}^3$; supposons encore que $\det u = 1$. On vérifie qu'alors 1 est nécessairement racine du polynôme caractéristique de u : s'il y a une racine λ non réelle (de module un), les racines seront $\mu \in \mathbb{R}$, λ et $\overline{\lambda}$, donc $1 = \det u = \mu\,|\lambda|^2 = \mu$; d'un autre côté, si les trois racines sont réelles, elles valent ± 1 et le produit 1, il y a donc au moins un 1 dans la liste. Il existe donc un vecteur f_1 (de norme un si on veut) tel que $u(f_1) = f_1$. Alors l'orthogonal F de $\mathbb{R} f_1$ est stable par u : si $v \in \mathrm{F}$, on aura $u(v) \,.\, f_1 = u(v) \,.\, u(f_1) = v \,.\, f_1 = 0$. Si (f_2, f_3) est une base orthonormée de F, la matrice U de u dans la base (f_1, f_2, f_3) est de la forme

$$\mathrm{U} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & u_{2,2} & u_{2,3} \\ 0 & u_{3,2} & u_{3,3} \end{pmatrix}$$

et la matrice U_1 de taille 2×2 qui est dans le coin sud-est est orthogonale, et vérifie $\det U_1 = \det U = 1$. D'après l'étude en dimension 2, on déduit que U_1 est une matrice de rotation. Finalement, u est une rotation de $\mathbb{R}^3$ autour de l'axe $\mathbb{R} f_1$.

Si $\det u = -1$, on peut considérer $-u$ pour déduire qu'il existe maintenant f_1 tel que $u(f_1) = -f_1$ (en effet, $\det(-u) = (-1)^3 \det u = 1$, et on utilise le cas précédent). Si on considère la réflexion r_{f_1} (c'est la symétrie orthogonale autour du plan $F = f_1^{\perp}$), on voit que $r_{f_1} \circ u$ est une isométrie de déterminant 1, qui laisse le vecteur f_1 fixe, donc $r_{f_1} \circ u$ est une rotation autour de la droite $\mathbb{R} f_1$. En résumé, une isométrie u de $\mathbb{R}^3$ est

– ou bien une rotation autour d'un axe : ce cas se produit lorsque $\det u = 1$ (si la rotation est d'angle nul, on obtient simplement l'application identique).

– ou bien une rotation autour d'un axe de vecteur directeur f suivie (ou précédée) de la symétrie autour du plan $f^{\perp}$ orthogonal à l'axe de rotation ; ce cas se produit lorsque $\det u = -1$.

Il résulte de l'étude que les éléments de $SO(3)$ sont exactement les rotations autour d'un axe.

Théorème 4.3.1. *Tout endomorphisme orthogonal u d'un espace euclidien de dimension finie est produit de réflexions.*

Démonstration. On pose $n = \dim E > 0$. On considère le sous-espace vectoriel $F(u)$ de E formé des vecteurs fixes pour u,

$$F(u) = \{v \in E : u(v) = v\}.$$

On va montrer que si $\dim F(u) < n$, c'est à dire si $F(u) \neq E$, on peut trouver une réflexion r_w telle que $\dim F(r_w \circ u) > \dim F(u)$. Une fois ce fait établi, on raisonne ainsi : en partant de $u_0 = u$, on trouvera de proche en proche des réflexions $r_1, \ldots, r_k$ telles que

$$\dim F(u_0) < \dim F(r_1 \circ u) < \ldots < \dim F(r_k \circ \cdots \circ r_1 \circ u).$$

Puisque la dimension de E est finie, on arrivera nécessairement à un moment où on aura $\dim F(r_k \circ \cdots \circ r_1 \circ u) = n = \dim E$, ce qui signifie que tous les vecteurs sont fixes pour $r_k \circ \cdots \circ r_1 \circ u$, c'est à dire que $r_k \circ \cdots \circ r_1 \circ u = \mathrm{Id}_E$, ce qui donne la décomposition de u en produit de réflexions

$$u = r_1 \circ \cdots \circ r_k.$$

Montrons le fait annoncé : on suppose que $F = F(u)$ n'est pas égal à E. On peut donc trouver un vecteur v non nul et orthogonal à F. On vérifie que $u(v)$ est lui aussi orthogonal à F : si $f \in F$, on a $u(v) \,.\, f = u(v) \,.\, u(f) = v \,.\, f = 0$. Alors $w = u(v) - v$ est orthogonal à F, et non nul puisque v n'appartient pas à l'ensemble F des vecteurs fixes pour u. On va voir que $r_w \circ u$ laisse les vecteurs de F fixes, mais fixe aussi le vecteur v, donc $\dim F(r_w \circ u) > \dim F = \dim F(u)$, ce qu'il fallait démontrer. A l'amphi je n'ai pas eu le temps de détailler la justification de ces deux points :

puisque tout vecteur $f \in F$ est orthogonal à w, on a $r_w(f) = f$, donc $(r_w \circ u)(f) = r_w(u(f)) = r_w(f) = f$. D'autre part, $u(v) + v$ est orthogonal à $u(v) - v = w$ puisque

$$(u(v) + v) \,.\, (u(v) - v) = u(v) \,.\, u(v) - v \,.\, v = 0$$

parce que u est une isométrie. Il en résulte que $r_w(u(v)+v) = u(v)+v$, et $r_w(u(v)-v) = r_w(w) = -w = -u(v) + v$, ce qui donne $r_w(u(v)) = v$ par addition. Alors $(r_w \circ u)(v) = r_w(u(v)) = v$.