ALGÈBRE GÉOMÉTRIQUE

COURS DE M1 2007/8, UNIVERSITÉ PARIS VI

Jan Nekovář

http://www.math.jussieu.fr/∼nekovar/co/ag/

3. Formes bilinéaires et sesquilinéaires

Convention : Fixons un corps K (commutatif). Les espaces vectoriels seront toujours supposés de dimension finie (sur K).

3.1 Formes sesquilinéaires : généralités

(3.1.1) Produit scalaire euclidien. Le produit scalaire usuel

$$f : \mathbf{R}^n \times \mathbf{R}^n \longrightarrow \mathbf{R}, \qquad f(x,y) = \sum_{j=1}^{n} x_j y_j = {}^t x y, \qquad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \qquad y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

satisfait aux propriétés suivantes (pour tous $x, x', y, y' \in \mathbf{R}^n$ et $\lambda, \mu \in \mathbf{R}$) :

(3.1.1.1) (Biadditivité :) $\quad f(x+x', y) = f(x,y) + f(x',y), \qquad f(x, y+y') = f(x,y) + f(x,y')$.

(3.1.1.2) $\quad f(\lambda x, \mu y) = \lambda\mu\, f(x,y)$.

(3.1.1.3) $\quad f(y,x) = f(x,y)$.

(3.1.2) Exemples d'autres produits "naturels" : (i) Le produit pseudo-euclidien

$$f : \mathbf{R}^{p+q} \times \mathbf{R}^{p+q} \longrightarrow \mathbf{R}, \qquad f(x,y) = \sum_{j=1}^{p} x_j y_j - \sum_{k=1}^{q} x_{p+k} y_{p+k}$$

vérifie (3.1.1.1-3).

(ii) Le produit hermitien

$$f : \mathbf{C}^n \times \mathbf{C}^n \longrightarrow \mathbf{C}, \qquad f(x,y) = \sum_{j=1}^{n} x_j \overline{y}_j = {}^t x \overline{y};$$

on a

$$f(\lambda x, \mu y) = \lambda \overline{\mu}\, f(x,y), \qquad f(y,x) = \overline{f(x,y)}.$$

(iii) L'air orienté dans $\mathbf{R}^2$

$$f : \mathbf{R}^2 \times \mathbf{R}^2 \longrightarrow \mathbf{R}, \qquad f(x,y) = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}$$

vérifie

$$f(\lambda x, \mu y) = \lambda\mu\, f(x,y), \qquad f(y,x) = -f(x,y).$$

(3.1.3) Le cas général. Fixons un automorphisme de corps $\sigma : K \longrightarrow K$, i.e. une bijection vérifiant

$$(\forall \lambda, \mu \in K) \qquad \sigma(\lambda + \mu) = \sigma(\lambda) + \sigma(\mu), \qquad \sigma(\lambda\mu) = \sigma(\lambda)\sigma(\mu)$$

(ce qui entraîne $\sigma(0) = 0$ et $\sigma(\pm 1) = \pm 1$). On écrit $\sigma^2 = \sigma \circ \sigma$ ($\Longrightarrow \sigma^2(\lambda) = \sigma(\sigma(\lambda))$).
Exemples : (i) $K = \mathbf{C}$, $\sigma(a + ib) = a - ib$ $(a, b \in \mathbf{R})$.
(ii) $K = \mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$, $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$ $(a, b \in \mathbf{Q})$.
(iii) $K = \mathbf{F}_{p^n}$, $\sigma(a) = a^p$.
On écrit souvent ${}^{\sigma}\lambda$ au lieu de $\sigma(\lambda)$.

Pour toute matrice $A = (A_{ij}) \in M_n(K)$ on définit

$$f : K^n \times K^n \longrightarrow K, \qquad f(x, y) = {}^{t}x A\, {}^{\sigma}y = \sum_{i,j=1}^{n} A_{ij}\, x_i\, {}^{\sigma}y_j.$$

Ce "produit" est biadditif et on a

$$f(\lambda x, \mu y) = \lambda\, {}^{\sigma}\mu\, f(x, y) \qquad\qquad (x, y \in K^n,\ \lambda, \mu \in K).$$

(3.1.4) Définition. *Une* **forme σ-sesquilinéaire** *sur un espace vectoriel V est une application $f : V \times V \longrightarrow K$ vérifiant*
(i) *Pour $y \in V$ fixé, l'application $x \mapsto f(x, y)$ est linéaire.*
(ii) *Pour $x \in V$ fixé, l'application $y \mapsto f(x, y)$ est* **σ-semi-linéaire**, *i.e. on a*

$$(\forall y, y' \in V,\ \forall \lambda \in K) \qquad f(x, y + y') = f(x, y) + f(x, y'), \qquad f(x, \lambda y) = {}^{\sigma}\lambda\, f(x, y).$$

Si $\sigma = \mathrm{id}$, on dit que f est une **forme bilinéaire**. *D'ici jusqu'à 3.1.9 on suppose que f est une forme σ-sesquilinéaire sur V.*

(3.1.5) Équivalence entre 3.1.3 et 3.1.4. Si $e_1, \ldots, e_n$ est une base de V et $x = \sum_{i=1}^n x_i e_i, y = \sum_{j=1}^n y_j e_j \in V$, on a

$$f(x, y) = f\Big(\sum_{i=1}^{n} x_i e_i, \sum_{j=1}^{n} y_j e_j\Big) = \sum_{i,j=1}^{n} x_i\, {}^{\sigma}y_j\, f(e_i, e_j) = \sum_{i,j=1}^{n} A_{ij}\, x_i\, {}^{\sigma}y_j = {}^{t}X A\, {}^{\sigma}Y,$$

où $A = (A_{ij}) = (f(e_i, e_j)) \in M_n(K)$, $X = {}^{t}(x_1, \ldots, x_n)$, $Y = {}^{t}(y_1, \ldots, y_n)$, donc f s'écrit sous la forme 3.1.3.
Si on choisit une autre base $e'_1, \ldots, e'_n$, on a

$$x = \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} x'_i e'_i, \qquad X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = P \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = PX',$$

où $P \in GL_n(P)$ est la matrice de passage entre les deux bases (et de même pour y). Les formules $X = PX'$, $Y = PY'$ entraînent

$$f(x, y) = {}^{t}X A\, {}^{\sigma}Y = {}^{t}X'\, {}^{t}P A\, {}^{\sigma}P\, {}^{\sigma}Y' = {}^{t}X' A'\, {}^{\sigma}Y', \qquad A' = {}^{t}P A\, {}^{\sigma}P.$$

(3.1.6) Définition. *Pour $x, y \in V$, on définit*

$$x \perp y := f(x, y) = 0$$

(on dit que x **est perpendiculaire à** *y). Si $S \subset V$, on définit*

$$x \perp S \iff (\forall y \in S) \quad x \perp y, \qquad S \perp y \iff (\forall x \in S) \quad x \perp y.$$

(3.1.7) Définition. *Le noyau à gauche (resp. à droite) de f est le sous-espace vectoriel de V*

$${}_{g}\mathrm{Ker}(f) = \{x \in V \mid (\forall y \in V) \quad f(x, y) = 0\} = \{x \in V \mid x \perp V\}$$

resp.

$$\mathrm{Ker}_d(f) = \{y \in V \mid (\forall x \in V) \quad f(x,y) = 0\} = \{y \in V \mid V \perp y\}.$$

Si on utilise l'écriture matricielle $f(x,y) = {}^t x A\, {}^\sigma y$, on obtient

$$\begin{aligned} {}_g\mathrm{Ker}(f) &= \{x \in V \mid {}^t x A = {}^t({}^t A x) = 0\} \\ \mathrm{Ker}_d(f) &= \{y \in V \mid A\, {}^\sigma y = {}^\sigma({}^{\sigma^{-1}} A\, y) = 0\} = \{y \in V \mid {}^{\sigma^{-1}} A\, y = 0\}, \end{aligned}$$

donc

$$\dim\left({}_g\mathrm{Ker}(f)\right) = n - \mathrm{rg}({}^t A) = n - \mathrm{rg}(A) = n - \mathrm{rg}({}^{\sigma^{-1}} A) = \dim\left(\mathrm{Ker}_d(f)\right)$$

(voir Exercice 3.1.10 ci-dessous).

(3.1.8) Définition. *La forme f est* **non-dégénérée** *si ${}_g\mathrm{Ker}(f) = 0$ ($\iff$ $\mathrm{Ker}_d(f) = 0$ $\iff$ $\det(A) \neq 0$).*

(3.1.9) Définition. *Le* **discriminant** *de la forme f est l'image de $\det(A)$ dans $K/\{\lambda\, {}^\sigma\lambda \mid \lambda \in K^*\}$. Ceci est bien défini, puisqu'un changement de base remplace A par ${}^t P A\, {}^\sigma P$ ($P \in GL_n(K)$), et ainsi $\det(A)$ est multiplié par $\lambda\, {}^\sigma\lambda$, où $\lambda = \det(P)$.*

(3.1.10) Exercice. *Pour toute matrice $B \in M_n(K)$ et tout automorphisme σ du corps K, on a $\mathrm{rg}({}^\sigma B) = \mathrm{rg}(B)$.*

(3.1.11) Définition. *Le* **rang** *de la forme f est le rang de la matrice A (pour n'importe quel choix de base $e_1, \ldots, e_n$).*

3.2 Propriétés de symétrie

Dans tout ce paragraphe, $\sigma : K \longrightarrow K$ est un automorphisme de corps et $f : V \times V \longrightarrow K$ une forme σ-sesquilinéaire.

(3.2.1) Définition. *La forme f est* **réflexive** *si on a*

$$(\forall x, y \in V) \qquad [x \perp y \iff y \perp x],$$

i.e. si on a

$$(\forall x, y \in V) \qquad [f(x,y) = 0 \iff f(y,x) = 0].$$

(3.2.2) Exemple/Définition : La forme f est réflexive dans tous les cas suivants :

(3.2.2.1) f est bilinéaire **symétrique**, i.e. on a $(\forall x, y \in V) \qquad f(y,x) = f(x,y)$.
(3.2.2.2) f est bilinéaire **antisymétrique**, i.e. on a $(\forall x, y \in V) \qquad f(y,x) = -f(x,y)$.
(3.2.2.3) f est **hermitienne**, i.e. $\sigma \neq \mathrm{id}$ et on a $(\forall x, y \in V) \qquad f(y,x) = {}^\sigma f(x,y)$.

Si on utilise l'écriture matricielle, i.e. si $e_1, \ldots, e_n$ est une base de V et $A = (f(e_i, e_j)) \in M_n(K)$, alors on a

$$\begin{aligned} f \text{ est bilinéaire symétrique} &\iff \sigma = \mathrm{id}, \quad {}^t A = A \\ f \text{ est bilinéaire antisymétrique} &\iff \sigma = \mathrm{id}, \quad {}^t A = -A \end{aligned}$$

puisque

$$f(y,x) = {}^t y A\, x = {}^t({}^t y A\, x) = {}^t x\, {}^t A\, y, \qquad f(x,y) = {}^t x A\, y$$

si $\sigma = \mathrm{id}$.

(3.2.3) Proposition. (i) *Si la forme f est hermitienne et $f \neq 0$, alors σ est une involution, i.e.* $\sigma^2 = \mathrm{id}$.
(ii) *La forme f est hermitienne et non nulle* $\iff$ $\sigma \neq \mathrm{id}$, $\sigma^2 = \mathrm{id}$ *et* ${}^tA = {}^{\sigma}A \neq 0$.

Preuve. (i) Pour tous $x, y \in V$, on a

$$f(x,y) = {}^{\sigma}f(y,x) = {}^{\sigma}({}^{\sigma}f(x,y)) = {}^{\sigma^2}f(x,y).$$

En remplaçant x par λx ($\lambda \in K$), on obtient

$$\lambda\, f(x,y) = f(\lambda x, y) = {}^{\sigma^2}f(\lambda x, y) = {}^{\sigma^2}(\lambda\, f(x,y)) = {}^{\sigma^2}\lambda\, {}^{\sigma^2}f(x,y) = {}^{\sigma^2}\lambda\, f(x,y).$$

Il existe $x, y \in V$ tels que $f(x,y) \neq 0$, donc $\lambda = {}^{\sigma^2}\lambda$ pour tout $\lambda \in K$, i.e. $\sigma^2 = \mathrm{id}$.
(ii) Si $\sigma^2 = \mathrm{id}$, alors on a

$$(\forall x, y \in V \xrightarrow{\sim} K^n) \qquad f(y,x) = {}^tyA\,{}^{\sigma}x = {}^t({}^tyA\,{}^{\sigma}x) = {}^{\sigma}({}^tx){}^tA\,y, \qquad {}^{\sigma}f(x,y) = {}^{\sigma}({}^tx)\,{}^{\sigma}A\,{}^{\sigma^2}y = {}^{\sigma}({}^tx){}^{\sigma}A\,y,$$

donc

$$[(\forall x, y \in V) \qquad f(y,x) = {}^{\sigma}f(x,y)] \iff {}^tA = {}^{\sigma}A.$$

(3.2.4) Proposition. *Soit $f : V \times V \longrightarrow K$ une forme σ-sesquilinéaire,* **non-dégénérée** *et* **réflexive**. *Si* $\dim(V) \geq 2$, *alors on a :*
(i) $\sigma^2 = \mathrm{id}$, *i.e. σ est une* **involution**.
(ii) *Si $\sigma = \mathrm{id}$, alors f est une forme bilinéaire* **symétrique** *ou* **antisymétrique**.
(iii) *Si $\sigma \neq \mathrm{id}$, alors il existe $\alpha \in K^*$ tel que αf soit* **hermitienne**.

Preuve. On utilise l'écriture matricielle, i.e. on choisit une base de $V \xrightarrow{\sim} K^n$ et on écrit $f(x,y) = {}^txA\,{}^{\sigma}y$, où $A \in GL_n(K)$ (la forme f étant non-dégénérée). Fixons $y \in K^n$, $y \neq \vec{0}$. Pour tout $x \in K^n$, on a

$$x \perp y \iff {}^tx(A\,{}^{\sigma}y) = 0 \overset{\sigma}{\iff} {}^{\sigma}({}^tx)({}^{\sigma}A\,{}^{\sigma^2}y) = 0, \tag{3.2.4.1}$$

ce qui est une équation linéaire non nulle pour le vecteur ${}^{\sigma}x \in K^n$. Puisque la condition

$$y \perp x \iff {}^tyA\,{}^{\sigma}x = 0 \iff 0 = {}^t({}^tyA\,{}^{\sigma}x) = {}^{\sigma}({}^tx)({}^tA\,y) \tag{3.2.4.2}$$

s'écrit de la même manière, la propriété de reflexivité 3.2.1 entraîne que les deux équations (3.2.4.1-2) sont proportionnelles, i.e.

$$(\forall y \in K^n - \{\vec{0}\})\,(\exists \varepsilon_y \in K^*) \qquad {}^tA\,y = \varepsilon_y {}^{\sigma}A\,{}^{\sigma^2}y, \qquad By = \varepsilon_y\,{}^{\sigma^2}y,$$

où l'on a posé $B = ({}^{\sigma}A)^{-1}\,{}^tA \in GL_n(K)$. Par hypothèse, $n \geq 2$; si $y, z \in K^n$ sont deux vecteurs linéairement indépendants, on déduit des équations

$$By = \varepsilon_y\,{}^{\sigma^2}y, \qquad Bz = \varepsilon_z\,{}^{\sigma^2}z, \qquad By + Bz = B(y+z) = \varepsilon_{y+z}\,{}^{\sigma^2}(y+z)$$

que

$$\varepsilon_y = \varepsilon_{y+z} = \varepsilon_z.$$

Si $v \in K^n - \{\vec{0}\}$ est un vecteur colinéaire à y, alors v et z sont linéairement indépendants, donc $\varepsilon_v = \varepsilon_{v+z} = \varepsilon_z$. En résumé, le scalaire $\varepsilon = \varepsilon_y \in K^*$ ne dépend pas de $y \in K^n - \{\vec{0}\}$, donc on a

$$(\forall y \in K^n) \qquad By = \varepsilon\,{}^{\sigma^2}y.$$

Preuve de (i) : fixons $y \in K^n - \{\vec{0}\}$; pour tout $\lambda \in K$, on a

$$\varepsilon\lambda\,{}^{\sigma^2}y = \lambda By = B\lambda y = \varepsilon\,{}^{\sigma^2}(\lambda y) = \varepsilon\,{}^{\sigma^2}\lambda\,{}^{\sigma^2}y \implies {}^{\sigma^2}\lambda = \lambda \implies \sigma^2 = \mathrm{id}.$$

En particulier, on a

$$(\forall y \in K^n) \qquad ({}^\sigma A)^{-1}\, {}^t A\, y = By = \varepsilon y,$$

donc $({}^\sigma A)^{-1}\, {}^t A = \varepsilon I$, ${}^t A = \varepsilon\, {}^\sigma A$. On en déduit que

$${}^\sigma A = {}^t({}^\sigma({}^t A)) = {}^t({}^\sigma \varepsilon\, A) = {}^\sigma\varepsilon \varepsilon\, {}^\sigma A \implies {}^\sigma \varepsilon \varepsilon = 1.$$

Preuve de (ii) : si $\sigma = \mathrm{id}$, on a ${}^\sigma\varepsilon = \varepsilon$, donc $\varepsilon^2 = 1$, $\varepsilon = \pm 1$ et ${}^t A = \pm A$.
Preuve de (iii) : si $\sigma \neq \mathrm{id}$, on a

$$f(y,x) = {}^t y A\, {}^\sigma x = {}^t({}^t y A\, {}^\sigma x) = {}^\sigma({}^t x){}^t A\, y = \varepsilon\, {}^\sigma({}^t x)\, {}^\sigma A\, y = \varepsilon\, {}^\sigma({}^t x A\, {}^\sigma y) = \varepsilon\, {}^\sigma f(x,y).$$

D'après Lemme 3.2.5 ci-dessous, il existe $\alpha \in K^*$ tel que ${}^\sigma\alpha/\alpha = \varepsilon$. La forme αf est alors σ-sesquilinéaire et hermitienne, puisqu'on a

$$(\forall x, y \in K^n) \qquad (\alpha f)(y,x) = \alpha\varepsilon\, {}^\sigma f(x,y) = {}^\sigma\alpha\, {}^\sigma f(x,y) = {}^\sigma(\alpha f(x,y)).$$

(3.2.5) Lemme (un cas particulier du Théorème 90 de Hilbert). *Si $\varepsilon \in K^*$ vérifie ${}^\sigma\varepsilon\varepsilon = 1$, alors il existe $\alpha \in K^*$ tel que ${}^\sigma\alpha/\alpha = \varepsilon$.*

Preuve. Soit $\alpha = a + {}^\sigma\varepsilon\, {}^\sigma a \in K$, où $a \in K$. Comme ${}^\sigma\alpha = ({}^\sigma a + \varepsilon a) = \varepsilon(a + {}^\sigma\varepsilon\, {}^\sigma a) = \varepsilon\alpha$, il faut trouver $a \in K$ tel que l'on ait $\alpha \neq 0$. Si $\varepsilon \neq -1$, on prend $a = 1$ et $\alpha = 1 + {}^\sigma\varepsilon \neq 0$. Si $\varepsilon = -1$, on prend $a \in K$ vérifiant ${}^\sigma a \neq a$; dans ce cas $\alpha = a - {}^\sigma a \neq 0$.

(3.2.6) Définition. *La forme f est* **alternée** *si on a*

$$(\forall x \in V) \qquad f(x,x) = 0.$$

(3.2.7) Proposition. *Si la forme f est alternée et $f \neq 0$, alors $\sigma = \mathrm{id}$ et f est une forme bilinéaire antisymétrique.*

Preuve. Pour tous $x, y \in V$ on a

$$0 = f(x+y, x+y) = f(x,x) + f(y,y) + f(x,y) + f(y,x) = f(x,y) + f(y,x) \implies f(y,x) = -f(x,y).$$

Il faut encore démontrer que $\sigma = \mathrm{id}$; fixons $x, y \in V$ tels que $f(x,y) \neq 0$. Pour tout $\lambda \in K$, on a

$$\lambda\, f(x,y) = -\lambda\, f(y,x) = -f(\lambda y, x) = f(x, \lambda y) = {}^\sigma\lambda\, f(x,y) \implies {}^\sigma\lambda = \lambda,$$

donc $\sigma = \mathrm{id}$.

(3.2.8) Proposition. *Si f est une forme bilinéaire antisymétrique et si la caractéristique du corps K n'est pas égale à 2 (c'est-à-dire que $2 \neq 0$ dans K; notation : $\mathrm{car}(K) \neq 2$), alors f est alternée.*

Preuve. Pour tout $x \in V$, on a $f(x,x) = -f(x,x)$, donc $2\, f(x,x) = 0$; comme 2 est inversible dans K, on obtient $f(x,x) = 0$.

(3.2.9) Définition. *Si f est une forme bilinéaire symétrique, la* **forme quadratique associée à** *f est la fonction $q(x) = f(x,x)$, $q : V \longrightarrow K$ (i.e. $q(x) = {}^t x A x$, si on utilise l'écriture matricielle). Si $\mathrm{car}(K) \neq 2$, alors on a*

$$(\forall x, y) \qquad f(x,y) = 2^{-1}\left(q(x+y) - q(x) - q(y)\right). \tag{3.2.9.1}$$

En effet,

$$q(x+y) = f(x+y, x+y) = f(x,x) + f(y,y) + f(x,y) + f(y,x) = q(x) + q(y) + 2f(x,y).$$

Si $\mathrm{car}(K) = 2$, on peut bien avoir $q = 0$ même si $f \neq 0$. Ceci est le cas, par exemple, pour

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad f(x,y) = x_1y_2 + x_2y_1, \qquad q(x) = 2x_1x_2 = 0.$$

(3.2.10) Exercice. *On suppose que* $\sigma^2 = \mathrm{id}$, $\sigma \neq \mathrm{id}$ *et* $\mathrm{car}(K) \neq 2$. *Montrer :*
(i) $k := K^{\sigma=1} = \{\lambda \in K \mid \sigma(\lambda) = \lambda\}$ *est un sous-corps de* K.
(ii) *Il existe un élément* $a \in K^*$ *tel que* $\sigma(a) = -a$*; on fixe un tel élément.*
(iii) *Tout élément* $\lambda \in K$ *s'écrit, de manière unique, comme* $\lambda = u + av$, $u, v \in k$. *On pose* $R(\lambda) = u$, $I(\lambda) = v$.
(iv) *Les applications* $R, I : K \longrightarrow k$ *sont* k*-linéaires; de plus,* R *ne dépend pas du choix de* a. *[Il faut garder dans sa tête l'exemple "classique" :* $K = \mathbf{C}$, $\sigma(u + vi) = u - vi$, $k = \mathbf{R}$, $a = i$, $R = \mathrm{Re}$, $I = \mathrm{Im}$.*]*

(3.2.11) Exercice. *Sous les hypothèses de 3.2.10, soit* $f : V \times V \longrightarrow K$ *une forme hermitienne. Montrer que l'application* $g = R \circ f : V \times V \longrightarrow k$, $g(x,y) = R(f(x,y))$ *(resp.* $h = I \circ f : V \times V \longrightarrow k$, $h(x,y) = I(f(x,y))$*) est une forme* k*-bilinéaire symétrique (resp. antisymétrique).*

(3.2.12) Définition. *Si* f *est une forme hermitienne. la* **forme quadratique hermitienne associée à** f *est la fonction* $q(x) = f(x,x)$, $q : V \longrightarrow K$ *(i.e.* $q(x) = {}^t\!x A\, {}^\sigma\! x$, *si on utilise l'écriture matricielle). Si* $\mathrm{car}(K) \neq 2$, *fixons* $a \in K^*$ *comme en 3.2.10(ii). On a*

$$(\forall x, y) \qquad f(x,y) = 4^{-1}\left(q(x+y) - q(x-y)\right) + (4a)^{-1}\left(q(ax+y) - q(ax-y)\right). \tag{3.2.12.1}$$

En effet, on a

$$\begin{gathered} q(x \pm y) = f(x \pm y, x \pm y) = f(x,x) + f(y,y) \pm f(x,y) \pm f(y,x), \\ q(ax \pm y) = -a^2 f(x,x) + f(y,y) \pm a\, f(x,y) \mp a\, f(y,x), \\ q(x+y) - q(x-y) = 2(f(x,y) + f(y,x)) \\ q(ax+y) - q(ax-y) = 2a(f(x,y) - f(y,x)). \end{gathered}$$

(3.2.13) Exercice. *Déterminer toutes les solutions de l'équation diophantienne*

$$a^2 + b^2 = c^2 \qquad\qquad (a, b, c \in \mathbf{Z})$$

à l'aide de 3.2.5 (pour $K = \{x + iy \mid x, y \in \mathbf{Q}\}$ *et* $\sigma(x + iy) = x - iy$*).*

3.3 Orthogonalité

Dans tout ce paragraphe, $f : V \times V \longrightarrow K$ une forme σ-sesquilinéaire, soit **bilinéaire symétrique**, soit **bilinéaire antisymétrique**, soit **hermitienne**. En particulier, f est réflexive, i.e. on a $[x \perp y \iff y \perp x]$.

(3.3.1) Définition. *Soient* $X, Y \subset V$ *deux sous-ensembles (non-vides). On dit que* X **est orthogonal à** Y *si on a*

$$(\forall x \in X)\,(\forall y \in Y) \qquad x \perp y.$$

L'orthogonal de X *est l'ensemble*

$$X^\perp = \{y \in V \mid y \perp X\}$$

($X^\perp$ *est un sous-espace vectoriel de* V *– exercice!). Par exemple,* $\{\vec{0}\}^\perp = V$ *et* $V^\perp = \mathrm{Ker}(f)$ *(*$:= {}_g\mathrm{Ker}(f) = \mathrm{Ker}_d(f)$*).*

(3.3.2) Exercice. *Pour tout sous-ensemble (non-vide)* $X \subset V$, *on a* $X \subset (X^\perp)^\perp$ *et* $X^\perp = (\mathrm{vect}(X))^\perp$, *où on a noté* $\mathrm{vect}(X)$ *le sous-espace vectoriel de* V *engendré par* X.

(3.3.3) Définition. *Une somme directe* $V = V_1 \oplus \cdots \oplus V_m$ *est* **orthogonale** *si on a* $(\forall i \neq j) \quad V_i \perp V_j$ *(***notation :** $V = V_1 \perp \ldots \perp V_m$*).*

Dans ce cas on a

$$f(\sum_{i=1}^{m} x_i, \sum_{j=1}^{m} y_j) = \sum_{i=1}^{m} f_i(x_i, y_i), \qquad\qquad (x_i, y_i \in V_i)$$

où on a noté $f_i : V_i \times V_i \longrightarrow K$ la restriction de f à $V_i \times V_i$. Si on fixe, pour tout $i = 1, \ldots, m$, une base de V_i, la matrice A de f dans la réunion de ces bases est égale à

$$\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_m \end{pmatrix}$$

où A_i est la matrice de f_i. Par exemple, si $V = \mathbf{R}^n$ et $f(x, y) = {}^t x y$ est le produit scalaire euclidien, on a $V = \mathbf{R}e_1 \perp \ldots \perp \mathbf{R}e_n$, où $e_1, \ldots, e_n$ est la base canonique de $\mathbf{R}^n$, et $A = I$.

(3.3.4) Définition. *Un vecteur* $x \in V$ *est* **isotrope** *si* $x \neq \vec{0}$ *et* $f(x, x) = 0$ *(si c'est le cas,* λx *est isotrope, pour tout* $\lambda \in K^*$*; les vecteurs isotropes* $(\cup\{\vec{0}\})$ *forment le* **cône isotrope** $C(q) = \{x \in V \mid q(x) = 0\}$*).*

(3.3.5) Exemples : (i) Si $V = \mathbf{R}^2$ et $f(x, y) = x_0 y_0 - x_1 y_1$, on note W_a la droite $x_1 = a x_0$ $(a \neq 0)$. Le cône isotrope $C(q)$ est égal à la réunion $C(q) = W_1 \cup W_{-1}$. On a $W_a^\perp = W_{1/a}$, donc $W_{\pm 1}^\perp = W_{\pm 1}$. Par contre, si $a \neq \pm 1$ ($\iff W_a \not\subset C(q)$), alors on a $W_a \oplus W_a^\perp = V$.
(ii) Si $V = \mathbf{R}^3$ et $f(x, y) = x_0 y_0 - x_1 y_1 - x_2 y_2$, on a $q(x) = f(x, x) = x_0^2 - x_1^2 - x_2^2$. Les vecteurs isotropes $(\cup\{\vec{0}\})$ forment le cône

$$C = \{{}^t(x_0, x_1, x_2) \in \mathbf{R}^3 \mid x_0^2 - x_1^2 - x_2^2 = 0\}.$$

Soit $W \subset V$ une droite vectorielle.
(i) Si $W \not\subset C$, alors $W^\perp$ est un plan vérifiant $W \cap W^\perp = \{\vec{0}\}$ et $W \perp W^\perp = V$.
(ii) Si $W \subset C$, chaque vecteur non nul $x \in W$ est isotrope, donc $W \subset W^\perp$. Dans ce cas $W^\perp$ est un plan tangent au cône C et l'intersection $W^\perp \cap C$ est égale à W.

Si $H \subset V$ est un hyperplan affine général, la correspondance $H \cap W \mapsto H \cap W^\perp$ est la polarité (cf. 2.7.9) par rapport à la conique $H \cap C$ (exercice).

(3.3.6) Définition. *Un sous-espace vectoriel* $W \subset V$ *est* **totalement isotrope** *si on a*

$$(\forall x, y \in W) \qquad f(x, y) = 0 \qquad\qquad (\iff W \perp W \iff W \subset W^\perp).$$

Par exemple, si $X \subset V$ *est un sous-espace vectoriel, alors* $W = X \cap X^\perp$ *est totalement isotrope.* **L'indice de** f *est défini comme* $\nu(f) := \max\{\dim(W) \mid W \subset V,\ W \text{ est totalement isotrope}\}$.

Exemple : Si $n = 2m$ et $f(x, y) = x_1 y_1 + \cdots + x_m y_m - x_{m+1} y_{m+1} - \cdots - x_{2m} y_{2m}$, alors le sous-espace

$$W = \{{}^t(x_1, \ldots, x_{2m}) \mid (\forall i = 1, \ldots, m) \quad x_{m+i} = x_i\}$$

est totalement isotrope, $\dim(W) = m = \dim(V)/2$.

(3.3.7) Proposition. *On suppose que la forme* f *est non-dégénérée. Si* $X, Y \subset V$ *sont deux sous-espaces vectoriels de* V*, alors on a :*
(i) $\dim(X) + \dim(X^\perp) = \dim(V)$.
(ii) $(X^\perp)^\perp = X$.
(iii) $(X + Y)^\perp = X^\perp \cap Y^\perp$.

(iv) $(X \cap Y)^\perp = X^\perp + Y^\perp$.
(v) *Si* $X \cap X^\perp = \{\vec{0}\}$, *alors* $V = X \perp X^\perp$.

Preuve. (i) On écrit f sous la forme matricielle $f(x,y) = {}^t x A\,{}^\sigma y$, où $x, y \in K^n$ ($n = \dim(V)$) et $A \in GL_n(K)$, donc

$$X^\perp = \{y \in K^n \mid (\forall x \in K^n) \quad {}^t y A\,{}^\sigma x = 0\}.$$

Comme $\{A\,{}^\sigma x \mid x \in X\} = A\,{}^\sigma X$ est un sous-espace vectoriel de K^n dont la dimension est égale à $\dim({}^\sigma X) = \dim(X)$ (la matrice A est inversible!), on a $\dim(X^\perp) = n - \dim(X)$.
(ii) On sait que l'on a $X \subset (X^\perp)^\perp$; comme $\dim((X^\perp)^\perp) = n - \dim(X^\perp) = \dim(X)$, on obtient l'égalité $X = (X^\perp)^\perp$.
(iii) Exercice.
(iv) D'après (ii) et (iii), on a $(X^\perp + Y^\perp)^\perp = (X^\perp)^\perp \cap (Y^\perp)^\perp = X \cap Y$, donc $X^\perp + Y^\perp = (X \cap Y)^\perp$.
(v) Il résulte de $X \cap X^\perp = \{\vec{0}\}$ et de $\dim(X) + \dim(X^\perp) = \dim(V)$ que V est égal à la somme directe $V = X \oplus X^\perp$; comme $X \perp X^\perp$ par définition, on a $V = X \perp X^\perp$.

(3.3.8) Proposition. *Si la forme f est non-dégénérée, alors $\nu(f) \le \dim(V)/2 = \mathrm{rg}(f)/2$.*

Preuve. Si $W \subset V$ est un sous-espace totalement isotrope, alors on a $W \subset W^\perp$, donc $\dim(W) \le \dim(W^\perp) = \dim(V) - \dim(W)$, d'où $2\dim(W) \le \dim(V)$.

(3.3.9) Proposition (réduction au cas non-dégénéré). *Si $W \subset V$ est un sous-espace vectoriel supplémentaire à* $\mathrm{Ker}(f) = V^\perp$ *($\iff V = W \oplus V^\perp$), alors on a $V = W \perp V^\perp$, et la restriction g de f à $W \times W$ est non-dégénérée.*

Preuve. Par définition de $V^\perp$, on a $W \perp V^\perp$, ce qui entraîne que la somme directe $V = W \oplus V^\perp$ est orthogonale : on a $V = W \perp V^\perp$. La dimension de W est égale à $\dim(W) = \dim(V) - \dim(\mathrm{Ker}(f)) = \mathrm{rg}(f) = r$. On fixe une base de $V^\perp$ et une base de W. La matrice A de f dans la réunion des deux bases est égale à

$$A = \begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix},$$

où $B \in M_r(K)$ est la matrice de g. Comme $\mathrm{rg}(B) = \mathrm{rg}(A) = r$, la matrice B est inversible, donc la forme g est non-dégénérée.

3.4 Groupe unitaire, orthogonal et symplectique

(3.4.1) Définition. *Soit $f : V \times V \longrightarrow K$ une forme σ-sesquilinéaire non-dégénérée, soit hermitienne, soit bilinéaire symétrique, soit bilinéaire alternée. Une* **isométrie** *de f est une bijection linéaire $u \in GL(V)$ vérifiant*

$$(\forall x, y \in V) \qquad f(u(x), u(y)) = f(x,y). \tag{$\star$}$$

Les isométries de f forment un sous-groupe de $GL(V)$, qui est noté, respectivement, $U(f)$ (le **groupe unitaire***), resp. $O(f)$ (le* **groupe orthogonal***) resp. $Sp(f)$ (le* **groupe symplectique***).*

(3.4.2) Si on utilise l'écriture matricielle, on a $f(x,y) = {}^t x A\,{}^\sigma y$ ($A \in GL_n(K)$, $n = \dim(V)$) et $u : x \mapsto Ux$ ($U \in GL_n(K)$), donc la condition ($\star$) équivaut à

$$(\forall x, y \in K^n) \qquad {}^t(Ux) A\,{}^\sigma(Uy) = {}^t x\,{}^t U A\,{}^\sigma U\,{}^\sigma y = {}^t x A\,{}^\sigma y \iff {}^t U A\,{}^\sigma U = A,$$

i.e. le groupe des isométries de f s'identifie à

$$\{U \in GL_n(K) \mid {}^t U A\,{}^\sigma U = A\}.$$

Exemples : (i) Produit scalaire euclidien : $K = \mathbf{R}$, $\sigma = \mathrm{id}$, $f(x,y) = {}^t x y$, donc $A = I$ et $O(f) = \{U \in GL_n(\mathbf{R}) \mid {}^t U U = I\} = O(n)$ est le groupe orthogonal classique.

(ii) Produit hermitien euclidien : $K = \mathbf{C}$, $\sigma(a+ib) = a - ib$, $f(x,y) = {}^t x\overline{y}$, donc $A = I$ et $U(f) = \{U \in GL_n(\mathbf{C}) \mid {}^t U\overline{U} = I\} = U(n)$ est le groupe unitaire classique.
(iii) Si u est une isométrie de f, alors on a : $[x \perp y \Longrightarrow u(x) \perp u(y)]$.
(iv) Si u est une isométrie de f et $W \subset V$ est un sous-espace vectoriel tel que $u(W) \subset W$, alors $u(W) = W$ (u étant injectif, les dimensions de W et de $u(W)$ sont les mêmes) et $[x \perp W \overset{(iii)}{\Longrightarrow} u(x) \perp u(W) = W]$, donc $u(W^\perp) \subset W^\perp$ ($\overset{(iii)}{\Longrightarrow} u(W^\perp) = W^\perp$).

(3.4.3) On va démontrer en 3.4.3.4 ci-dessous que la condition $(\star)$ seule entraîne que l'application u est une bijection linéaire.

(3.4.3.1) Voici l'idée de la preuve dans le cas euclidien ($K = \mathbf{R}$, $f(x,y) = {}^t xy$) : si $e_1, \ldots, e_n \in \mathbf{R}^n$ est un système **orthonormé** (i.e. si on a $f(e_i, e_j) = \delta_{ij}$ pour tous $i, j = 1, \ldots, n$), alors on a :

(3.4.3.1.1) $e_1, \ldots, e_n$ est une base de $\mathbf{R}^n$;
(3.4.3.1.2) $(\forall y \in \mathbf{R}^n) \qquad y = \sum_{i=1}^n f(y, e_i)\, e_i$.

Si $u : \mathbf{R}^n \longrightarrow \mathbf{R}^n$ est une application vérifiant $(\star)$, alors $u(e_1), \ldots, u(e_n)$ est aussi un système orthonormé; en appliquant (3.4.3.1.2) à $\{u(e_i)\}$ et $y = u(x)$ ($x \in \mathbf{R}^n$), on obtient

$$u(x) = \sum_{i=1}^n f(u(x), u(e_i))\, u(e_i) = \sum_{i=1}^n f(x, e_i)\, u(e_i),$$

ce qui est une application linéaire en x.

En général, un système orthonormé n'existe pas; néanmoins, on peut démontrer une variante de (3.4.3.1.1-2) :

(3.4.3.2) Proposition. *Soit $f : V \times V \longrightarrow K$ une forme σ-sesquilinéaire non-dégénérée, $n = \dim(V)$. Si $e_1, \ldots, e_n \in V$ et $e'_1, \ldots, e'_n \in V$ sont des vecteurs vérifiant $f(e_i, e'_j) = \delta_{ij}$ ($\forall i, j = 1, \ldots, n$), alors on a :*
(i) $e_1, \ldots, e_n$ (resp. $e'_1, \ldots, e'_n$) est une base de V.
(ii) $(\forall y \in V) \qquad y = \sum_{i=1}^n f(y, e'_i)\, e_i$.

Preuve. (i) Il suffit de montrer que les vecteurs $e_1, \ldots, e_n$ (resp. $e'_1, \ldots, e'_n$) sont linéairement indépendants, puisque $n = \dim(V)$.

$$\sum_{i=1}^n \lambda_i e_i = 0 \quad (\lambda_i \in K) \implies (\forall j = 1, \ldots, n) \qquad 0 = f(\sum_i \lambda_i e_i, e'_j) = \sum_i \lambda_i\, f(e_i, e'_j) = \lambda_j.$$

$$\sum_{j=1}^n \mu_j e'_j = 0 \quad (\mu_j \in K) \implies (\forall i = 1, \ldots, n) \qquad 0 = f(e_i, \sum_j \mu_j e'_j) = \sum_j {}^\sigma\mu_j\, f(e_i, e'_j) = {}^\sigma\mu_i.$$

(ii) Posons $z = \sum_{i=1}^n f(y, e'_i)\, e_i$. On va montrer que $z - y \perp V$:

$$(\forall j = 1, \ldots, n) \qquad f(z, e'_j) = f(\sum_i f(y, e'_i)\, e_i, e'_j) = \sum_i f(y, e'_i)\, f(e_i, e'_j) = f(y, e'_j),$$

donc $z - y \perp \{e'_1, \ldots, e'_n\}$, ce qui entraîne que $z - y \perp \mathrm{vect}(e'_1, \ldots, e'_n) = V$, i.e. $z - y \in V^\perp = \{\vec{0}\}$ (puisque f est non-dégénérée).

(3.4.3.3) On cherche à trouver des vecteurs $e_1, \ldots, e_n$ et $e'_1, \ldots, e'_n$ vérifiants $f(e_i, e'_j) = \delta_{ij}$. Soient $U, U' \in M_n(K)$ deux matrices; si on note e_i (resp. e'_i) la i-ème colonne de la matrice U (resp. de U'), alors le produit matriciel

$$B = {}^t U A\, {}^\sigma U'$$

est égal à

$$B = (B_{ij}), \qquad B_{ij} = {}^t e_i A\, {}^\sigma e'_j = f(e_i, e'_j).$$

Il en résulte que la condition $f(e_i, e'_j) = \delta_{ij}$ équivaut à

$$B = (\delta_{ij}) = I \iff {}^t U A\, {}^\sigma U' = I. \tag{3.4.3.3.1}$$

La matrice A étant inversible (puisque la forme f est non-dégénérée), il existe beaucoup de solutions de (3.4.3.3.1), par exemple $U' = I$ et $U = ({}^t A)^{-1}$. On s'aperçoit aussi que des matrices U, U' vérifiant (3.4.3.3.1) sont forcément inversibles, donc leurs colonnes forment deux bases de K^n, ce qui donne une autre (?) démonstration de 3.4.3.2(i).

(3.4.3.4) Proposition. *Soit $f : V \times V \longrightarrow K$ une forme σ-sesquilinéaire non-dégénérée. Si $u : V \longrightarrow V$ est une application vérifiant*

$$(\forall x, y \in V) \qquad f(u(x), u(y)) = f(x, y),$$

alors u est linéaire et bijective (i.e. $u \in GL(V)$).

Preuve. On fixe des vecteurs $e_1, \ldots, e_n \in V$ et $e'_1, \ldots, e'_n \in V$ vérifiant $(\forall i, j = 1, \ldots, n) \quad f(e_i, e'_j) = \delta_{ij}$. On a $f(u(e_i), u(e'_j)) = f(e_i, e'_j) = \delta_{ij}$, donc 3.4.3.2(ii) s'applique à $u(e_i), u(e'_j)$:

$$(\forall y \in V) \qquad y = \sum_{i=1}^{n} f(y, u(e'_i))\, u(e_i).$$

Si $y = u(x)$ $(x \in V)$, on obtient alors

$$u(x) = \sum_{i=1}^{n} f(u(x), u(e'_i))\, u(e_i) = \sum_{i=1}^{n} f(x, e'_i)\, u(e_i),$$

ce qui montre que l'application u est linéaire. Elle est bijective, puisque les vecteurs $u(e_1), \ldots, u(e_n)$ forment une base de V, d'après 3.4.3.2(i).

(3.4.4) Proposition. *Si $f : V \times V \longrightarrow K$ est une forme bilinéaire symétrique (resp. hermitienne) non-dégénérée et si* $\mathrm{car}(K) \neq 2$, *alors le groupe orthogonal $O(f)$ (resp. le groupe unitaire $U(f)$) est égal à*

$$\{u \in GL(V) \mid (\forall x \in V) \quad q(u(x)) = q(x)\},$$

où $q(x) = f(x, x)$ est la forme quadratique (resp. la forme quadratique hermitienne) associée à f.

Preuve. Ceci résulte de la formule (3.2.9.1) (resp. (3.2.12.1)).

(3.4.5) Convention. Désormais (jusqu'à la fin du cours) on suppose que, si f est une forme bilinéaire symétrique (resp. hermitienne), alors $\mathrm{car}(K) \neq 2$. Grâce à 3.4.4, on écrit souvent $O(q)$ (resp. $U(q)$) au lieu de $O(f)$ (resp. de $U(f)$).

(3.4.6) Remarques. (i) Pour $\lambda \in K^*$, $u \in GL(V)$ est une isométrie de $f \iff u$ est une isométrie de λf.
(ii) Pour $\lambda \in K^*$, l'application $\lambda \cdot \mathrm{id}$ est une isométrie de $f \iff {}^\sigma\lambda\lambda = 1$ ($\iff \lambda = \pm 1$ si $\sigma = \mathrm{id}$). En particulier, si $\dim(V) = 1$, alors on a

$$O(f) = \{\pm 1\}, \qquad U(f) = \{\lambda \in K^* \mid {}^\sigma\lambda\lambda = 1\}.$$

(iii) Si u est une isométrie de f, alors il résulte de l'équation matricielle ${}^t U A\, {}^\sigma A = A$ que le déterminant de u satisfait à ${}^\sigma\!\det(u) \det(u) = 1$ (en particulier, $\det(u) = \pm 1$ si $\sigma = \mathrm{id}$).
(iv) On verra (voir 3.5.6 ci-dessous) que si f est une forme non-dégénérée alternée, alors la dimension $\dim(V) = 2m$ est toujours paire et le déterminant de chaque isométrie $u \in Sp(f)$ est égal à $\det(u) = 1$.
(v) Si $V = K^2$ et

$$f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1 y_2 - x_2 y_1,$$

alors la forme f est bilinéaire alternée, non-dégénérée, et on a

$$(\forall u \in GL(V) = GL_2(K)) \qquad f(u(x), u(y)) = \det(u)\, f(x, y),$$

donc

$$Sp(f) = SL_2(K).$$

(3.4.7) Définition. *On pose $SL(V) = \{u \in GL(V) \mid \det(u) = 1\}$. Si $f : V \times V \longrightarrow K$ est une forme bilinéaire symétrique (resp. hermitienne) non-dégénérée, on note $SO(f) = O^+(f) := O(f) \cap SL(V)$ le* **groupe spécial orthogonal** *(resp. $SU(f) = U^+(f) := U(f) \cap SL(V)$ le* **groupe spécial unitaire***) de f. On dit qu'un élément de $SO(f)$ (resp. $SU(f)$) est une* **isométrie positive**.
Si $V = \mathbf{R}^n$ (resp. $V = \mathbf{C}^n$) et $f(x, y) = {}^t xy$ (resp. $f(x, y) = {}^t x\overline{y}$) est le produit scalaire euclidien (resp. le produit hermitien euclidien), on utilise la notation $O_n(\mathbf{R}) = O(n) = O(f)$ et $SO_n(\mathbf{R}) = SO(n) = O^+(n) = SO(f)$ (resp. $U_n(\mathbf{C}) = U(n) = U(f)$ et $SU_n(\mathbf{C}) = SU(n) = SU(f)$).

(3.4.8) Définition. *Sous les hypothèses de 3.4.1, soit $u \in GL(V)$. On dit que u est une* **similitude de multiplicateur** *$\mu \in K^*$ (relativement à f) si on a*

$$(\forall x, y \in V) \qquad f(u(x), u(y)) = \mu\, f(x, y).$$

Le groupe des similitudes est noté $GU(f)$, resp. $GO(f)$ resp. $GSp(f)$. Sous la forme matricielle, ce groupe s'identifie à

$$\{U \in GL_n(K) \mid {}^t U A\, {}^\sigma U = \mu I\}.$$

Le facteur μ est déterminé par u; l'application $u \mapsto \mu$ est un homomorphisme de groupes $GU(f) \longrightarrow K^*$ (resp. $GO(f) \longrightarrow K^*$, resp. $GSp(f) \longrightarrow K^*$), dont le noyau est égal à $U(f)$ (resp. $O(f)$, resp. $Sp(f)$).

(3.4.9) Exercice. *Si f est une forme bilinéaire symétrique (non-dégénérée) et si $2 \nmid \dim(V)$, alors l'application canonique $SO(f) \longrightarrow PGO(f)$ est un isomorphisme (où l'on a noté $PGO(f)$ l'image de $GO(f) \subset GL(V)$ dans $PGL(V) = GL(V)/K^* \cdot \mathrm{id}$).*

(3.4.10) Proposition (Symétries orthogonales). *Soit $f : V \times V \longrightarrow K$ une forme symétrique bilinéaire (donc $\mathrm{car}(K) \neq 2$), non-dégénérée. Si $u \in GL(V)$ est un élément vérifiant $u^2 = \mathrm{id}$, alors on a :*
(i) *$V = V^+ \oplus V^-$, où*

$$V^{\pm} = V^{\pm}(u) = \{x \in V \mid u(x) = \pm x\},$$

donc la matrice de u dans la réunion d'une base de V^+ et d'une base de V^- est égale à

$$\begin{pmatrix} I_m & 0 \\ 0 & -I_{n-m} \end{pmatrix} \qquad\qquad (m = \dim(V^+)).$$

(ii) *$[u \in O(f) \iff V^+ \perp V^-]$. Si c'est le cas, alors on a $V = V^+ \perp V^-$ et $(V^{\pm})^{\perp} = V^{\mp}$; on dit que u est une* **symétrie orthogonale**.
(iii) *Réciproquement, si $W \subset V$ est un sous-espace vectoriel vérifiant $W \cap W^{\perp} = \{\vec{0}\}$, alors il existe un unique élément $u \in O(f)$ tel que l'on ait $u^2 = \mathrm{id}$ et $W = V^+(u)$.*

Preuve. (i) Tout $x \in V$ s'écrit $x = x_+ + x_-$, où $x_{\pm} = \frac{1}{2}(x \pm u(x)) \in V^{\pm}$, donc $V = V^+ + V^-$. Si $x \in V^+ \cap V^-$, alors $x = u(x) = -x$, donc $2x = \vec{0} \Longrightarrow x = \vec{0}$, d'où $V = V^+ \oplus V^-$.
(ii) Soient $x_{\pm} \in V^{\pm}$. Si $u \in O(f)$, alors on a

$$f(x_+, x_-) = f(u(x_+), u(x_-)) = f(x_+, -x_-) = -f(x_+, x_-),$$

donc $f(x_+, x_-) = 0$, ce qui montre que $V^+ \perp V^-$. Réciproquement, si $x, y \in V$ et $V^+ \perp V^-$, on écrit $x = x_+ + x_-$ et $y = y^+ + y_-$, où $x_{\pm}, y_{\pm} \in V^{\pm}$. Comme $u(x) = x_+ - x_-$, $u(y) = y_+ - y_-$ et $V^+ \perp V^-$, on a

$$f(x, y) = f(x_+, y_+) + f(x_-, y_-) = f(x_+, y_+) + f(-x_-, -y_-) = f(u(x), u(y)),$$

i.e. $u \in O(f)$.
(iii) On a $V = W \perp W^{\perp}$; si on définit $u \in GL(V)$ par la formule $u(w + w') = w - w'$ ($w \in W$, $w' \in W^{\perp}$), alors on a $u^2 = \mathrm{id}$, $V^+(u) = W$ et $V^-(u) = W^{\perp}$, donc $u \in O(f)$, d'après (ii). Réciproquement, si u est une symétrie orthogonale vérifiant $V^+(u) = W$, alors on a $V^-(u) = (V^+(u))^{\perp} = W^{\perp}$, d'où $u(w + w') = w - w'$ ($w \in W$, $w' \in W^{\perp}$).

(3.4.11) Proposition-Définition (Réflexions orthogonales). *Sous les hypothèses de 3.4.10, on dit qu'une symétrie orthogonale $u \in O(f)$ est une* **réflexion** *si le sous-espace $H = V^+(u) \subset V$ est un* **hyperplan** *(vérifiant $H \cap H^\perp = \{\vec{0}\}$); on note $u = \tau_H$.*
Si $x \in V - \{\vec{0}\}$ n'est pas isotrope, alors $H = (Kx)^\perp$ est un hyperplan et on a $H \cap H^\perp = (Kx)^\perp \cap Kx = \{\vec{0}\}$; la réflexion τ_H, qui est souvent notée τ_x, est égale à

$$\tau_x(y) = y - 2\,\frac{f(x,y)}{f(x,x)}\,x. \tag{3.4.11.1}$$

Preuve (de la formule). Un élément $y \in V$ se décompose comme $y = y_+ + y_-$, où $y_- \in V^-(\tau_x) = Kx$ et $y_+ \in V^+(\tau_x) = (Kx)^\perp$. Si on écrit $y_- = \lambda x$ ($\lambda \in K$), alors on a

$$y - \lambda x \perp x \implies 0 = f(x, y - \lambda x) = f(x,y) - \lambda\, f(x,x) \implies \lambda = f(x,y)/f(x,x), \tag{3.4.11.2}$$

donc

$$\tau_x(y) = \tau_x(y_+ + y_-) = y_+ - y_- = y - 2\lambda x = y - 2\,\frac{f(x,y)}{f(x,x)}\,x.$$

(3.4.12) Projections orthogonales. Sous les hypothèses de 3.4.10, soit $W \subset V$ un sous-espace vectoriel vérifiant $W \cap W^\perp = \{\vec{0}\}$. Dans ce cas $V = W \perp W^\perp$, ce qui signifie qu'un vecteur quelconque $y \in V$ s'écrit, de manière unique, comme $y = y_+ + y_-$, où $y_+ \in W$ et $y_- \in W^\perp$. La **projection orthogonale à** W est l'application linéaire

$$p : V \longrightarrow W, \qquad p(y) = y_+.$$

Si $W = H = (Kx)^\perp$ est un hyperplan (où $x \in V$ n'est pas isotrope), alors le calcul (3.4.11.2) montre que l'on a

$$p(y) = y - y_- = y - \lambda x = y - \frac{f(x,y)}{f(x,x)}\,x. \tag{3.4.12.1}$$

3.5 Diagonalisation

(3.5.1) Exemple : Comme

$$x_1^2 + x_1x_2 - x_2^2 = \left(x_1 + \tfrac{1}{2}x_2\right)^2 - \tfrac{5}{4}x_2^2 = x_1'^2 - \tfrac{5}{4}x_2'^2,$$

le changement de coordonnées

$$\begin{pmatrix} x_1' \\ x_2' \end{pmatrix} = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

diagonalise la forme quadratique $x_1^2 + x_1x_2 - x_2^2$.

(3.5.2) Théorème. *Soit $f : V \times V \longrightarrow K$ une forme symétrique bilinéaire ou une forme hermitienne ($\mathrm{car}(K) \neq 2$). Alors il existe une base $e_1', \ldots, e_n'$ de V telle que $V = Ke_1' \perp \cdots \perp Ke_n'$ (une* **base orthogonale de** *V), ce qui équivaut à*

$$A' = \left(f(e_i', e_j')\right) = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix} \qquad (\forall i = 1, \ldots, n) \qquad {}^{\sigma}d_i = d_i.$$

(3.5.3) Formulation matricielle : Si $A \in M_n(K)$, ${}^tA = {}^\sigma\! A$, alors il existe $P \in GL_n(K)$ telle que la matrice ${}^tPA\,{}^\sigma\! P$ soit diagonale.

Preuve de 3.5.2. **(1) Preuve algorithmique** (dans le cas symétrique bilinéaire) : on écrit $f(x,y) = \sum_{i,j=1}^n A_{ij}x_ix_j \quad (A_{ij} = A_{ji})$, d'où

$$q(x) = f(x,x) = \sum_{i=1}^n A_{ii}\,x_i^2 + 2\sum_{1\le i<j\le n} A_{ij}\,x_ix_j.$$

Il faut trouver un changement de coordonnées qui diagonalise $q(x)$. On peut supposer que $f \neq 0$ ($\Longrightarrow q \neq 0$, grâce à (3.2.9.1)).

(1a) S'il existe un terme diagonal non nul, i.e. si $(\exists i \quad A_{ii} \neq 0)$, on échange x_i et x_1 pour obtenir $A_{11} \neq 0$. La forme $q(x)$ s'écrit alors

$$\begin{aligned} q(x) &= A_{11}x_1^2 + 2A_{12}x_1x_2 + \cdots + 2A_{1n}x_1x_n + q_1(x_2,\ldots,x_n) = \\ &= A_{11}\left(x_1 + \frac{A_{12}}{A_{11}}\,x_2 + \cdots + \frac{A_{1n}}{A_{11}}\,x_n\right)^2 + q_2(x_2,\ldots,x_n) = A_{11}x_1'^2 + q_2(x_2,\ldots,x_n), \end{aligned}$$

où on a noté

$$x_1' = x_1 + \frac{A_{12}}{A_{11}}\,x_2 + \cdots + \frac{A_{1n}}{A_{11}}\,x_n.$$

(1b) Si tous les termes diagonaux s'annulent, i.e. si $(\forall i \quad A_{ii} = 0)$, il existe deux indices $i < j$ tels que $A_{ij} \neq 0$; en échangeant x_i et x_1 (et x_j et x_2), on peut supposer que $A_{12} \neq 0$, donc

$$q(x) = 0\cdot x_1^2 + 2A_{12}x_1x_2 + 0\cdot x_2^2 + \cdots = 2A_{12}\,x_1'^2 + \cdots,$$

où on a posé

$$x_1 = x_1' + x_2', \qquad x_2 = x_1' - x_2' \qquad \left(x_1' = \tfrac{1}{2}(x_1+x_2), \qquad x_2' = \tfrac{1}{2}(x_1 - x_2)\right).$$

Ceci signifie que le cas (1a) s'applique à la forme q exprimée en les variables $x_1', x_2', x_3, \ldots, x_n$; on obtient donc $q(x) = d_1x_1'^2 + q_2(x_2', x_3, \ldots, x_n)$.

Ensuite, on applique le même argument à la forme q_2, etc.

(2) Preuve abstraite On fixe un sous-espace $W \subset V$ supplémentaire à $V^\perp$ ($V = W \oplus V^\perp$) et on note $g : W \times W \longrightarrow K$ la restriction de f à $W \times W$. La matrice de f dans la réunion d'une base de W et d'une base de $V^\perp$ est égale à

$$\begin{pmatrix} B & 0 \\ 0 & 0 \end{pmatrix},$$

où B est la matrice de g. En remplaçant f par g, on se ramène au cas d'une forme non-dégénérée [(1)]. Dans ce cas on a $f \neq 0$, donc $q \neq 0$, i.e. $(\exists e_1' \in V) \quad q(e_1') \neq 0 \Longrightarrow V = Ke_1' \perp (Ke_1')^\perp$. Par récurrence, on obtient $V = Ke_1' \perp Ke_2' \perp \cdots \perp Ke_n'$.

(3.5.4) Exercice. *Trouver une preuve algorithmique dans le cas d'une forme hermitienne.*

(3.5.5) Théorème. *Soit $f : V \times V \longrightarrow K$ une forme bilinéaire alternée. Alors il existe une base de V dans laquelle la matrice de f est égale à*

$$\begin{pmatrix} 0 & I_m & 0 \\ -I_m & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

[(1)] La forme g est, en effet, non-dégénérée : si $x \in W \cap W^\perp$ et $y \in V$, alors $y = w + u$, où $w \in W$ et $u \in V^\perp$; il en résulte que $f(x,y) = f(x, w+u) = f(x,w) + f(x,u) = 0 + 0 = 0$, donc $x \in W \cap V^\perp = \{\vec{0}\}$.

Preuve. Comme dans la preuve abstraite de 3.5.2, on se ramène au cas d'une forme alternée non-dégénérée. Dans ce cas il existe deux vecteurs $e_1, e_1' \in V$ tels que $f(e_1, e_1') \neq 0$. Quitte à multiplier e_1' par un scalaire $\lambda \in K^*$, on peut supposer que $f(e_1, e_1') = 1$. La forme f étant alternée, on a $f(e_1, e_1) = 0$ ($\Longrightarrow e_1' \neq Ke_1$), $f(e_1', e_1') = 0$ et $f(e_1', e_1) = -f(e_1, e_1') = -1$, donc la matrice de la restriction de f au sous-espace $Z = Ke_1 + Ke_1' = Ke_1 \oplus Ke_1' \subset V$ est égale à

$$\begin{pmatrix} f(e_1,e_1) & f(e_1,e_1') \\ f(e_1',e_1) & f(e_1',e_1') \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Cette matrice est inversible, ce qui signifie que $Z \cap Z^\perp = \{\vec{0}\}$, donc la restriction de f à $Z^\perp \times Z^\perp$ est non-dégénérée. On applique le même argument à $Z^\perp$ au lieu de V; on obtient, par récurrence, une base $e_1, \ldots, e_m, e_1', \ldots, e_m'$ de V vérifiant

$$(\forall i, j = 1, \ldots, m) \qquad f(e_i, e_j) = f(e_i', e_j') = 0, \qquad f(e_i, e_j') = -f(e_j', e_i) = \delta_{ij}.$$

(3.5.6) Corollaire. *Si $f : V \times V \longrightarrow K$ est une forme* **symplectique** *(= bilinéaire alternée et non-dégénérée), alors il existe une base de V dans laquelle la matrice de f est égale à*

$$\begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix}.$$

En particulier, la dimension $\dim(V) = 2m$ est **paire**.

(3.5.7) Définition. *Deux formes σ-sesquilinéaires $f : V \times V \longrightarrow K$ et $f' : V' \times V' \longrightarrow K$ sont* **équivalentes** *(notation : $f \sim f'$) s'il existe une bijection linéaire $u : V' \longrightarrow V$ vérifiant*

$$(\forall x', y' \in V') \qquad f'(x', y') = f(u(x'), u(y')). \tag{3.5.7.1}$$

(3.5.8) Formulation matricielle : Si $A = (f(e_i, e_j)) \in M_n(K)$ et $A' = (f'(e_i', e_j')) \in M_n(K)$ sont les matrices de f et f' dans les bases respectives $e_1, \ldots, e_n$ et $e_1', \ldots, e_n'$ de V et V', alors on a :

$$f \sim f' \iff (\exists U \in GL_n(K)) \qquad A' = {}^tU A\, {}^\sigma U$$

(U étant la matrice de u dans les bases $\{e_i'\}$ et $\{e_i\}$).

(3.5.9) Remarques. (i) Soient $f : V \times V \longrightarrow K$ et $f' : V' \times V' \longrightarrow K$ des formes bilinéaires symétriques, $q(x) = f(x, x)$, $q'(x') = f'(x', x')$ les formes quadratiques associées et $u : V' \longrightarrow V$ une bijection linéaire. Grâce à (3.2.9.1), la propriété (3.5.7.1) équivaut à

$$(\forall x' \in V') \qquad q'(x') = q(u(x')). \tag{3.5.9.1}$$

Au lieu d'équivalence $f \sim f'$, on parle souvent d'équivalence $q \sim q'$ (qui est définie en remplaçant (3.5.7.1) par (3.5.9.1)).

(ii) Si on a $f \sim f'$, alors un élément $g \in GL(V')$ est une isométrie de f' $\iff$ on a

$$(\forall x', y' \in V') \qquad f(ug(x'), ug(y')) = f'(g(x'), g(y')) = f'(x', y') = (f(u(x'), u(y')) \iff$$
$$(\forall x, y \in V) \qquad f(ugu^{-1}(x), ugu^{-1}(y)) = f(x, y) \iff$$

$\iff$ ugu^{-1} est une isométrie de f.

(iii) D'après 3.5.6, une forme symplectique quelconque f sur K^n est équivalente à la forme "standard"

$$(x, y) \mapsto {}^t x J y, \qquad J = J_{2m} = \begin{pmatrix} 0 & I_m \\ -I_m & 0 \end{pmatrix} \qquad (x, y \in K^{2m})$$

(où $n = 2m$). La remarque (ii) alors montre que $Sp(f) \subset GL_{2m}(K)$ est conjugué au groupe

$$Sp(2m, K) = Sp_{2m}(K) := \{U \in GL_{2m}(K) \mid {}^tU J_{2m} U = J_{2m}\}.$$

(iv) Si $f \sim f'$, alors on a

$$\begin{aligned} & rg(f)\ (= rg(A))\ = rg(f') \\ & \nu(f) = \nu(f') \\ & \mathrm{disc}(f)\ (= \text{ l'image de } \det(A) \text{ dans } K/\{{}^\sigma\lambda\lambda \mid \lambda \in K^*\})\ = \mathrm{disc}(f'). \end{aligned}$$

(3.5.10) Exercice. *Soient $p_1, \ldots, p_n$ (resp. $q_1, \ldots, q_n$) n nombres premiers distincts. Montrer que les formes quadratiques $p_1x_1^2 + \cdots + p_nx_n^2$ et $q_1x_1^2 + \cdots + q_nx_n^2$ sont équivalentes sur $K = \mathbf{Q} \iff \{p_1, \ldots, p_n\} = \{q_1, \ldots, q_n\}$.*

(3.5.11) Exercice. *Soient $f : V \times V \longrightarrow K$ une forme bilinéaire symétrique non-dégénérée et $u \in GL(V)$.*
(i) *On a : $u \in GO(f) \iff [(\forall x, y \in V) \quad (x \perp y \iff u(x) \perp u(y))]$.*
(ii) *Si le cône isotrope $C(q) = \{x \in V \mid q(x) = 0\}$ n'est pas égal à $\{\vec{0}\}$ (où $q(x) = f(x, x)$), alors on a :*

$$u \in GO(f) \iff u(C(q)) = C(q).$$

(3.5.12) Exercice. *Soient $f : \mathbf{R}^{2n} \times \mathbf{R}^{2n} \longrightarrow \mathbf{R}$ la forme symplectique*

$$f\left(\begin{pmatrix} x \\ y \end{pmatrix}, \begin{pmatrix} x' \\ y' \end{pmatrix}\right) = {}^txy' - {}^tyx' \qquad\qquad (x, y, x', y' \in \mathbf{R}^n).$$

(i) *En écrivant une matrice quelconque $g \in M_{2n}(\mathbf{R})$ sous la forme $g = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ $(A, B, C, D \in M_n(\mathbf{R}))$, caractériser les matrices symplectiques $g \in Sp(f)$ en termes d'un système d'équations pour A, B, C et D.*
(ii) *Déterminer toutes les matrices $g \in Sp(f)$ vérifiant $B = C = 0$.*
(iii) *Déterminer toutes les matrices $g \in Sp(f)$ vérifiant $A = D = I_n$ et $C = 0$.*
(iv) *Déterminer toutes les matrices $g \in Sp(f)$ vérifiant $C = 0$.*
(v) *Déterminer toutes les matrices $Q \in M_n(\mathbf{R})$ telles que l'espace $W = \left\{\begin{pmatrix} Qy \\ y \end{pmatrix} \,\middle|\, y \in \mathbf{R}^n\right\}$ soit totalement isotrope, c'est-à-dire que l'on ait $(\forall u, v \in W) \quad f(u, v) = 0$. Y a-t-il un lien avec les questions précédentes?*

3.6 Diagonalisation simultanée de deux formes quadratiques *

(3.6.1) Exemple : On cherche à trouver un changement de coordonnées qui diagonalise (sur $\mathbf{R}$) à la fois les formes quadratiques

$$f(x_1, x_2) = x_1^2 - x_2^2, \qquad g(x_1, x_2) = 2x_1x_2.$$

Si

$$\begin{aligned} x_1 &= ax_1' + bx_2' \\ x_2 &= cx_1' + dx_2' \end{aligned} \qquad\qquad (ad - bc \neq 0),$$

alors on a

$$\begin{aligned} f(x_1, x_2) &= A'_{11}x_1'^2 + 2(ab - cd)\, x_1'x_2' + A'_{22}x_2'^2 \\ g(x_1, x_2) &= B'_{11}x_1'^2 + 2(ad + bc)\, x_1'x_2' + B'_{22}x_2'^2, \end{aligned}$$

donc on est amené à résoudre le système

* **Ce paragraphe est facultatif.**

$$ab - cd = ad + bc = 0, \qquad ad - bc \neq 0.$$

Comme

$$(ab - cd)^2 + (ad + bc)^2 = (a^2 + c^2)(b^2 + d^2),$$

il n'y a pas de solutions réelles; par contre, $a = d = 1$, $b = c = i$ est une solution complexe.
En résumé, le changement de coordonnées

$$x_1 = x_1' + ix_2', \qquad x_2 = ix_1' + x_2'$$

diagonalise à la fois f et g :

$$f(x_1, x_2) = 2x_1'^2 - 2x_2'^2, \qquad g(x_1, x_2) = 2ix_1'^2 + 2ix_2'^2,$$

mais aucune diagonalisation simultanée de f et g à coefficients réels n'est possible.

(3.6.2) Rappel. Soit $M \in M_n(K)$. Considérons les propriétés suivantes :

(a) La matrice M a n valeurs propres distinctes, toutes contenues dans K.
(b) La matrice M a n vecteurs propres $v_1, \ldots, v_n \in K^n$, linéairement indépendants.
(c) Il existe $P \in GL_n(K)$ telle que la matrice $P^{-1}MP$ soit diagonale.
(d) Toutes les valeurs propres de M sont contenues dans K.

On a

$$(a) \implies (b) \iff (c) \implies (d).$$

En effet, si on note $v_1, \ldots, v_n \in K^n$ les colonnes de la matrice $P \in GL_n(K)$, alors on a

$$P^{-1}MP = \begin{pmatrix} d_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_n \end{pmatrix} = D \iff MP = PD \iff (\forall i = 1, \ldots, n) \qquad Mv_i = d_i v_i.$$

(3.6.3) Proposition. *Soient $F, G : V \times V \longrightarrow K$ ($\mathrm{car}(K) \neq 2$) des formes bilinéaires symétriques et $f(x) = F(x,x)$, $g(x) = G(x,x)$ les formes quadratiques associées. Soient $A = (F(e_i, e_j)), B = (G(e_i, e_j)) \in M_n(K)$ les matrices de F et G dans une base $e_1, \ldots, e_n$ de V. Si la forme G est non-dégénérée, alors les propriétés suivantes sont équivalentes :*
(i) *Il existe une base $e_1', \ldots, e_n'$ de V telle que les matrices $A' = (F(e_i', e_j'))$ et $B' = (G(e_i', e_j'))$ soient diagonales.*
(ii) *Il existe $P \in GL_n(K)$ telle que la matrice $P^{-1}(B^{-1}A)P$ soit diagonale.*

Preuve. "(i) $\implies$ (ii)" : On a $A' = {}^tPAP$ et $B' = {}^tPBP$, où $P \in GL_n(K)$ est la matrice de changement de base. Par hypothèse, B est inversible et les matrices A', B' sont diagonales, donc la matrice $P^{-1}(B^{-1}A)P = (B')^{-1}A'$ est aussi diagonale.

"(ii) $\implies$ (i)" : Si la matrice $P^{-1}(B^{-1}A)P = D$ est diagonale, on peut supposer (quitte à multiplier P par une matrice de permutation) que

$$D = \begin{pmatrix} d_1 \cdot I_{n_1} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_r \cdot I_{n_r} \end{pmatrix},$$

où les valeurs $d_1, \ldots, d_r \in K$ sont **distinctes** et $n_1 + \cdots + n_r = n$. On écrit la matrice $A' := {}^tPAP$ sous la forme

$$A' = \begin{pmatrix} A'_{11} & \cdots & A'_{1r} \\ \vdots & \ddots & \vdots \\ A'_{r1} & \cdots & A'_{rr} \end{pmatrix},$$

où $A'_{ij} \in M_{n_i,n_j}(K)$ $(i, j = 1, \dots, r)$, et de même pour $B' := {}^tPBP$. Les équations

$$A' = B'D, \qquad {}^tA' = A', \qquad {}^tB' = B'$$

entraînent, pour tous $i, j = 1, \dots, r$,

$$d_j B'_{ij} = A'_{ij} = A'_{ji} = d_i B'_{ji} = d_i B'_{ij} \implies (d_i - d_j) B'_{ij} = 0,$$

donc $A'_{ij} = B'_{ij} = 0$ si $i \neq j$:

$$A' = \begin{pmatrix} A'_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & A'_{rr} \end{pmatrix}, \qquad B' = \begin{pmatrix} d_1 A'_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_r A'_{rr} \end{pmatrix}.$$

Comme chaque matrice $A'_{ii} \in M_{n_i}(K)$ est symétrique, il existe $Q_i \in GL_{n_i}(K)$ telle que ${}^tQ_i A'_{ii} Q_i$ (donc aussi ${}^tQ_i B'_{ii} Q_i = d_i {}^tQ_i A'_{ii} Q_i$) soit diagonale. Il en résulte que, si on pose

$$Q = \begin{pmatrix} Q_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & Q_r \end{pmatrix} \in GL_n(K),$$

alors les matrices ${}^t(PQ)A(PQ) = {}^tQA'Q$ et ${}^t(PQ)B(PQ) = {}^tQB'Q$ seront diagonales.

(3.6.4) Exemple : En 3.6.1, on a

$$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad B^{-1}A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix};$$

les valeurs propres de la matrice $B^{-1}A$ sont égales à $\pm i$.

(3.6.5) Exercice. *Que se passe-t-il si $B = I$ et $K = \mathbf{R}$ (resp. $K = \mathbf{C}$)?*

(3.6.6) Exercice. *Trouver un exemple de deux formes quadratiques non-dégénérées réelles f, g sur $\mathbf{R}^2$ qui n'admettent pas une diagonalisation simultanée sur $\mathbf{C}$.*

3.7 Formes quadratiques et hermitiennes sur R et C

(3.7.1) Rappel. Un corps K est dit **algébriquement clos** si tout polynôme non-constant $f \in K[X]$ a une racine $\alpha \in K$. Par exemple, le corps $\mathbf{C}$ est algébriquement clos.

(3.7.2) Théorème. (i) *Si le corps K ($\mathrm{car}(K) \neq 2$) est algébriquement clos, toute forme bilinéaire symétrique sur K^n est équivalente à la forme $x_1y_1 + \cdots + x_ry_r$, où $0 \leq r = rg(f) \leq n$ ($\implies$ la forme quadratique associée est équivalente à la forme $x_1^2 + \cdots + x_r^2$).*
(ii) *(Sylvester) Si $K = \mathbf{R}$, pour toute forme bilinéaire symétrique f sur $\mathbf{R}^n$ il existe un unique couple d'entiers $r, s \geq 0$ ($r + s = rg(f) \leq n$) tel que l'on ait $f \sim x_1y_1 + \cdots + x_ry_r - x_{r+1}y_{r+1} - \cdots - x_{r+s}y_{r+s}$ ($\implies$ la forme quadratique associée est équivalente à la forme $x_1^2 + \cdots + x_r^2 - x_{r+1}^2 - \cdots - x_{r+s}^2$).*
(iii) *Si $K = \mathbf{C}$ et $\sigma(a + bi) = a - bi$, pour toute forme hermitienne f sur $\mathbf{C}^n$ il existe un unique couple d'entiers $r, s \geq 0$ ($r + s = rg(f) \leq n$) tel que l'on ait $f \sim x_1\overline{y_1} + \cdots + x_r\overline{y_r} - x_{r+1}\overline{y_{r+1}} - \cdots - x_{r+s}\overline{y_{r+s}}$.*

Preuve. (i) D'après 3.5.9(i), il suffit de démontrer que $q \sim x_1^2 + \cdots + x_r^2$. On sait qu'il existe une base orthogonale de V, ce qui entraîne que $q \sim a_1x_1^2 + \cdots + a_rx_r^2$, où $a_j \in K^*$ $(j = 1, \dots, r)$ et $r = rg(f)$. Le

corps K étant algébriquement clos, pour tout $j = 1, \dots, r$ il existe $\alpha_j \in K^*$ tel que $\alpha_j^2 = a_j$; le changement de coordonnées $x_j := x_j/\alpha_j$ montre alors que $a_1x_1^2 + \cdots + a_rx_r^2 \sim x_1^2 + \cdots + x_r^2$.
(ii) Le même argument montre qu'on a $q \sim \sum_{i=1}^r a_ix_i^2 - \sum_{j=1}^s a_{r+j}x_{r+j}^2$, où $a_k > 0$ ($k = 1, \dots, r+s$), donc $q \sim \sum_{i=1}^r x_i^2 - \sum_{j=1}^s x_{r+j}^2$ (puisque tout nombre réel positif est un carré). On a $r + s = rg(f)$; il reste à démontrer que l'entier r est déterminé par f. On se ramène d'abord au cas $r + s = n$ comme dans la preuve abstraite de 3.5.2. Soient $e_1, \dots, e_n$ et $e'_1, \dots, e'_n$ deux bases orthogonales de $\mathbf{R}^n$ vérifiant

$$q(e_i) = \begin{cases} 1, & 1 \le i \le r \\ -1, & r+1 \le i \le n \end{cases} \qquad q(e'_i) = \begin{cases} 1, & 1 \le i \le r' \\ -1, & r'+1 \le i \le n. \end{cases}$$

On pose

$$W_+ = Ke_1 + \cdots + Ke_r \qquad W'_+ = Ke_1 + \cdots + Ke_{r'}$$
$$W_- = Ke_{r+1} + \cdots + Ke_n \qquad W'_- = Ke_{r'+1} + \cdots + Ke_n$$

Les inégalités

$$(\forall x \in W_+ - \{\vec{0}\}) \qquad q(x) > 0, \qquad (\forall x \in W'_- - \{\vec{0}\}) \qquad q(x) < 0$$

entraînent

$$W_+ \cap W'_- = \{\vec{0}\} \implies \underbrace{\dim(W_+)}_{r} + \underbrace{\dim(W'_-)}_{n-r'} \le n \implies r \le r'.$$

En échangeant les rôles des bases $\{e_i\}$ et $\{e'_i\}$, on obtient $r' \le r$, d'où $r = r'$.
(iii) Exercice.

(3.7.3) Notation. (i) On note $O_n(K)$ le groupe des isométries de la forme symétrique bilinéaire $x_1y_1 + \cdots + x_ny_n$, et on pose $SO_n(K) = O_n(K) \cap SL_n(K)$.
(ii) Si $K = \mathbf{R}$, on note $O_{r,n-r}(\mathbf{R}) = O(r, n-r)$ le groupe des isométries de la forme symétrique bilinéaire $x_1y_1 + \cdots + x_ry_r - x_{r+1}y_{r+1} - \cdots - x_ny_n$, et on pose $SO_{r,n-r}(\mathbf{R}) = SO(r, n-r) = O_{r,n-r}(\mathbf{R}) \cap SL_n(\mathbf{R})$.
(ii) Si $K = \mathbf{C}$, on note $U_{r,n-r}(\mathbf{C}) = U(r, n-r)$ le groupe des isométries de la forme hermitienne $x_1\overline{y_1} + \cdots + x_r\overline{y_r} - x_{r+1}\overline{y_{r+1}} - \cdots - x_n\overline{y_n}$, et on pose $SU_{r,n-r}(\mathbf{C}) = SU(r, n-r) = U_{r,n-r}(\mathbf{C}) \cap SL_n(\mathbf{C})$.

(3.7.4) Exercice. *Soient $f : \mathbf{R}^2 \times \mathbf{R}^2 \longrightarrow \mathbf{R}$ la forme symétrique bilinéaire dont la forme quadratique est égale à $q(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}) = 2x_1x_2$.*
(i) *Déterminer la matrice de f (dans la base canonique) et son groupe des isométries $O(f) \subset GL_2(\mathbf{R})$.*
(ii) *Montrer que le sous-groupe $SO(f) = O(f)^+ \subset O(f)$ est commutatif.*
(iii) *Montrer que tout élément $g \in O(f)^+$ s'écrit $g = h_1h_2$, $h_i \in O(f)^- := O(f) - O(f)^+$.*
(iv) *Montrer : si $g \in O(f)^+$ et $h \in O(f)^-$, alors on a $hgh^{-1} = g^{-1}$.*
(v) *Montrer : $g \in O(f)$ est une réflexion $\iff$ $g \in O(f)^-$.*
(vi) *Montrer : si $x, y \in \mathbf{R}^2$ et $q(x) = q(y) \ne 0$, alors il existe une réflexion $\tau \in O(f)$ telle que $\tau(x) = y$. Que se passe-t-il si $q(x) = q(y) = 0$?*
(vii) *Montrer que tout élément $g \in O(f)$ est diagonalisable sur $\mathbf{R}$.*
(viii) *Peut-on déduire de (ii)-(vii) les énoncés analogues pour un groupe de type $O(r, s)$?*

3.8 Quadriques projectives

Soit K un corps, $\mathrm{car}(K) \ne 2$.

(3.8.1) Soit $A = {}^tA \in M_{n+1}(K)$, $A \ne 0$, une matrice symétrique non nulle; on note $q = \sum_{i,j=0}^n A_{ij}X_iX_j$ la forme quadratique associée (on a $q \ne 0$, d'après (3.2.9.1)). L'équation $q = 0$ définit une **quadrique projective** $Q \subset \mathbf{P}^n$ (sur K). Si $n = 2$, on parle d'une **conique projective**. Pour tout corps $L \supset K$, l'ensemble des points L-rationnels de Q est égal à

$$Q(L) = \{(X_0 : \cdots : X_n) \in \mathbf{P}^n(L) \mid q(X_0, \cdots, X_n) = 0\} = \pi(C(q_L) - \{\vec{0}\}),$$

où $\pi : L^{n+1} - \{\vec{0}\} \longrightarrow \mathbf{P}^n(L)$ est la projection usuelle (voir 2.3.1) et

$$C(q_L) = \text{ le cône isotrope } \{x \in L^{n+1} \mid q(x) = 0\}.$$

On définit

$$rg(Q) := rg(q) = rg(A).$$

(3.8.2) (i) Il se peut que $Q(K) = \emptyset$ ($\iff$ $C(q) = \{\vec{0}\}$) : par exemple, si $K = \mathbf{R}$, $n = 1$ et $q = X_0^2 + X_1^2$.
(ii) **Exercice :** Soient $Q, Q' \subset \mathbf{P}^n$ des quadriques projectives (sur K) $Q : q = 0$, $Q' : q' = 0$. Si le corps K est algébriquement clos (par exemple, si $K = \mathbf{C}$), alors on a :

$$[Q(K) = Q'(K) \iff (\exists \lambda \in K^*) \qquad q' = \lambda q]\,.$$

(iii) Pour tout corps K il existe un corps algébriquement clos contenant K.

(3.8.3) Définition. *Une quadrique projective $Q : q = 0 \subset \mathbf{P}^n$ est non-singulière (= lisse) si la forme quadratique q est non-dégénérée ($\iff$ $\det(A) \neq 0 \iff rg(Q) = n + 1$).*

Par exemple, si $n = 2$, les coniques

$$X_0^2 = 0 \qquad \text{(une droite double)}, \qquad X_0^2 - X_1^2 = 0 \qquad \text{(deux droites distinctes)}$$

sont singulières, mais la conique

$$X_0^2 - X_1^2 - X_2^2 = 0$$

est non-singulière.

(3.8.4) Définition. *Deux quadriques projectives $Q : q = 0$ et $Q' : q' = 0$ sur K (dans $\mathbf{P}^n$) sont* **équivalentes** *(sur K) s'il existe un changement de coordonnées homogènes qui transforme q en un multiple scalaire de q', i.e. si*

$$(\exists \lambda \in K^*)\ (\exists P \in GL_{n+1}(K)) \qquad {}^tPAP = \lambda A'$$

(où $q(x) = {}^txAx$, $q'(x) = {}^txA'x$). Si c'est le cas, alors on a $rg(Q) = rg(Q')$; en particulier, Q est non-singulière $\iff$ Q' l'est.

(3.8.5) On a une bijection évidente

$$\begin{array}{c}\{\text{classes d'équivalence des formes quadratiques (sur } K) \ \ q(X_0, \ldots, X_n) \neq 0\}/K^* \\ \downarrow \wr \\ \{\text{classes d'équivalence des quadriques projectives (sur } K) \ \ Q \subset \mathbf{P}^n\}\end{array}$$

(3.8.6) Classification sur un corps algébriquement clos. Si K est algébriquement clos (par exemple, si $K = \mathbf{C}$), les classes d'équivalence

$$\{q(X_0, \ldots, X_n) \neq 0\}/\sim$$

sont représentées par les formes

$$q_r = X_0^2 + \cdots + X_{r-1}^2, \qquad\qquad (1 \leq r = rg(q_r) \leq n + 1)$$

(d'après 3.7.2(i)). Pour tout $\lambda \in K^*$ il existe $\alpha \in K^*$ vérifiant $\lambda = \alpha^2$. Comme $\lambda X_j^2 = (\alpha X_j)^2$, le changement de coordonnées $\alpha X_j \mapsto X_j$ montre que l'on a $\lambda q_r \sim q_r$, donc il y a $n + 1$ classes de quadriques projectives $Q \subset \mathbf{P}^n$ sur K, représentées par les équations respectives

$$X_0^2 + \cdots + X_{r-1}^2 = 0 \qquad\qquad (1 \le r \le n+1).$$

L'unique classe de quadriques non-singulières correspond à $r = n+1$.

(3.8.7) Classification sur $K = \mathbf{R}$. D'après 3.7.2(ii), les classes d'équivalence

$$\{q(X_0, \ldots, X_n) \neq 0\}/\sim$$

sont représentées par les formes

$$q_{r,s} = X_0^2 + \cdots + X_{r-1}^2 - X_r^2 - \cdots - X_{r+s-1}^2 \qquad\qquad (0 \le r, s;\ 1 \le r+s = rg(q_{r,s}) \le n+1).$$

Soit $\lambda \in \mathbf{R}^*$; si $\lambda > 0$, alors $\lambda = (\sqrt{\lambda})^2$, donc $\lambda q_{r,s} \sim q_{r,s}$. Par contre, si $\lambda < 0$, alors $\lambda = -(\sqrt{-\lambda})^2$, donc $\lambda q_{r,s} \sim -q_{r,s} \sim q_{s,r}$. Il en résulte que les classes de quadriques projectives $Q \subset \mathbf{P}^n$ sur $\mathbf{R}$ sont représentées par les équations

$$X_0^2 + \cdots + X_{r-1}^2 - X_r^2 - \cdots - X_{r+s-1}^2 = 0 \qquad\qquad (0 \le s \le r;\ 1 \le r+s \le n+1).$$

Les classes des quadriques non-singulières correspondent aux valeurs $0 \le s \le r$; $r+s = n+1$.

(3.8.8) Classification de coniques ($n = 2$) : (i) $K = \mathbf{C}$:

$rg = 1 :\quad X_0^2 = 0$ (une droite double).
$rg = 2 :\quad X_0^2 + X_1^2 = (X_0 + iX_1)(X_0 - iX_1) = 0$ (deux droites).
$rg = 3 :\quad X_0^2 + X_1^2 + X_2^2 = 0$ (une conique non-singulière).

(ii) $K = \mathbf{R}$:

$rg = 1 :\quad X_0^2 = 0$ (une droite double).
$rg = 2 :\quad X_0^2 + X_1^2 = (X_0 + iX_1)(X_0 - iX_1) = 0$ (deux droites complexes conjuguées)
$\qquad\qquad X_0^2 - X_1^2 = (X_0 + X_1)(X_0 - X_1) = 0$ (deux droites réelles).
$rg = 3 :\quad X_0^2 + X_1^2 + X_2^2 = 0$ (une conique non-singulière sans aucun point réel)
$\qquad\qquad X_0^2 + X_1^2 - X_2^2 = 0$ (une conique non-singulière ayant un point réel).

(3.8.9) Exercice. (i) *Soit $Q : q(X_0, X_1, X_2) = 0$ une conique projective non-singulière (sur K), $O \in Q(K)$ et $D \subset \mathbf{P}^2(K)$ une droite qui ne passe pas par O. Montrer que la projection de centre O induit une bijection*

$$f : Q(K) \xrightarrow{\sim} D.$$

Si $D' \subset \mathbf{P}^2(K)$ est une autre droite qui ne passe pas par O et si $f' : Q(K) \xrightarrow{\sim} D'$ est la bijection définie de la même façon, montrer que la bijection $f' \circ f^{-1} : D \xrightarrow{\sim} D'$ est une homographie.
(ii) *En utilisant (i), déterminer toutes les solutions entières de l'équation $a^2 + b^2 = c^2$.*
(iii) *Que se passe-t-il en dimension supérieure? En particulier, peut-on déterminer toutes les solutions entières de l'équation $x_1^2 + \cdots + x_n^2 = x_0^2$?*

(3.8.10) Exercice. *La quadrique projective*

$$X_0^2 + X_1^2 - X_2^2 - X_3^2 = 0 \qquad (\subset \mathbf{P}^3)$$

sur un corps K s'écrit aussi

$$Q : Y_0Y_3 - Y_1Y_2 = 0,$$

où

$$Y_0 = X_0 + X_3, \qquad Y_3 = X_0 - X_3, \qquad Y_1 = X_2 + X_1, \qquad Y_2 = X_2 - X_1.$$

Montrer que l'application

$$(a:b),\ (c:d) \mapsto (ac : ad : bc : bd)$$

définit une bijection

$$\mathbf{P}^1(K) \times \mathbf{P}^1(K) \xrightarrow{\sim} Q(K).$$

En particulier, $Q(K)$ contient deux systèmes transverses de droites.

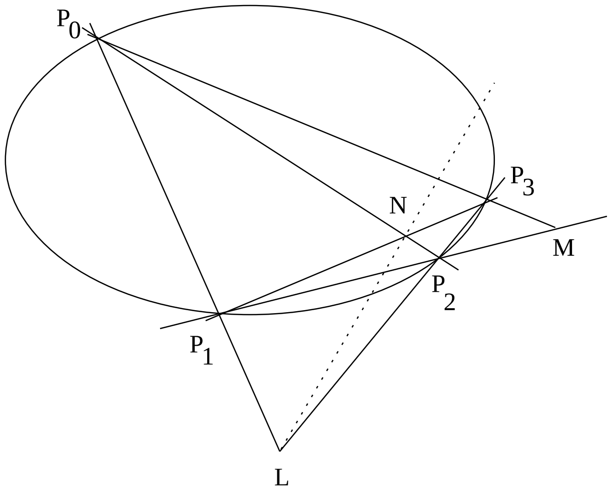
(3.8.11) Exercice. (i) *Soient $d_1, d_2, d_3 \subset \mathbf{P}^3(K)$ trois droites projectives telles que $d_1 \cap d_2 = d_2 \cap d_3 = d_3 \cap d_1 = \emptyset$. Déterminer l'ensemble de points $P \in \mathbf{P}^3(K)$ par lesquels passe au moins une droite projective qui intersecte toutes les droites d_1, d_2, d_3.*
(ii) *Déduire de (i) une solution de 2.4.9 pour $n = 4$ et $K = \mathbf{R}$.*

(3.8.12) Exercice. (i) *Soit P_0, P_1, P_2, P_3 un repère projectif d'un plan projectif réel Y. On choisit un système de coordonnées homogènes $(X_0 : X_1 : X_2)$ de Y et, pour tous $0 \leq i < j \leq 3$, une équation*

$$\ell_{ij} = a_{ij}X_0 + b_{ij}X_1 + c_{ij}X_2 = 0$$

de la droite $d_{ij} = (P_iP_j)$. Pour tout $\lambda = (a : b) \in \mathbf{P}^1(\mathbf{R})$ on définit une quadrique (= une conique) projective réelle $Q_\lambda \subset \mathbf{P}^2$ par l'équation quadratique suivante :

$$Q_\lambda : a\ell_{01}\ell_{23} + b\ell_{12}\ell_{03} = 0.$$



Déterminer toutes les coniques Q_λ qui sont singulières.
(ii) *Montrer que l'on a*

$$\{Q_\lambda \mid \lambda \in \mathbf{P}^1(\mathbf{R})\} = \{\text{coniques projectives réelles } Q \subset \mathbf{P}^2 \text{ qui passent par } P_0, P_1, P_2, P_3\}.$$

(iii) *Montrer que pour tout point $P_4 \in Y$ distinct de P_0, P_1, P_2, P_3 il existe une unique conique projective réelle $Q \subset \mathbf{P}^2$ qui passe par P_0, P_1, P_2, P_3 et P_4.*
(iv) *On note $L = d_{01} \cap d_{23}$, $M = d_{12} \cap d_{03}$ et $N = d_{02} \cap d_{13}$. Montrer que pour tout $\lambda \in \mathbf{P}^1(\mathbf{R})$ les points $L, N, R_\lambda, S_\lambda$ forment une division harmonique, où l'on a noté $(LN) \cap Q_\lambda = \{R_\lambda, S_\lambda\}$.*
(v) *Soit $d \subset Y$ une droite projective distincte de $d_{01}, \ldots, d_{23}$. Montrer qu'il existe une homographie $h : d \longrightarrow d$ ($h \neq \mathrm{id}$) qui satisfait à la propriété suivante : pour tout $\lambda \in \mathbf{P}^1(\mathbf{R})$ et tout point d'intersection $P \in d \cap Q_\lambda$ on a $h(P) \in d \cap Q_\lambda$.*
(vi) *Il y a combien de coniques projectives réelles $Q \subset \mathbf{P}^2$ qui passent par P_0, P_1, P_2, P_3 et qui sont tangentes à d ?* *[Indication : bien choisir les coordonnées homogènes.]*

3.9 Quadriques affines

Soit K un corps, $\mathrm{car}(K) \neq 2$.

(3.9.1) Quadrique projective $\Longrightarrow$ quadrique affine : Soit $Q : q(X_0, \ldots, X_n) = 0$ une quadrique projective sur K. Les points K-rationnels $Q(K) = \pi(C(q) - \{\vec{0}\})$ de la quadrique Q correspondent aux droites vectorielles $D \subset K^{n+1}$ contenues dans le cône isotrope

$$C(q) = \{{}^t(X_0, \ldots, X_n) \in K^{n+1} \mid q(X_0, \ldots, X_n) = 0\}.$$

On choisit $H_0 = \{X_0 = 0\} \subset \mathbf{P}^n(K)$ comme l'hyperplan à l'infini et on identifie l'espace affine $\mathbf{P}^n(K) - H_0$ à l'hyperplan affine $\{X_0 = 1\} \subset K^{n+1}$ comme en 2.3.4 :

$$\begin{array}{cccccc} \mathbf{P}^n(K) - H_0 & \stackrel{\sim}{\longrightarrow} & \{X_0 = 1\} & \stackrel{\sim}{\longrightarrow} & K^n \\ (X_0 : \cdots : X_n),\ X_0 \neq 0 & \mapsto & (1, X_1/X_0, \ldots, X_n/X_0) & \mapsto & (X_1/X_0, \ldots, X_n/X_0) \\ \text{droite vectorielle } D \subset K^{n+1},\ D \not\subset \{X_0 = 0\} & \mapsto & D \cap \{X_0 = 1\} & & \end{array}$$

Il en résulte que $Q(K) \cap (\mathbf{P}^n(K) - H_0)$ s'identifie naturellement à l'intersection du cône $C(q)$ et de l'hyperplan affine $\{X_0 = 1\}$:

$$\begin{array}{rcl} Q(K) \cap (\mathbf{P}^n(K) - H_0) & \stackrel{\sim}{\longrightarrow} & C(q) \cap \{X_0 = 1\} \\ \text{droite vectorielle } D \subset C(q),\ D \not\subset \{X_0 = 0\} & \mapsto & D \cap \{X_0 = 1\} \end{array}$$

En utilisant les coordonnées affines $x_i = X_i/X_0$ $(i = 1, \ldots, n)$ dans $\{X_0 = 1\}$, l'équation de $C(q) \cap \{X_0 = 1\}$ s'écrit

$$\sum_{i,j=0}^{n} A_{ij} \frac{X_i}{X_0} \frac{X_j}{X_0} = A_{00} + 2 \sum_{i=1}^{n} A_{0i}\, x_i + \sum_{i,j=1}^{n} A_{ij}\, x_i x_j = 0.$$

(3.9.2) Quadriques affines. Réciproquement, soit $x_1, \ldots, x_n$ un système de coordonnées cartésiennes dans un espace affine (de dimension n). Une **quadrique affine** (sur K) est définie par une équation

$$Q : q(x) = \sum_{i,j=1}^{n} a_{ij}\, x_i x_j + 2 \sum_{i=1}^{n} b_i\, x_i + c = {}^t x a x + 2\, {}^t b x + c = 0 \qquad (x \in K^n),$$

où $a = {}^t a \in M_n(K) - \{0\}$, $b \in K^n$, $c \in K$. La **projectivisée de** Q est la quadrique projective

$$\widetilde{Q} : \widetilde{q}(X) = 0 \qquad (\widetilde{Q} \subset \mathbf{P}^n), \qquad \widetilde{q}(X_0, \ldots, X_n) = X_0^2\, q(X_1/X_0, \ldots, X_n/X_0) = {}^t X A X,$$

où l'on a posé

$$A = \widetilde{a} = \begin{pmatrix} a & b \\ {}^t b & c \end{pmatrix}, \qquad X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \\ X_0 \end{pmatrix}, \quad \text{i.e.}$$

$$\widetilde{Q} : \sum_{i,j=1}^{n} a_{ij}\, X_i X_j + 2 \sum_{i=1}^{n} b_i\, X_i X_0 + c X_0^2 = 0, \qquad \widetilde{Q}(K) \cap \{X_0 = 1\} = Q(K).$$

(3.9.3) Changement de coordonnées. Un changement de coordonnées affines $x = Px' + p$ ($P \in GL_n(K)$, $p \in K^n$) s'écrit sous la forme matricielle

$$\begin{pmatrix} x \\ 1 \end{pmatrix} = \widetilde{P} \begin{pmatrix} x' \\ 1 \end{pmatrix}, \qquad \widetilde{P} = \begin{pmatrix} P & p \\ 0 & 1 \end{pmatrix} \in GL_{n+1}(K)$$

(voir 1.6.4-5). L'équation $Q : q(x) = 0$ est transformée en l'équation

$$q'(x') = {}^t(Px' + p) a (Px' + p) + 2\, {}^t b (Px' + p) + c = {}^t(x') a' x' + 2\, {}^t(b') x' + c' = 0,$$

où

$$\widetilde{a}' = \begin{pmatrix} a' & b' \\ {}^t(b') & c' \end{pmatrix} = {}^t\widetilde{P}\widetilde{a}\widetilde{P} = {}^t\begin{pmatrix} P & p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ {}^tb & c \end{pmatrix} \begin{pmatrix} P & p \\ 0 & 1 \end{pmatrix}.$$

(3.9.4) Définition. *Deux quadriques affines*

$$Q : q(x) = {}^txax + 2\,{}^tbx + c = 0, \qquad Q' : q'(x) = {}^txa'x + 2\,{}^t(b')x + c' = 0$$

(dans un espace affine de dimension $n \geq 1$) sont **équivalentes** *(sur K) s'il existe un changement de coordonnées affines qui transforme q en un multiple scalaire de q', i.e. si*

$$(\exists P \in GL_n(K))\,(\exists p \in K^n)\,(\exists \lambda \in K^*) \qquad {}^t\begin{pmatrix} P & p \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ {}^tb & c \end{pmatrix} \begin{pmatrix} P & p \\ 0 & 1 \end{pmatrix} = \lambda \begin{pmatrix} a' & b' \\ {}^t(b') & c' \end{pmatrix}.$$

Si c'est le cas, alors les projectivisées $\widetilde{Q}$ et $\widetilde{Q}'$ sont équivalentes (mais la réciproque est fausse : voir 2.3.12) et on a ${}^tPaP = \lambda a'$.

(3.9.5) Définition. Le rang *$rg(Q) := rg(a)$ ne dépend que de la classe d'équivalence de Q; on a*

$$rg(Q) = rg(a) \leq rg(\widetilde{a}) = rg(\widetilde{Q}).$$

(3.9.6) Trois familles de quadriques affines. Soit

$$Q : q(x) = {}^txax + 2\,{}^tbx + c = 0$$

une quadrique affine sur K. Pour simplifier cette équation, on diagonalise d'abord la partie quadratique : d'après 3.5.2-3, il existe $P \in GL_n(K)$ tel que la matrice ${}^tPaP$ soit diagonale; en remplaçant x par Px, on peut supposer que Q s'écrit sous la forme diagonale

$$Q : \sum_{i=1}^r a_i x_i^2 + 2\sum_{i=1}^n b_i x_i + c = 0 \qquad\qquad (r = rg(Q), \quad \prod_{i=1}^r a_i \neq 0).$$

Ensuite, on écrit, pour tout $i = 1, \ldots, r$,

$$a_i x_i^2 + 2\,b_i x_i = a_i(x_i + b_i/a_i)^2 - b_i^2/a_i;$$

en remplaçant $x_i + b_i/a_i$ par x_i et c par $c - \sum_{i=1}^r b_i^2/a_i$, on obtient l'équation

$$Q : \sum_{i=1}^r a_i x_i^2 + 2\sum_{i=r+1}^n b_i x_i + c = 0, \qquad\qquad \prod_{i=1}^r a_i \neq 0.$$

Si tous les coefficients b_i ($i = r+1, \ldots, n$) s'annulent, quitte à multiplier par $1/c$ (si $c \neq 0$), on obtient les équations respectives

$$(I) \qquad Q : \sum_{i=1}^r a_i x_i^2 = 0, \qquad \prod_{i=1}^r a_i \neq 0, \qquad 1 \leq r \leq n$$

(si $c = 0$), resp.

$$(II) \qquad Q : \sum_{i=1}^r a_i x_i^2 + 1 = 0, \qquad \prod_{i=1}^r a_i \neq 0, \qquad 1 \leq r \leq n$$

(si $c \neq 0$).

S'il existe $j \in \{r+1, \ldots, n\}$ tel que $b_j \neq 0$ (on a forcément $r \leq n-1$ dans ce cas), on échange d'abord x_j et x_n (donc b_n deviendra non nul) et ensuite on remplace $\sum_{i=r+1}^{n} b_i x_i$ par x_n. L'équation de Q se simplifie alors en

$$(III) \qquad Q : \sum_{i=1}^{r} a_i x_i^2 + 2x_n = 0, \qquad \prod_{i=1}^{r} a_i \neq 0, \qquad 1 \leq r \leq n-1.$$

Dans les trois cas respecrifs (I), (II) et (III), on a

$$\begin{array}{lll} (I) & rg(Q) = r, & rg(\widetilde{Q}) = r \\ (II) & rg(Q) = r, & rg(\widetilde{Q}) = r+1 \\ (III) & rg(Q) = r, & rg(\widetilde{Q}) = r+2 \end{array}$$

On en déduit que deux quadriques affines appartenant à deux familles distinctes ne sont pas équivalentes (puisque $rg(Q)$ et $rg(\widetilde{Q})$ ne dépendent que de la classe d'équivalence de Q).

La projectivisée $\widetilde{Q}$ est non-singulière $\iff$ on est dans le cas (II), $r = n$ (resp. (III), $r = n-1$).

(3.9.7) Quadriques affines sur C. Si $K = \mathbf{C}$ (plus généralement, si le corps K est algébriquement clos), il résulte de 3.8.6 et 3.9.6 que les classes d'équivalence de quadriques affines $Q \subset K^n$ sont representées par les quadriques suivantes :

$$\begin{array}{rll} I(r) : & \sum_{j=1}^{r} x_j^2 = 0 & (1 \leq r \leq n) \\ II(r) : & \sum_{j=1}^{r} x_j^2 + 1 = 0 & (1 \leq r \leq n) \\ III(r) : & \sum_{j=1}^{r} x_j^2 + 2x_n = 0 & (1 \leq r \leq n-1) \end{array}$$

La projectivisée $\widetilde{Q}$ est non-singulière $\iff$ on est dans le cas II(n) ou III($n-1$).

(3.9.7) Quadriques affines sur R. Si $K = \mathbf{R}$, on déduit de 3.8.7 et 3.9.7 que les classes d'équivalence de quadriques affines réelles $Q \subset \mathbf{R}^n$ sont representées par les quadriques suivantes :

$$\begin{array}{rll} I(r,s) : & \sum_{i=1}^{r} x_i^2 - \sum_{j=1}^{s} x_{r+j}^2 = 0 & (0 \leq s \leq r,\ 1 \leq r+s = rg(Q) \leq n) \\ II(r,s) : & \sum_{i=1}^{r} x_i^2 - \sum_{j=1}^{s} x_{r+j}^2 + 1 = 0 & (r, s \geq 0,\ 1 \leq r+s = rg(Q) \leq n) \\ III(r,s) : & \sum_{i=1}^{r} x_i^2 - \sum_{j=1}^{s} x_{r+j}^2 + 2x_n = 0 & (0 \leq s \leq r,\ 1 \leq r+s = rg(Q) \leq n-1) \end{array}$$

(si on a $r < s$ dans le cas III(r, s), on multiplie l'équation par (-1) et on remplace x_n par $-x_n$).

La projectivisée $\widetilde{Q}$ est non-singulière $\iff$ on est dans le cas II($r, n-r$) ou (III($r, n-1-r$), $r \geq (n-1)/2$).

(3.9.8) Exemple : coniques affines réelles. Si $K = \mathbf{R}$ et $n = 2$, on a les classes suivantes :

$$\begin{aligned}
I(1,0) &: x_1^2 = 0\\
I(1,1) &: x_1^2 - x_2^2 = 0\\
I(2,0) &: x_1^2 + x_2^2 = 0\\
II(0,1) &: -x_1^2 + 1 = 0\\
II(0,2) &: -x_1^2 - x_2^2 + 1 = 0\\
II(1,0) &: x_1^2 + 1 = 0\\
II(1,1) &: x_1^2 - x_2^2 + 1 = 0\\
II(2,0) &: x_1^2 + x_2^2 + 1 = 0\\
III(1,0) &: x_1^2 + 2x_2 = 0
\end{aligned}$$

Respectivement : une droite réelle double, deux droites réelles non-parallèles, deux droites imaginaires non-parallèles, deux droites réelles parallèles, une ellipse, deux droites imaginaires parallèles, une hyperbole, une conique sans points réels dont la projectivisée est non-singulière, une parabole.

(3.9.9) Exercice. *Classifier les quadriques affines réelles $Q \subset \mathbf{R}^3$.*

(3.9.10) Exercice. *Considérons les quadriques affines réelles $Q_i \subset \mathbf{R}^3$ suivantes :*

$$Q_1 : x^2 + y^2 + z^2 = 1, \qquad Q_2 : z^2 = xy - 1, \qquad Q_3 : z^2 = xy + 1,$$
$$Q_4 : z^2 = xy, \qquad Q_5 : z = x^2 + y^2, \qquad Q_4 : z = xy.$$

Décrire le type géométrique de chaque quadrique Q_i. On note $\widetilde{Q}_i \subset \mathbf{P}^3(\mathbf{R})$ la projectivisée de Q_i. Pour quels couples d'indices $i \neq j$ les quadriques projectives $\widetilde{Q}_i$ et $\widetilde{Q}_j$ sont-elles équivalentes (resp., ne le sont pas)?

(3.9.11) Exercice. (i) *Donner des représentants de toutes les classes d'équivalence de quadriques affines réelles $Q \subset \mathbf{R}^4$ dont les projectivisées sont équivalentes à la quadrique projective $\widetilde{Q}_1 : X_0^2 + X_1^2 + X_2^2 + X_3^2 - X_4^2 = 0$ (resp., à $\widetilde{Q}_2 : X_0^2 + X_1^2 + X_2^2 - X_3^2 - X_4^2 = 0$) dans $\mathbf{P}^4(\mathbf{R})$.*
(ii) *La projectivisée de la quadrique affine réelle*

$$x_1^2 - 2x_1x_2 + 4x_1x_3 - 2x_1x_4 + 2x_2^2 - 6x_2x_3 + 4x_2x_4 + 5x_3^2 - 2x_3x_4 - 2x_4^2 +$$
$$+ 2x_1 - 4x_2 + 4x_3 - 8x_4 + 5 = 0,$$

est-elle équivalente à $\widetilde{Q}_1$ (resp., à $\widetilde{Q}_2$) ?

3.10 Le groupe orthogonal euclidien

(3.10.1) Rappel. Un **espace euclidien** est un espace vectoriel réel V muni d'une forme bilinéaire symétrique $f : V \times V \longrightarrow \mathbf{R}$ dont la forme quadratique associée $q(x) = f(x,x)$ est **définie positive :**

$$(\forall x \in V - \{\vec{0}\}) \qquad q(x) > 0$$

(on note, parfois, $(x \mid y) = f(x,y)$). Ceci implique, compte tenu de 3.7.2(ii), qu'il existe une **base orthonormée** $e_1, \dots, e_n$ de V ($n = \dim(V)$), i.e. une base vérifiant $f(e_i, e_j) = \delta_{ij}$ (en particulier, f est non-dégénérée). En utilisant une telle base, on identifie V à $\mathbf{R}^n$, $f(x,y)$ au produit scalaire euclidien usuel ${}^t xy = \sum_{j=1}^n x_j y_j$, $q(x)$ à $\sum_{j=1}^n x_j^2$ et le groupe orthogonal $O(q)$ (resp. le groupe spécial orthogonal $SO(q)$) au groupe

$$O(n) = O_n(\mathbf{R}) = \{U \in GL_n(\mathbf{R}) \mid {}^tUU = I\}, \qquad \text{resp.} \quad SO(n) = SO_n(\mathbf{R}) = O^+(n) = O(n) \cap SL_n(\mathbf{R}).$$

On note $\|x\| = \sqrt{q(x)} \geq 0$ la **norme** (= la **longeur**) d'un vecteur $x \in V$.

(3.10.2) (i) V n'a pas de vecteurs isotropes.
(ii) Tout sous-espace vectoriel $W \subset V$ (muni de la restriction f_W de f à $W \times W$) est un espace euclidien; comme f_W est non-dégénérée, on a $W \cap W^\perp = \{\vec{0}\}$, donc $V = W \perp W^\perp$.
(iii) Si $n = 1$, on a $O(q) = \{\pm \mathrm{id}\}$ et $SO(q) = \{\mathrm{id}\}$.
(iv) $\lambda \cdot \mathrm{id} \in O(q) \iff \lambda = \pm 1$.
(v) $\lambda \cdot \mathrm{id} \in SO(q) \iff [\lambda = \pm 1 \wedge \lambda^n = 1] \iff \lambda = 1$ (resp. $\lambda = \pm 1$) si $2 \nmid n$ (resp. si $2 \mid n$).
(vi) On note $O^-(n) = \{U \in O(n) \mid \det(U) = -1\}$.

(3.10.3) Réflexions. Pour tout hyperplan vectoriel $H \subset V$ on a $V = H \perp H^\perp$; la réflexion orthogonale $\tau_H \in O(q)$ associée à H (voir 3.4.11 ci-dessus) est caractérisée par la formule suivante :

$$(\forall u \in H)\,(\forall v \in H^\perp) \qquad \tau_H(u+v) = u - v.$$

La matrice de τ_H dans la réunion des bases respectives de H et $H^\perp$ est égale à

$$\begin{pmatrix} I_{n-1} & 0 \\ 0 & -1 \end{pmatrix}.$$

En particulier, on a

$$\det(\tau_H) = -1 \implies \tau_H \notin SO(q).$$

(3.10.4) Exercice. *Établir des isomorphismes de groupes*

$$\begin{aligned} &O(q) \xrightarrow{\sim} SO(q) \times \{\pm \mathrm{id}\}, && \text{si } 2 \nmid n \\ &O(q) \xrightarrow{\sim} SO(q) \rtimes \{\mathrm{id}, \tau\}, && \text{si } 2 \mid n, \end{aligned}$$

où $\tau = \tau_H$ est une réflexion arbitraire.

(3.10.5) Proposition. *Si $x, y \in V$ et $q(x) = q(y)$, alors il existe une réflexion $\tau = \tau_H \in O(q)$ vérifiant $\tau(x) = y$.*

Preuve. Si $x = y$, on prend $\tau = \tau_H$, où H est un hyperplan contenant x. Si $x \neq y$, soit $H = (x-y)^\perp$; on a $(x+y)/2 \in H$ et $(x-y)/2 \in H^\perp$, donc

$$\tau_H(x) = \tau_H\left(\frac{x+y}{2} + \frac{x-y}{2}\right) = \frac{x+y}{2} - \frac{x-y}{2} = y.$$

(3.10.6) Théorème. *Pour tout élément $u \in O(q)$ il existe des réflexions $\tau_1, \ldots, \tau_m \in O(q)$ ($m \leq \dim(V) = n$) telles que l'on ait $u = \tau_1 \cdots \tau_m$.*

Preuve. Récurrence : si $n = 1$, alors on a $u = \mathrm{id}$ ($m = 0$, i.e. le produit vide) ou $u = -\mathrm{id} = \tau$. Si $n > 1$, soit $x \in V - \{\vec{0}\}$. D'après 3.10.5 il existe une réflexion τ_1 vérifiant $\tau_1(x) = u(x)$. L'élément $g = \tau_1^{-1} u = \tau_1 u \in O(q)$ fixe alors la droite $\mathbf{R} \cdot x$, ce qui entraîne que l'hyperplan $V' = (\mathbf{R} \cdot x)^\perp \subset V$ est stable par g; on note $g' \in O(V')$ la restriction de g à V'. Par hypothèse de récurrence, il existe des réflexions $\tau'_i = \tau_{H'_i} \in O(V')$ ($i = 2, \ldots, m \leq n$, $H'_i \subset V'$ un hyperplan) vérifiant $g' = \tau'_2 \cdots \tau'_m$. Pour tout $i = 2, \ldots, m$, soit $\tau_i = \tau_{H_i} \in O(q)$ la réflexion par rapport à l'hyperplan $H_i = \mathbf{R} \cdot x \oplus H'_i = \mathbf{R} \cdot x \perp H'_i \subset V$. La restriction de τ_i à $\mathbf{R} \cdot x$ (resp. à H'_i) est égale à id (resp. à τ'_i), donc $\tau_2 \cdots \tau_m = g = \tau_1^{-1} u \Longrightarrow u = \tau_1 \cdots \tau_m$.

(3.10.7) (i) On a $\det(u) = \det(\tau_1 \cdots \tau_m) = (-1)^m$. En particulier, $u \in SO(n) \iff 2 \mid m$.
(ii) Si $u \in O(2)$, $u \notin SO(2)$, alors $u = \tau_1$ est une réflexion.

(3.10.8) Proposition (les groupes $O(2)$ et $SO(2)$). *On a $O(2) = O^+(2) \cup O^-(2)$, où*

$$O^+(2) = SO(2) = \left\{ \begin{pmatrix} a & -c \\ c & a \end{pmatrix} \,\middle|\, a, c \in \mathbf{R},\ a^2 + c^2 = 1 \right\}$$

$$O^-(2) = \left\{ \begin{pmatrix} a & c \\ c & -a \end{pmatrix} \;\middle|\; a, c \in \mathbf{R},\ a^2 + c^2 = 1 \right\}$$

Preuve. Soit

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{R}).$$

On a

$$\begin{aligned} U \in O(2) &\iff {}^tUU = I \\ &\iff a^2 + c^2 = b^2 + d^2 = 1, \qquad \begin{pmatrix} a \\ c \end{pmatrix} \perp \begin{pmatrix} b \\ d \end{pmatrix} \\ &\iff a^2 + c^2 = b^2 + d^2 = 1, \qquad \begin{pmatrix} b \\ d \end{pmatrix} = \lambda \begin{pmatrix} -c \\ a \end{pmatrix} \qquad (\lambda \in \mathbf{R}) \\ &\iff a^2 + c^2 = 1, \qquad \begin{pmatrix} b \\ d \end{pmatrix} = \pm \begin{pmatrix} -c \\ a \end{pmatrix} \qquad (\det(U) = \pm 1). \end{aligned}$$

(3.10.9) Exercice. (i) *On sait, grâce à 3.10.7(ii) et 3.10.8, que toute matrice*

$$\begin{pmatrix} a & c \\ c & -a \end{pmatrix} \qquad (a, c \in \mathbf{R},\ a^2 + c^2 = 1)$$

représente une réflexion. Décrire géométriquement cette réflexion.
(ii) *Décrire géométriquement la composition $\tau_H \circ \tau_{H'}$ de deux réflexions $\tau_H, \tau_{H'} \in O(2)$.*

(3.10.10) Proposition. *L'application*

$$e^{it} \mapsto R(t) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$

définit un isomorphisme de groupes $U(1) = \{z \in \mathbf{C} \mid z\overline{z} = 1\} \xrightarrow{\sim} SO(2)$. [Géométriquement, la matrice $R(t)$ représente la rotation d'angle $t \in \mathbf{R}/2\pi\mathbf{Z}$.]

Preuve. Cette application est bijective, puisque tout couple $a, c \in \mathbf{R}$ vérifiant $a^2 + c^2 = 1$ s'écrit, de manière unique, comme $a = \cos(t)$, $c = \sin(t)$ ($t \in \mathbf{R}/2\pi\mathbf{Z}$). Il s'agit d'un homomorphisme de groupes, car on a $e^{it}e^{is} = e^{i(t+s)}$ et

$$R(t)R(s) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix} \begin{pmatrix} \cos(s) & -\sin(s) \\ \sin(s) & \cos(s) \end{pmatrix} = \begin{pmatrix} \cos(t+s) & -\sin(t+s) \\ \sin(t+s) & \cos(t+s) \end{pmatrix} = R(t+s).$$

(3.10.11) Un plongement $\mathbf{C} \hookrightarrow M_2(\mathbf{R})$. Le morphisme $e^{it} \mapsto R(t)$ provient de la construction générale suivante. L'anneau $\mathbf{C}$ agit sur lui-même par multiplication : pour tout $z = u + vi \in \mathbf{C}$, l'application

$$m(z) : \mathbf{C} \longrightarrow \mathbf{C}, \qquad z' \mapsto zz'$$

est $\mathbf{C}$-linéaire, en particulier $\mathbf{R}$-linéaire : $m(z) \in \mathrm{End}_{\mathbf{R}}(\mathbf{C})$. Si on identifie

$$\mathbf{C} \xrightarrow{\sim} \mathbf{R}^2, \qquad a + bi \mapsto \begin{pmatrix} a \\ b \end{pmatrix},$$

l'application $m(z)$ est représentée par la matrice

$$M(z) = M(u+vi) = \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \in M_2(\mathbf{R}),$$

puisqu'on calcule

$$m(u+vi) : a+bi \mapsto (u+vi)(a+bi) = (ua-vb)+(va+ub)i$$
$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} ua-vb \\ va+ub \end{pmatrix} = \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

On a

$$m(z_1+z_2) = m(z_1)+m(z_2), \quad m(z_1z_2) = m(z_1)\circ m(z_2), \quad (\forall \lambda \in \mathbf{R})\ m(\lambda) = \lambda \cdot \mathrm{id}, \quad z \neq 0 \Longrightarrow m(z) \neq 0,$$

donc l'application $M : \mathbf{C} \longrightarrow M_2(\mathbf{R})$ est un homomorphisme injectif d'anneaux (plus précisement, de $\mathbf{R}$-algèbres).

(3.10.12) L'écriture complexe de $O(2)$. Si on identifie $\mathbf{R}^2$ à $\mathbf{C}$ comme en 3.10.11, alors les éléments de $O(2)$ s'écrivent

$$O^+(2) = SO(2) = \{z \mapsto e^{it}z \mid t \in \mathbf{R}/2\pi\mathbf{Z}\}$$
$$O^-(2) = O(2) - SO(2) = \{z \mapsto e^{it}\overline{z} \mid t \in \mathbf{R}/2\pi\mathbf{Z}\}.$$

(3.10.13) Propriétés de $M : \mathbf{C} \hookrightarrow M_2(\mathbf{R})$. (i) L'image de $m : \mathbf{C} \hookrightarrow \mathrm{End}_{\mathbf{R}}(\mathbf{C})$ consiste en les applications qui sont $\mathbf{C}$-linéaires (i.e. telles qui commutent avec $m(i)$), donc

$$\mathrm{Im}\,(M : \mathbf{C} \hookrightarrow M_2(\mathbf{R})) = \{g \in M_2(\mathbf{R}) \mid Jg = gJ\}, \qquad J = M(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

(ii) On a $M(e^{it}) = R(t)$, donc M induit un isomorphisme de groupes

$$U(1) \xrightarrow{\sim} SO(2) = O(2) \cap SL_2(\mathbf{R}).$$

(iii) Les valeurs propres de la matrice $M(u+vi)$ sont égales à $u \pm vi$. Plus précisement, on a

$$\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix}^{-1} \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} = \begin{pmatrix} u+iv & 0 \\ 0 & u-iv \end{pmatrix}.$$

En particulier, les valeurs propres de $R(t)$ sont égales à $e^{\pm it} = \cos(t) \pm i\sin(t)$.

(3.10.14) Exercice. (i) *L'application*

$$M : M_n(\mathbf{C}) \longrightarrow M_{2n}(\mathbf{R}), \qquad A+iB \mapsto \begin{pmatrix} A & -B \\ B & A \end{pmatrix}$$

est un homomorphisme injectif d'anneaux, dont l'image est égale à

$$\{g \in M_{2n}(\mathbf{R}) \mid J_n g = gJ_n\}, \qquad J_n = M(i \cdot I_n) = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}.$$

(ii) *M induit un isomorphisme de groupes $U(n) \xrightarrow{\sim} O(2n) \cap Sp(2n, \mathbf{R})$. [Indication : voir 3.11.9 ci-dessous.]*
(iii) *Expliquer le lien avec 3.2.11.*

(3.10.15) Proposition. (i) *Si $U \in SO(2)$ et $P \in O(2)$, alors on a $P^{-1}UP = U^{\pm 1}$, où $\det(P) = \pm 1$.*
(ii) *Si V est un espace euclidien de dimension $\dim(V) = 2$ et $u \in SO(q)$ une isométrie positive de V, alors la matrice de u dans une base orthonormée arbitraire de V est égale à $R(\theta)$ ou $R(-\theta)$, où $e^{\pm i\theta}$ sont les valeurs propres de u.*

Preuve. (i) Si $\det(P) = 1$, alors $P \in SO(2)$, donc $P^{-1}UP = U$, puisque le groupe $SO(2) \xrightarrow{\sim} U(1)$ est commutatif. Si $\det(P) = -1$, alors on a $P = R\tau$, où $R \in SO(2)$ et

$$\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

d'où (en écrivant $U = R(\theta)$)

$$P^{-1}UP = \tau^{-1}R^{-1}UR\tau = \tau^{-1}U\tau = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} R(\theta) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = R(-\theta) = R(\theta)^{-1}.$$

(ii) Dans une base orthonormée fixée de V, l'isométrie u est representée par $U = R(\theta) \in SO(2)$. Un changement de base orthonormée est défini par une matrice $P \in O(2)$, qui transforme U en $P^{-1}UP = U^{\pm 1} = R(\pm\theta)$, d'après (i). Les valeurs propres de U sont égales à $e^{\pm i\theta}$ (voir 3.10.13(iii)).

(3.10.16) Rappel-Exercice. *Si $\lambda \in \mathbf{C}$ est une valeur propre d'une matrice unitaire $U \in U(n)$, alors $|\lambda| = 1$ (i.e. $\lambda \in U(1)$).*

(3.10.17) Théorème. *Soit V un espace euclidien. Pour toute isométrie $u \in O(q)$ de V, il existe une base orthonormée de V dans laquelle u s'écrit*

$$\begin{pmatrix} I_a & 0 & 0 & \cdots & 0 \\ 0 & -I_b & 0 & \cdots & 0 \\ 0 & 0 & R(\theta_1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & R(\theta_r), \end{pmatrix} \tag{3.10.17.1}$$

où $\theta_1, \ldots, \theta_r \notin \pi\mathbf{Z}$ ($\iff$ il existe une décomposition orthogonale $V = V^+ \perp V^- \perp W_1 \perp \cdots \perp W_r$, où les sous-espaces V^+, V^-, W_j sont stables par u, la restriction de u à $V^\pm$ est égale à $\pm\mathrm{id}$, $\dim(W_j) = 2$ et u agit sur W_j par une rotation plane $\neq \pm\mathrm{id}$).

(3.10.18) (i) **Reformulation matricielle** : pour tout $U \in O(n)$ il existe $P \in O(n)$ tel que la matrice $P^{-1}UP$ soit de la forme (3.10.17.1).
(ii) Les **valeurs propres** de u sont égales à $+1$ (a-fois), -1 (b-fois) et $\cos(\theta_j) \pm i\sin(\theta_j)$ ($j = 1, \ldots, r$).
(iii) $b = \dim(V^-)$ est paire $\iff$ $u \in SO(n)$.
(iv) $a + b = \dim(V^+ \oplus V^-) \equiv n = \dim(V) \pmod 2$.
(v) On a $\dim(\mathrm{Ker}(u-1)) = a$, $\dim(\mathrm{Im}(u-1)) = \dim(V) - a = b + 2r$, d'où

$$\det(u) = (-1)^b = (-1)^{\dim(\mathrm{Im}(u-1))}, \qquad \det(-u) = (-1)^{b+\dim(V)} = (-1)^a = (-1)^{\dim(\mathrm{Ker}(u-1))}.$$

Preuve de 3.10.17. Récurrence : le cas $n = \dim(V) = 1$ est trivial. Le cas $n = 2$: si $u \in SO(2)$, voir 3.10.15(ii). Si $u \notin SO(2)$, alors $u = \tau_H$ est une réflexion, dont la matrice dans la réunion des bases orthonormées des droites H et $H^\perp$ est égale à

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

Soit $n \geq 3$. On choisit une base orthonormée de V, ce qui nous permet d'identifier V à $\mathbf{R}^n$ et $O(q)$ à $O(n)$. On note $\lambda_1, \ldots, \lambda_n \in U(1)$ les valeurs propres de u.

(a) $(\exists j = 1, \ldots, n) \quad \lambda = \lambda_j = \pm 1$: soit $v \in \mathbf{R}^n$ un vecteur propre orthonormé : $u(v) = \pm v$, $\|v\| = 1$. La décomposition orhogonale $V = \mathbf{R}v \perp (\mathbf{R}v)^\perp$ est stable par u et u agit sur $\mathbf{R}v$ comme $\pm\mathrm{id}$. L'hypothèse de récurrence alors s'applique à la restriction de u à $(\mathbf{R}v)^\perp$, ce qui montre le résultat dans ce cas.

(b) Toutes les valeurs propres λ_j sont imaginaires; on fixe $\lambda = \lambda_j = e^{i\theta}$, $\theta \notin \pi\mathbf{Z}$. Soit $v \in \mathbf{C}^n$ un vecteur propre : $u(v) = e^{i\theta}v$; on a $u(\overline{v}) = e^{-i\theta}\overline{v}$. Les vecteurs $x = (v + \overline{v})/2 \in \mathbf{R}^n$ et $y = i(v - \overline{v})/2 \in \mathbf{R}^n$ engendrent un plan $W = \mathbf{R}x + \mathbf{R}y \subset V$ qui est stable par u. On a $\mathbf{C}W = \mathbf{C}x + \mathbf{C}y = \mathbf{C}v + \mathbf{C}\overline{v}$, donc les valeurs propres de la restriction de u à W sont égales à $e^{i\theta}, e^{-i\theta}$; il en résulte que $u|_W \in SO(q|_W)$ est une isométrie directe de W. D'après 3.10.15(ii), la matrice de $u|_W$ dans une base othonormée arbitraire de W est égale à $R(\theta)$ ou $R(-\theta)$. On écrit $V = W \perp W^\perp$ et on applique l'hypothèse de récurrence à $W^\perp$.(1)

(3.10.19) Exemple : $\dim(V) = 3$. (i) Si $u \in SO(3)$, alors la matrice de u s'écrit, dans une base orthonormée convenable,

$$\begin{pmatrix} 1 & 0 \\ 0 & R(\theta) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix}$$

Si $\theta \in 2\pi\mathbf{Z}$ (resp. $\theta \in \pi + 2\pi\mathbf{Z}$), alors $u = \mathrm{id}$ (resp. $u = -\mathrm{id}$). Si $\theta \notin \pi\mathbf{Z}$, alors u est une rotation d'axe $\mathrm{Ker}(u - \mathrm{id})$ et d'angle θ.

(ii) Si $u \notin SO(3)$, alors la matrice de u s'écrit, dans une base orthonormée convenable,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} -1 & 0 & 0 \\ 0 & \cos(\theta) & -\sin(\theta) \\ 0 & \sin(\theta) & \cos(\theta) \end{pmatrix} \qquad (\theta \notin 2\pi\mathbf{Z})$$

(la réflexion par rapport au plan $\mathrm{Ker}(u - \mathrm{id})$, resp. le produit de cette réflexion et d'une rotation d'axe $\mathrm{Ker}(u - \mathrm{id})^\perp$ et d'angle θ).

(3.10.20) Proposition. *Le groupe $SO(n)$ est connexe par arcs, i.e. pour tous $g_0, g_1 \in SO(n)$ il existe une application continue $\gamma : [0,1] \longrightarrow SO(n)$ vérifiant $\gamma(0) = g_0$ et $\gamma(1) = g_1$.*

Preuve. La multiplication matricielle $GL_n(\mathbf{R}) \times GL_n(\mathbf{R}) \longrightarrow GL_n(\mathbf{R})$ est continue; il suffit donc de trouver une application continue $\alpha : [0,1] \longrightarrow SO(n)$ telle que l'on ait $\alpha(0) = I$ et $\alpha(1) = g_0^{-1}g_1 = U$; on pose alors $\gamma(t) = g_0\alpha(t)$. D'après 3.10.17-18, il existe $P \in O(n)$ vérifiant

$$P^{-1}UP = \begin{pmatrix} I_a & 0 & 0 & \cdots & 0 \\ 0 & -I_b & 0 & \cdots & 0 \\ 0 & 0 & R(\theta_1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & R(\theta_r) \end{pmatrix}, \qquad -I_b = \underbrace{\begin{pmatrix} R(\pi) & 0 & \cdots & 0 \\ 0 & R(\pi) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R(\pi) \end{pmatrix}}_{b/2-\text{fois}}$$

(l'entier b est pair, puisque $U \in SO(n)$). On définit

(1) On peut vérifier directement que l'on a $u(x) = (\cos(\theta))x + (\sin(\theta))y$ et $u(y) = (-\sin(\theta))x + (\cos(\theta))y$, donc la matrice de u dans la base x, y de W est égale à $R(\theta)$. La formule $f(v,v) = f(u(v), u(v)) = e^{2i\theta}f(v,v)$ entraîne $v \perp v$ et on obtient de même $\overline{v} \perp \overline{v}$, ce qui montre que l'on a $x \perp y$ et $c := \|x\| = \|y\|$, donc x/c et y/c forment une base othonormée de W.

$$\alpha(t) = P \begin{pmatrix} I_a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & R(t\pi) & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & R(t\pi) & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & R(t\theta_1) & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & R(t\theta_r) \end{pmatrix} P^{-1}.$$

(3.10.21) Exercice. *Déterminer le groupe $O(1,1) \subset GL_2(\mathbf{R})$. Montrer que le sous-groupe $SO(1,1)$ n'est pas connexe par arcs (il a deux composantes connexes - lesquelles?).*

(3.10.22) Proposition. *Les groupes $O(n), SO(n)$ sont compacts (en tant que sous-ensembles de l'espace $M_n(\mathbf{R}) \xrightarrow{\sim} \mathbf{R}^{n^2}$).*

Preuve. L'équation ${}^tUU - I_n = 0$ exprime $O(n) \subset \mathbf{R}^{n^2}$ comme l'ensemble des zéros d'un ensemble (fini) de fonctions continues $\mathbf{R}^{n^2} \longrightarrow \mathbf{R}$. Il en résulte que $O(n)$ est fermé dans $\mathbf{R}^{n^2}$. Toute colonne de $U \in O(n)$ est un vecteur de longeur 1, donc $|U_{ij}| \leq 1$ pour tous $i, j = 1, \ldots, n$. On vient de démontrer que $O(n) \subset \mathbf{R}^{n^2}$ est à la fois fermé et borné, donc compact (et de même pour $SO(n)$).

(3.10.23) Exercice. *Les groupes $O(1,1), SO(1,1)$ sont-ils fermés dans $M_2(\mathbf{R}) \xrightarrow{\sim} \mathbf{R}^4$? Sont-ils bornés?*

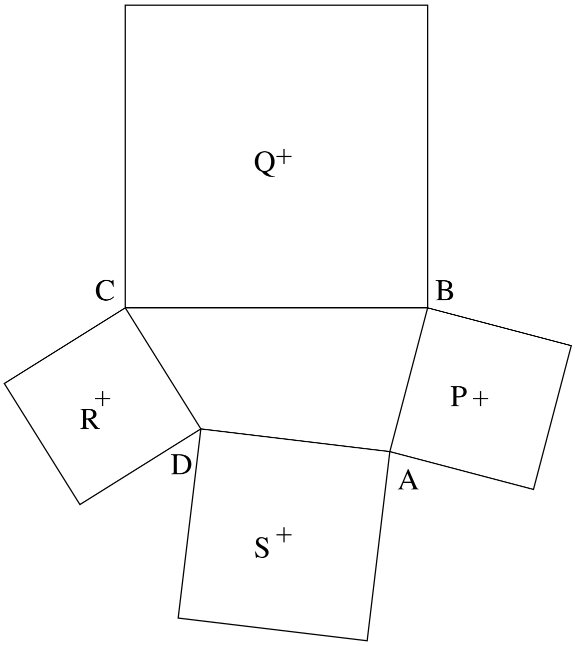
(3.10.24) Proposition. *Pour toute isométrie $u \in O(q)$ d'un espace euclidien V, on a $\mathrm{Ker}(u-1) \perp \mathrm{Im}(u-1) = V$.*

Preuve. Si $x \in \mathrm{Ker}(u-1)$ et $y \in \mathrm{Im}(u-1)$, alors on a $(1-u)x = 0$, $y = (u-1)z$ $(z \in V)$ et

$$(x \mid y) = (x \mid (u-1)z) = (x \mid uz) - (x \mid z) = (u^{-1}x \mid z) - (x \mid z) = (u^{-1}(1-u)x \mid z) = 0,$$

ce qui entraîne que $\mathrm{Ker}(u-1) \perp \mathrm{Im}(u-1)$. En particulier, $\mathrm{Ker}(u-1) \cap \mathrm{Im}(u-1) = 0$ (comme il n'y a pas de vecteurs isotropes). D'après le théorème du rang, on a $\dim(\mathrm{Ker}(u-1)) + \dim(\mathrm{Im}(u-1)) = \dim(V)$, d'où $\mathrm{Ker}(u-1) \oplus \mathrm{Im}(u-1) = V$.

(3.10.25) Exercice. *Soit $ABCD$ un quadrilatère convexe et P, Q, R et S les centres de quatres carrés extérieurs à $ABCD$, construits sur les cotés de $ABCD$. Montrer que les vecteurs $\overrightarrow{PR}$ et $\overrightarrow{QS}$ sont orthogonaux et de même longeur. [On pourra utiliser les coordonnées usuelles $\begin{pmatrix} x \\ y \end{pmatrix}$ dans $\mathbf{R}^2$, ou, encore mieux, la coordonnée complexe $z = x + iy$.]*



3.11 Groupe unitaire

(3.11.1) On considère l'espace $\mathbf{C}^n$ muni du produit hermitien euclidien ${}^t x\overline{y} = \sum_{j=1} x_j \overline{y}_j$. On note

$$\mathrm{Herm}_n(\mathbf{C}) = \{A \in M_n(\mathbf{C}) \mid {}^tA = \overline{A}\}$$

l'ensemble de matrices hermitiennes de degré n.

(3.11.2) Définition. *Une matrice $A \in \mathrm{Herm}_n(\mathbf{C})$ est dite* **définie positive** *(notation : $A >> 0$) si le produit hermitien ${}^t xA\overline{y}$ l'est, c'est-à-dire que l'on a*

$$(\forall x \in \mathbf{C}^n - \{0\}) \qquad {}^t xA\overline{x} > 0.$$

On note $\mathrm{Herm}_n^{++}(\mathbf{C}) = \{A \in \mathrm{Herm}_n(\mathbf{C}) \mid A >> 0\}$.

(3.11.3) Rappel-Exercice. *Soit $A \in \mathrm{Herm}_n(\mathbf{C})$.*
(i) *Toutes les valeurs propres de A sont réelles.*
(ii) *Deux vecteurs propres de A dont les valeurs propres sont distinctes sont orthogonaux (par rapport au produit hermitien ${}^t x\overline{y}$).*
(iii) *Il existe une matrice unitaire $U \in U(n)$ telle que la matrice $D = {}^t\overline{U}AU = U^{-1}AU$ soit diagonnalle.*
[Les colonnes de U sont des vecteurs propres de A; les éléments diagonaux de D sont les valeurs propres de A.]
(iv) *A est définie positive $\iff$ toutes ses valeurs propres sont strictement positive.*
(v) *Si A est définie positive, alors il existe une matrice unique $B \in \mathrm{Herm}_n^{++}(\mathbf{C})$ telle que $B^2 = A$.*

(3.11.4) Exercice. *Pour tout $U \in U(n)$ il existe $P \in U(n)$ tel que l'on ait*

$$P^{-1}UP = \begin{pmatrix} e^{i\theta_1} & 0 & \cdots & 0 \\ 0 & e^{i\theta_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & e^{i\theta_n} \end{pmatrix} \qquad\qquad (\theta_j \in \mathbf{R}/2\pi\mathbf{Z}).$$

(3.11.5) Exercice. *Les groupes $U(n)$ et $SU(n)$ sont connexes par arcs.*

(3.11.6) Exercice. *Les groupes $U(n)$ et $SU(n)$ sont compacts.*

(3.11.7) Proposition (Décomposition polaire). *Soit $M \in GL_n(\mathbf{C})$. Il existe un couple unique $(P, U) \in \mathrm{Herm}_n^{++}(\mathbf{C}) \times U(n)$ tel que $M = PU$.*

Nombres	Matrices
$z \in \mathbf{C}$	$A \in M_n(\mathbf{C})$
$\overline{z} \in \mathbf{C}$	${}^t\overline{A}$
$\overline{z} = z \in \mathbf{R}$	${}^t\overline{A} = A \in \mathrm{Herm}_n(\mathbf{C})$
$\overline{u}u = 1 \iff \lvert u\rvert = 1$	${}^t\overline{U}U = I \iff U \in U(n)$
$\lvert u\rvert = 1 \iff u = e^{it}$, $t \in \mathbf{R}$	$U \in U(n) \iff U = e^{iA}$, $A \in \mathrm{Herm}_n(\mathbf{C})$
$z \in \mathbf{C}^* \iff z = ru$, $r \in \mathbf{R}_{>0}$, $\lvert u\rvert = 1$	$M \in GL_n(\mathbf{C}) \iff M = PU$, $P \in \mathrm{Herm}_n^{++}(\mathbf{C})$, $U \in U(n)$

Preuve de 3.11.7. La matrice $A := M{}^t\overline{M}$ appartient à $\mathrm{Herm}_n^{++}(\mathbf{C})$, puisque ${}^t\overline{A} = A$ et ${}^tx A\overline{x} = {}^t({}^tMx)\overline{{}^tMx} > 0$ (pour tout $x \in \mathbf{C}^n - \{0\}$). D'après 3.11.3(v), il existe une matrice unique $P \in \mathrm{Herm}_n^{++}(\mathbf{C})$ telle que $A = M{}^t\overline{M} = P^2 = P{}^t\overline{P}$, ce qui entraîne que la matrice $U = P^{-1}M$ est unitaire ($U{}^t\overline{U} = P^{-1}M{}^t\overline{M}P^{-1} = I$), donc $M = PU$. Réciproquement, la décomposition $M = PU$ est unique, car $M{}^t\overline{M} = PU{}^t\overline{U}{}^t\overline{P} = P^2$.

(3.11.8) Exercice. *Si $M \in GL_n(\mathbf{R})$, alors la matrice P est réelle symétrique (définie positive) et $U \in O(n)$.*

(3.11.9) Exercice. *Soit V un espace vectoriel complexe; soit $h : V \times V \longrightarrow \mathbf{C}$ une forme hermitienne. On note $V_{\mathbf{R}}$ l'espace V en tant que l'espace vectoriel réel (c'est à dire que l'on oublie la multiplication par des nombres complexes qui ne sont pas réels).*
(i) *Montrer que la partie réelle de h*

$$g = \mathrm{Re} \circ h : V_{\mathbf{R}} \times V_{\mathbf{R}} \longrightarrow \mathbf{R}, \qquad g(z, w) = \mathrm{Re}(h(z, w))$$

est une forme bilinéaire symétrique, et que la partie imaginaire de h

$$\Omega = \mathrm{Im} \circ h : V_{\mathbf{R}} \times V_{\mathbf{R}} \longrightarrow \mathbf{R}, \qquad \Omega(z, w) = \mathrm{Im}(h(z, w))$$

est une forme bilinéaire antisymétrique.
(ii) *On note $J : V_{\mathbf{R}} \longrightarrow V_{\mathbf{R}}$ l'application $z \mapsto iz$. Montrer que l'on a*

$$g(J(z), J(w)) = g(z, w), \qquad \Omega(J(z), J(w)) = \Omega(z, w),$$
$$g(z, J(w)) = \Omega(z, w), \qquad \Omega(J(z), w) = g(z, w).$$

(iii) *Montrer : h est non-dégénérée $\iff$ g est non-dégénérée $\iff$ Ω est non-dégénérée.*
(iv) *Montrer que, si h est non-dégénérée, alors on a $U(h) = O(g) \cap Sp(\Omega)$.*
(v) *Si $h(z, w) = \sum_{k=1}^n z_k\overline{w}_k$ est le produit hermitien usuel sur $V = \mathbf{C}^n$, exprimer $g(z, w)$ et $\Omega(z, w)$ en termes de $x, y, u, v \in \mathbf{R}^n$, où $z = x + iy$ et $w = u + iv$.*

3.12 Quaternions et $SO(3)$

(3.12.1) Quaternions (rappel). L'anneau des quaternions est égal à

$$\mathbf{H} = \mathbf{R} \oplus \mathbf{R}i \oplus \mathbf{R}j \oplus \mathbf{R}k,$$

où

$$i^2 = j^2 = -1, \qquad ij = -ji = k \quad\Longrightarrow\quad k^2 = -1, \qquad jk = -kj = i, \qquad ki = -ik = j$$

et

$$(\forall x \in \mathbf{H})\,(\forall r \in \mathbf{R}) \qquad xr = rx.$$

Conjugué : Le conjugué d'un quaternion $x = a + bi + cj + dk$ est $\overline{x} = a - bi - cj - dk$; on a $\overline{xy} = \overline{y}\,\overline{x}$.
Trace : $\mathrm{Tr}(x) = x + \overline{x} = 2a$.
Norme : $N(x) = x\overline{x} = \overline{x}x = a^2 + b^2 + c^2 + d^2 \in \mathbf{R}_{\geq 0}$. On pose $\|x\| = \sqrt{N(x)}$. On a

$$N(xy) = \overline{xy}\,xy = \overline{y}\,\overline{x}x\,y = \overline{y}N(x)y = N(x)\,\overline{y}y = N(x)\,N(y).$$

H est un corps (non-commutatif) : Si $x \in \mathbf{H} - \{0\}$, alors $N(x) \in \mathbf{R}_{>0}$, donc $y := (N(x))^{-1}\overline{x}$ est l'inverse de x : $xy = yx = (N(x))^{-1}\overline{x}x = 1$. Le groupe des éléments inversibles $\mathbf{H}^*$ est donc égal à $\mathbf{H} - \{0\}$.
Quaternions purs : $\mathbf{H}_0 = \mathbf{H}^{\mathrm{Tr}=0} = \{bi + cj + dk\}$; on a $\mathbf{H} = \mathbf{R} \oplus \mathbf{H}_0$.
$\mathbf{H}_0$ est un espace euclidien : On identifie

$$\mathbf{H}_0 \xrightarrow{\sim} \mathbf{R}^3, \qquad x = bi + cj + dk \mapsto \begin{pmatrix} b \\ c \\ d \end{pmatrix}.$$

La restriction de la norme à $\mathbf{H}_0$ est égale à

$$\|x\|^2 = N(x) = N(bi + cj + dk) = b^2 + c^2 + d^2 = x\overline{x} = -x^2,$$

ce qui est la forme quadratique associée au produit scalaire euclidien (x, y) sur $\mathbf{R}^3$. Le produit scalaire s'écrit

$$(x, y) = \frac{1}{2}\left(\|x + y\|^2 - \|x\|^2 - \|y\|^2\right) = -\frac{1}{2}(xy + yx) = \frac{1}{2}(x\overline{y} + y\overline{x}) = \frac{1}{2}\mathrm{Tr}(x\overline{y}) \qquad (x, y \in \mathbf{H}_0)$$

Orthogonalité : Il résulte de la formule précedente que l'on a

$$(\forall x, y \in \mathbf{H}_0) \qquad [x \perp y \iff xy = -yx]\,.$$

Produit : Si $a, a' \in \mathbf{R}$ et $x, x' \in \mathbf{H}_0$, alors on a

$$(a + x)(a' + x') = (aa' - (x, x')) + (ax' + a'x + x \wedge x'),$$

où l'on a noté $x \wedge x'$ le produit vectoriel dans $\mathbf{H}_0 \xrightarrow{\sim} \mathbf{R}^3$.

(3.12.2) Exercice. (i) *Le* **centre** $Z(\mathbf{H}) = \{x \in \mathbf{H} \mid (\forall y \in \mathbf{H})\ \ xy = yx\}$ *de l'anneau* **H** *est égal à* **R**.
(ii) *Pour tout $x \in \mathbf{H}$, on a : $x^2 \in \mathbf{R} \iff x \in \mathbf{R}$ ou $x \in \mathbf{H}_0$.*

(3.12.3) Proposition (Plongements $\mathbf{C} \hookrightarrow \mathbf{H}$). *L'application $\rho \mapsto I := \rho(i)$ induit une bijection*

$$\left\{ \begin{matrix} \text{homomorphismes d'anneaux} \\ \rho : \mathbf{C} \longrightarrow \mathbf{H}, \qquad \rho|_{\mathbf{R}} = \mathrm{id} \end{matrix} \right\} \xrightarrow{\sim} S(\mathbf{H}_0) = \{x \in \mathbf{H}_0 \mid \|x\| = 1\} \xrightarrow{\sim} S^2.$$

Un homomorphisme d'anneaux $\rho : \mathbf{C} \longrightarrow \mathbf{H}$ vérifiant $\rho|_{\mathbf{R}} = \mathrm{id}$ est forcément injectif et on a $(\forall z \in \mathbf{C})$ $\overline{\rho(z)} = \rho(\overline{z})$.

Preuve. Si $I \in S(\mathbf{H}_0)$, alors on a $I^2 = -N(I) = -1$, donc l'application $\rho(u + iv) = u + Iv$ est un homomorphisme d'anneaux $\rho : \mathbf{C} \longrightarrow \mathbf{H}$ et $\rho|_{\mathbf{R}} = \mathrm{id}$. Réciproquement, étant donné ρ, l'élément $I := \rho(i) \in \mathbf{H}$ satisfait à $I^2 = \rho(i)^2 = \rho(i^2) = \rho(-1) = -1$. D'après 3.12.2(ii), I est contenu dans $\mathbf{R}$ ou dans $\mathbf{H}_0$; comme

$x^2 > 0$ pour tout $x \in \mathbf{R}$, on a $I \in \mathbf{H}_0$ et $\|I\|^2 = N(I) = -I^2 = 1$, donc $I \in S(\mathbf{H}_0)$. Si $z = u + iv \in \mathbf{C}$, alors on a $\overline{\rho(z)} = \overline{u + Iv} = u - Iv = \rho(\overline{z})$.

(3.12.4) Coordonnées polaires. Tout quaternion non nul $x \in \mathbf{H} - \{0\}$ s'écrit

$$x = \|x\| (\cos(\theta) + I \sin(\theta)) = \|x\| e^{\theta I} \qquad\qquad (I \in S(\mathbf{H}_0)),$$

pour un unique couple $(I, \theta) \in (S(\mathbf{H}_0) \times \mathbf{R}/2\pi\mathbf{Z})/\{\pm 1\}$ (pour tout $y \in \mathbf{H}$, on définit

$$e^y := \sum_{n=0}^{\infty} \tfrac{1}{n!}\, y^n \in \mathbf{H};$$

la série est absolument convergente).

(3.12.5) Le groupe $U_1(\mathbf{H})$. On note

$$U_1(\mathbf{H}) = \{x \in \mathbf{H}^* \mid N(x) = 1\} \subset \mathbf{H}^*$$

le groupe multiplicatif des **quaternions unitaires**.

(3.12.6) Représentation adjointe. Pour tout $x \in \mathbf{H}^*$, l'application

$$\mathrm{Ad}(x) : \mathbf{H} \longrightarrow \mathbf{H}, \qquad y \mapsto xyx^{-1}$$

est une bijection $\mathbf{R}$-linéaire. Comme $x(x'y(x')^{-1})x^{-1} = (xx')y(xx')^{-1}$, l'application

$$\mathrm{Ad} : \mathbf{H}^* \longrightarrow GL_{\mathbf{R}}(\mathbf{H}), \qquad x \mapsto \mathrm{Ad}(x)$$

est un homomorphisme de groupes, que l'on appelle la **représentation adjointe de** H^*.

Propriétés de Ad **:** (0) $\mathrm{Ad}(x)|_{\mathbf{R}} = \mathrm{id}$.

(1) $\mathrm{Ad}(x) = \mathrm{id} \iff x \in H^* \cap Z(\mathbf{H}) = \mathbf{R}^*$.

(2) $(\forall x \in \mathbf{H}^*)$ $\mathrm{Ad}(x\overline{x}) = \mathrm{id}$, donc $\mathrm{Ad}(\overline{x}) = \mathrm{Ad}(x)^{-1} = \mathrm{Ad}(x^{-1})$.

(3) $(\forall x \in \mathbf{H}^*)\,(\forall y \in \mathbf{H})$ $\overline{\mathrm{Ad}(x)y} = \overline{xyx^{-1}} = \overline{x}^{-1}\,\overline{y}\,\overline{x} = \mathrm{Ad}(\overline{x}^{-1})\overline{y} \overset{(2)}{=} \mathrm{Ad}(x)\overline{y}$.

(4) Si $y \in \mathbf{H}_0$ et $x \in \mathbf{H}^*$, alors $\overline{y} = -y$, donc $\overline{\mathrm{Ad}(x)y} \overset{(3)}{=} \mathrm{Ad}(x)\overline{y} = -\mathrm{Ad}(x)y$, d'où $\mathrm{Ad}(x)y \in \mathbf{H}_0$. Ceci signifie que $\mathrm{Ad}(x)(\mathbf{H}_0) = \mathbf{H}_0$.

(5) $(\forall x \in \mathbf{H}^*)\,(\forall y \in \mathbf{H})$ $N(\mathrm{Ad}(x)y) = N(x)N(y)N(x^{-1}) = N(y)$, donc la restriction de $\mathrm{Ad}(x)$ à $\mathbf{H}_0$ est un élément de $O(\mathbf{H}_0, N) = O(3)$.

(6) L'application

$$\mathrm{Ad}|_{\mathbf{H}_0} : \mathbf{H}^* \longrightarrow O(\mathbf{H}_0, N) = O(3)$$

est un homomorphisme de groupes, dont le noyau est égal à

$$\mathrm{Ker}(\mathrm{Ad}|_{\mathbf{H}_0}) = \mathbf{R}^*$$

(grâce à (0) et (1)).

(3.12.7) Proposition. $\mathrm{Ad}|_{\mathbf{H}_0}$ *induit des isomorphismes de groupes*

$$\mathrm{Ad}|_{\mathbf{H}_0} : U_1(\mathbf{H})/\{\pm 1\} = \mathbf{H}^*/\mathbf{R}^* \xrightarrow{\sim} SO(\mathbf{H}_0, N) = SO(3).$$

Preuve. On a $\mathbf{H}^* = \mathbf{R}^* \cdot U_1(\mathbf{H})$ et $\mathbf{R}^* \cap U_1(\mathbf{H}) = \{\pm 1\}$, d'où $U_1(\mathbf{H})/\{\pm 1\} = \mathbf{H}^*/\mathbf{R}^*$. Grâce à 3.12.6(6), il suffit de démontrer que l'image de $\mathrm{Ad}|_{\mathbf{H}_0}$ est égale à $SO(3)$. On décrit d'abord l'action de $\mathrm{Ad}(x)$ sur $\mathbf{H}_0$ géométriquement : tout $x \in U_1(\mathbf{H})$ s'écrit $x = e^{\theta I} = \cos(\theta) + I\sin(\theta)$, où $(I, \theta) \in (S(\mathbf{H}_0) \times \mathbf{R}/2\pi\mathbf{Z})/\{\pm 1\}$. On choisit un vecteur $J \in S(\mathbf{H}_0)$ orthogonal à I et on pose $K = IJ$. On a $IJ = -JI$, puisque $I \perp J$, et $I^2 = -N(I) = -1$, $J^2 = -N(J) = -1$. Il en résulte que les quaternions $I, J, K \in S(\mathbf{H}_0)$ satisfont aux même propriétés algébriques que i, j, k. On va calculer l'action de $\mathrm{Ad}(x)$ dans la base I, J, K de $\mathbf{H}_0$:

$$\begin{gathered} xI = Ix \implies \mathrm{Ad}(x)I = I \\ xJ = J\cos(\theta) + K\sin(\theta) = J(\cos(\theta) - I\sin(\theta)) = Je^{-\theta I} = Jx^{-1} \\ xK = xIJ = IxJ = IJe^{-\theta I} = Ke^{-\theta I} = Kx^{-1}, \end{gathered}$$

ce qui entraîne

$$\begin{gathered} \mathrm{Ad}(x)J = Je^{-2\theta I} = e^{2\theta I}J = (\cos(2\theta))J + (\sin(2\theta))K \\ \mathrm{Ad}(x)K = Ke^{-2\theta I} = e^{2\theta I}K = (-\sin(2\theta))J + (\cos(2\theta))K, \end{gathered}$$

donc $\mathrm{Ad}(x)$ agit trivialement sur la droite $\mathbf{R}I$ et par la matrice

$$R(2\theta) = \begin{pmatrix} \cos(2\theta) & -\sin(2\theta) \\ \sin(2\theta) & \cos(2\theta) \end{pmatrix}$$

sur le plan $\mathbf{R}J \oplus \mathbf{R}K = (\mathbf{R}I)^\perp$ (les quaternions J et K forment une base orthonormée de $(\mathbf{R}I)^\perp$). Il en résulte que $\mathrm{Ad}|_{\mathbf{H}_0}(x)$ est une rotation d'axe $\mathbf{R}I$ et d'angle 2θ. D'après 3.10.19, tout élément de $SO(3)$ est une rotation, donc l'image de $\mathrm{Ad}|_{\mathbf{H}_0}$ est égale à $SO(3)$.

(3.12.8) Exercice. *Décrire géométriquement les rotations qui correspondent à* $\mathrm{Ad}(q_1)$, $\mathrm{Ad}(q_2)$ *et* $\mathrm{Ad}(q_1q_2)$, *pour*

$$\begin{aligned} q_1 &= 1+i, & q_2 &= 1+j \\ q_1 &= \frac{1+i+j-k}{2}, & q_2 &= \frac{1+i+j+k}{2} \\ q_1 &= \frac{1+i-j-k}{2}, & q_2 &= \frac{1+i+j+k}{2}. \end{aligned}$$

(3.12.9) Proposition (les groupes $U(2)$ et $SU(2)$). *On a*

$$SU(2) = \left\{ \begin{pmatrix} a & -\overline{c} \\ c & \overline{a} \end{pmatrix} \;\middle|\; a, c \in \mathbf{C},\ |a|^2 + |c|^2 = 1 \right\}$$

$$U(2) = \left\{ \begin{pmatrix} a & -\lambda\overline{c} \\ c & \lambda\overline{a} \end{pmatrix} \;\middle|\; a, c, \lambda \in \mathbf{C},\ |a|^2 + |c|^2 = 1 = |\lambda| \right\}$$

Preuve. On considère le produit hermitien euclidien sur $\mathbf{C}^2$: $f(x,y) = {}^t x\overline{y} = x_1\overline{y_1} + x_2\overline{y_2}$. Si

$$U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{C}),$$

alors on a :

$$\begin{aligned} U \in U(2) &\iff {}^tU\overline{U} = I \\ &\iff |a|^2 + |c|^2 = |b|^2 + |d|^2 = 1, \quad \begin{pmatrix} a \\ c \end{pmatrix} \perp \begin{pmatrix} b \\ d \end{pmatrix} \\ &\iff |a|^2 + |c|^2 = |b|^2 + |d|^2 = 1, \quad \begin{pmatrix} b \\ d \end{pmatrix} = \lambda \begin{pmatrix} -\overline{c} \\ \overline{a} \end{pmatrix} \qquad (\lambda \in \mathbf{C}) \\ &\iff |a|^2 + |c|^2 = 1 = |\lambda|, \quad \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} -\lambda\overline{c} \\ \lambda\overline{a} \end{pmatrix} \qquad (\det(U) = \lambda). \end{aligned}$$

(3.12.10) Un plongement $\mathbf{H} \hookrightarrow M_2(\mathbf{C})$. On fait agir l'anneau $\mathbf{H}$ sur lui-même par multiplication à gauche : pour tout $x \in \mathbf{H}$, l'application

$$m(x) : \mathbf{H} \longrightarrow \mathbf{H}, \qquad y \mapsto xy$$

est $\mathbf{H}$-linéaire à droite, $m(x)(yz) = (m(x)y)z$ $(x, y, z \in \mathbf{H})$. Tout quaternion s'écrit, de manière unique, $x = u + jv$ $(u, v \in \mathbf{C})$. L'identification

$$\mathbf{H} \xrightarrow{\sim} \mathbf{C}^2, \qquad x = u + jv \mapsto \begin{pmatrix} u \\ v \end{pmatrix}, \qquad a + bi + cj + dk \mapsto \begin{pmatrix} a + bi \\ c - di \end{pmatrix}$$

est $\mathbf{C}$-linéaire à droite, ce qui nous permet de considérer $m(x)$ comme une matrice $M(x) \in \mathrm{End}_{\mathbf{C}}(\mathbf{C}^2) = M_2(\mathbf{C})$. On calcule (en utilisant la règle $(\forall z \in \mathbf{C})\ \ zj = j\overline{z}$)

$$m(u + jv) : a + jb \mapsto (u + jv)(a + jb) = (ua - \overline{v}b) + j(va + \overline{u}b)$$
$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto \begin{pmatrix} ua - \overline{v}b \\ va + \overline{u}b \end{pmatrix} = \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix},$$

d'où

$$M(u + jv) = \begin{pmatrix} u & -\overline{v} \\ v & \overline{u} \end{pmatrix}.$$

On a

$$m(x + x') = m(x) + m(x'), \qquad m(xx') = m(x) \circ m(x'), \qquad (\forall r \in \mathbf{R})\ \ m(r) = r \cdot \mathrm{id},$$

donc $M : \mathbf{H} \longrightarrow M_2(\mathbf{C})$ est un homomorphisme d'anneaux (plus précisement, de $\mathbf{R}$-algèbres).

(3.12.11) Proposition. *L'application $M : \mathbf{H} \hookrightarrow M_2(\mathbf{C})$ induit un isomorphisme de groupes $U_1(\mathbf{H}) \xrightarrow{\sim} SU(2)$.*

Preuve. D'après 3.12.9, M induit une bijection $U_1(\mathbf{H}) \xrightarrow{\sim} SU(2)$ (puisque $N(a + jc) = |a|^2 + |c|^2$). Comme $M(xy) = M(x)M(y)$, cette bijection est un homomorphisme (donc un isomorphisme) de groupes.

(3.12.12) Le groupe $U_n(\mathbf{H})$. On note

$$U_n(\mathbf{H}) = \{u \in GL_n(\mathbf{H}) \mid (\forall x, y \in \mathbf{H}^n)\ \ f(u(x), u(y)) = f(x, y)\},$$

où

$$f(x, y) = \sum_{\alpha=1}^{n} x_\alpha \overline{y_\alpha}, \qquad\qquad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in \mathbf{H}^n$$

est le produit quaternionique-hermitien sur $\mathbf{H}^n$.

(3.12.13) Exercice. (i) *L'application*

$$M : M_n(\mathbf{H}) \longrightarrow M_{2n}(\mathbf{C}), \qquad A + jB \mapsto \begin{pmatrix} A & -\overline{B} \\ B & \overline{A} \end{pmatrix}$$

est un homomorphisme injectif d'anneaux.
(ii) *Formuler et démontrer un analogue quaternionique de 3.11.9.*
(iii) *M induit un isomorphisme de groupes $U_n(\mathbf{H}) \xrightarrow{\sim} U(2n) \cap Sp(2n, \mathbf{C})$.*

(3.12.14) (i) Il est plus commode d'écrire l'isomorphisme 3.12.7 comme

$$SU(2)/\{\pm I\} \xrightarrow{\sim} SO(3).$$

(ii) Pour tout $n \geq 3$, il existe un groupe compact connexe $Spin(n)$ et un isomorphisme $Spin(n)/\{\pm 1\} \xrightarrow{\sim} SO(n)$.
(iii) Si on identifie $S(\mathbf{H}_0) \xrightarrow{\sim} S^2$ à $\mathbf{C} \cup \{\infty\}$ par la projection stéréographique, alors l'action induite de $SU(2) \xrightarrow{\sim} U_1(\mathbf{H}) \longrightarrow SO(3)$ sur $\mathbf{C} \cup \{\infty\}$ est conjuguée à l'action 'usuelle' par les homographies ($SU(2) \subset GL_2(\mathbf{C}) \longrightarrow PGL_2(\mathbf{C})$).

(3.12.15) Exercice. *Soit $C \subset \mathbf{R}^3$ le cube dont les sommets sont $\begin{pmatrix} \pm 1 \\ \pm 1 \\ \pm 1 \end{pmatrix}$. On admet le fait que le groupe*

$$G = \{g \in SO(3) \mid g(C) = C\}$$

des rotations qui conservent C a 24 éléments.
(i) *Décrire géométriquement tous les éléments de G (donner l'axe et l'angle).*
(ii) *Déterminer les 48 quaternions de norme 1 qui donnent lieu aux éléments de G, via l'homomorphisme $U_1(\mathbf{H}) \longrightarrow SO(3)$.*
(iii) *Montrer que l'on a, effectivement, $|G| = 24$.* *[Indication : voir [N].]*

(3.12.16) Exercice ($Spin(4) = Spin(3) \times Spin(3)$). *On identifie l'espace des quaternions $\mathbf{H}$ muni de la forme quadratique $N(q) = q\overline{q} = \overline{q}q$ à $\mathbf{R}^4$ muni de la forme quadratique $a^2 + b^2 + c^2 + d^2$:*

$$a + bi + cj + dk \mapsto \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

(i) *Soient $q_1, q_2 \in U_1(\mathbf{H})$; on note $p(q_1, q_2) : \mathbf{H} \longrightarrow \mathbf{H}$ l'endomorphisme $\mathbf{R}$-linéaire suivant :*

$$p(q_1, q_2) : y \mapsto q_1\, y\, q_2^{-1}.$$

Montrer que $p(q_1, q_2)$ est une isométrie de $(\mathbf{H}, N)$.
(ii) *Montrer que p définit un homomorphisme de groupes*

$$p : U_1(\mathbf{H}) \times U_1(\mathbf{H}) \longrightarrow O(\mathbf{H}, N) = O(4),$$

c'est-à-dire que l'on a $p(q_1, q_2) \circ p(q_1', q_2') = p(q_1 q_1', q_2 q_2')$.
(iii) *Déterminer le noyau de p.*
(iv) *On sait que si $I, J \in U_1(\mathbf{H}) \cap \mathbf{H}_0$ vérifient $JI = -IJ$, alors $1, I, J$ et $K = IJ$ forment une base orthonormée de $\mathbf{H}$. Soient $q_1 = e^{\theta I} = \cos\theta + I \sin\theta$ et $q_2 = e^{\theta' I} = \cos\theta' + I \sin\theta'$, où $\theta, \theta' \in \mathbf{R}/2\pi\mathbf{Z}$. Déterminer les matrices respectives de $p(q_1, 1)$, $p(1, q_2)$ et $p(q_1, q_2)$ dans la base $1, I, J, K$.*
(v) *Montrer que l'on a $p(q_1, q_2) \in SO(4)$, pour tous $q_1, q_2 \in U_1(\mathbf{H})$.*
(vi) *Montrer que $\mathrm{Im}(p) = SO(4)$ (c'est-à-dire que tout $U \in SO(4)$ s'écrit $U = p(q_1, q_2)$).* *[On pourra utiliser 3.10.17.]*
(vii) *Que se passe-t-il si l'on remplace $\mathbf{H}$ par $M_2(\mathbf{R})$?* *[Indication : voir 3.13.]*

3.13 Quaternions généralisés

(3.13.1) Dictionnaire $\mathbf{H} \longleftrightarrow M_2(\mathbf{R})$. La construction 3.12.6 s'applique aussi à l'anneau $M_2(\mathbf{R})$:

$\mathbf{H}$	$M_2(\mathbf{R})$
$x = a + bi + cj + dk$	$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
$\overline{x} = a - bi - cj - dk$	$\overline{x} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$
$\mathbf{R} = \mathbf{R} \cdot 1 \subset \mathbf{H}$	$\mathbf{R} = \mathbf{R} \cdot I \subset M_2(\mathbf{R})$
$\mathrm{Tr}(x) = x + \overline{x} = 2a$	$\mathrm{Tr}(x) = x + \overline{x} = a + d$
$N(x) = x\overline{x} = a^2 + b^2 + c^2 + d^2$	$N(x) = x\overline{x} = ad - bc = \det(x)$
$x \in \mathbf{H}^* \iff N(x) \neq 0 \iff x \neq 0$	$x \in M_2(\mathbf{R})^* \iff \det(x) \neq 0 \iff x \in GL_2(\mathbf{R})$
$x \in U_1(\mathbf{H}) \iff N(x) = 1$	$x \in SL_2(\mathbf{R}) \iff \det(x) = 1$
$x \in \mathbf{H}_0 \iff \mathrm{Tr}(x) = 0 \iff$ $x = bi + cj + dk$	$x \in M_2(\mathbf{R})^0 \iff \mathrm{Tr}(x) = 0 \iff$ $x = \begin{pmatrix} u & v+w \\ v-w & -u \end{pmatrix}$
$N\lvert_{\mathbf{H}_0} = b^2 + c^2 + d^2$	$\det\lvert_{M_2(\mathbf{R})^0} = -u^2 - v^2 + w^2$
$\mathrm{Ad}(x)(y) = xyx^{-1}$	$\mathrm{Ad}(x)(y) = xyx^{-1}$
$\mathrm{Ad} : \mathbf{H}^* \longrightarrow GL_{\mathbf{R}}(\mathbf{H})$	$\mathrm{Ad} : GL_2(\mathbf{R}) \longrightarrow GL_{\mathbf{R}}(M_2(\mathbf{R}))$
$\mathrm{Tr}(xyx^{-1}) = \mathrm{Tr}(y)$	$\mathrm{Tr}(xyx^{-1}) = \mathrm{Tr}(y)$
$N(xyx^{-1}) = N(y)$	$\det(xyx^{-1}) = \det(y)$
$\mathrm{Ad}\lvert_{\mathbf{H}_0} : \mathbf{H}^*/\mathbf{R}^* \hookrightarrow O(\mathbf{H}_0, N) = O(3)$	$\mathrm{Ad}\lvert_{M_2(\mathbf{R})^0} : GL_2(\mathbf{R})/\mathbf{R}^* I \hookrightarrow O(M_2(\mathbf{R})^0, \det) = O(1,2)$
$\mathrm{Ad}\lvert_{\mathbf{H}_0} : \mathbf{H}^*/\mathbf{R}^* \xrightarrow{\sim} SO(3)$	$\mathrm{Ad}\lvert_{M_2(\mathbf{R})^0} : PGL_2(\mathbf{R}) \xrightarrow{\sim} SO(1,2)$
$\mathrm{Ad}\lvert_{\mathbf{H}_0} : U_1(\mathbf{H})/\{\pm 1\} \xrightarrow{\sim} SO(3)$	$\mathrm{Ad}\lvert_{M_2(\mathbf{R})^0} : SL_2(\mathbf{R})/\{\pm I\} \xrightarrow{\sim} SO^+(1,2)$

Ici, on a noté $SO^+(1,2)$ la composante connexe de $SO(1,2)$ qui contient I.
D'où provient la seconde colonne du dictionnaire?

(3.13.2) Explication algébrique : quaternions généralisés. Soit K un corps, $\mathrm{car}(K) \neq 2$; fixons $\alpha, \beta \in K^*$. On définit l'anneau des quaternions généralisés comme

$$\mathbf{H}_{\alpha,\beta} = \left(\frac{\alpha, \beta}{K}\right)_2 = K \oplus Ki \oplus Kj \oplus Kk,$$

où

$$i^2 = \alpha, \qquad j^2 = \beta, \qquad k = ij = -ji \quad (\Longrightarrow \quad k^2 = -\alpha\beta, \qquad jk = -kj = -\beta i, \qquad ki = -ik = -\alpha j)$$

et

$$(\forall a \in K)\,(\forall x \in \mathbf{H}_{\alpha,\beta}) \qquad ax = xa.$$

Le conjugué, la trace et la norme sont définis comme en 3.12.1. En particulier, on a

$$\mathbf{H}_{\alpha,\beta}^{\mathrm{Tr}=0} = \{xi + yj + zk \mid x, y, z \in K\}$$
$$N(xi + yj + zk) = \alpha x^2 + \beta y^2 - \alpha\beta z^2 = \alpha\beta\left(\alpha(y/\alpha)^2 + \beta(x/\beta)^2 - z^2\right).$$

Propriété principale : Si l'équation $\alpha x^2 + \beta y^2 - z^2 = 0$ admet une solution non nulle $(x, y, z) \in K^3 - \{(0,0,0)\}$, alors il existe un isomorphisme de K-algèbres $\mathbf{H}_{\alpha,\beta} \xrightarrow{\sim} M_2(K)$ qui transforme Tr (resp.

N) en la trace (resp. le déterminant). S'il n'y a aucune solution non nulle, alors $\mathbf{H}_{\alpha,\beta}$ est un corps (non-commutatif).

Exemple : Si $\alpha = \beta = 1$, alors l'application

$$\mathbf{H}_{1,1} \xrightarrow{\sim} M_2(K), \qquad a + bi + cj + dk \mapsto \begin{pmatrix} a+b & c+d \\ c-d & a-b \end{pmatrix}$$

est un isomorphisme de K-algèbres.

En général, la construction 3.12.6 définit un isomorphisme de groupes

$$\mathbf{H}^*_{\alpha,\beta}/K^* \xrightarrow{\sim} SO(\mathbf{H}^{\mathrm{Tr}=0}_{\alpha,\beta}, N).$$

Si $K = \mathbf{R}$ et $\alpha = \beta = -1$ (resp. $\alpha = \beta = 1$), on obtient la première (resp. la seconde) colonne du dictionnaire 3.13.1.

(3.13.3) Explication géométrique. Soit K un corps, $\mathrm{car}(K) \neq 2$. Soit

$$Q : q(X_0, X_1, X_2) = \sum_{i,j=0}^{2} A_{ij} X_i X_j = 0$$

une conique projective non-singulière sur K (i.e. $A = (A_{ij}) = A^T \in GL_3(K)$). On suppose que $Q(K) \neq \emptyset$ ($\iff$ le cône isotrope $C(q) \neq \{\vec{0}\}$).

La conique Q satisfait aux propriétés suivantes :

(3.13.3.1) Pour tout point K-rationnel $O \in Q(K)$ et toute droite $D \subset \mathbf{P}^2(K)$ qui ne passe pas par O, la projection de centre O induit une **bijection** $f : Q(K) \xrightarrow{\sim} D$ ($\xrightarrow{\sim} \mathbf{P}^1(K)$) (voir 3.8.9).

(3.13.3.2) Si $O, O' \in Q(K)$ sont deux points K-rationnels de Q et $D \subset \mathbf{P}^2(K)$ (resp. $D' \subset \mathbf{P}^2(K)$) une droite qui ne passe pas par O (resp. par O'), alors l'application $f' \circ f^{-1} : D \xrightarrow{\sim} Q(K) \xrightarrow{\sim} D'$ est une **homographie** (voir 3.8.9).

(3.13.3.3) Soit

$$GP(Q) := \{g \in GP(\mathbf{P}^2(K)) = PGL_3(K) = GL_3(K)/K^* \cdot I \mid g(Q(K)) = Q(K)\}.$$

D'après 3.5.11(ii), on a $GP(Q) = PGO(q) = GO(q)/K^* \cdot I$. D'après 3.4.9, l'application canonique $SO(q) \longrightarrow PGO(q)$ est un isomorphisme.

(3.13.3.4) Fixons $O \in Q(K)$ et $D \subset \mathbf{P}^2(K)$ comme en (3.13.3.1); soit $f : Q(K) \xrightarrow{\sim} D$ la bijection correspondante. Il résulte de (3.13.3.2) que, pour tout $g \in GP(Q)$, la bijection

$$f \circ g|_{Q(K)} \circ f^{-1} : D \xrightarrow{\sim} Q(K) \xrightarrow{\sim} Q(K) \xrightarrow{\sim} D$$

est une homographie. L'homomorphisme ainsi défini

$$GP(Q) \longrightarrow GP(D) \xrightarrow{\sim} PGL_2(K), \qquad g \mapsto f \circ g|_{Q(K)} \circ f^{-1}$$

est un **isomorphisme**.

En résumé, on obtient des isomorphismes de groupes

$$SO(q) \xrightarrow{\sim} PGO(q) \xrightarrow{\sim} GP(Q) \xrightarrow{\sim} GP(D) \xrightarrow{\sim} GP(\mathbf{P}^1(K)) = PGL_2(K).$$

Par exemple, si $K = \mathbf{R}$ et $q = X_0^2 - X_1^2 - X_2^2$, on obtient un isomorphisme

$$SO(1,2) \xrightarrow{\sim} PGO(1,2) \xrightarrow{\sim} PGL_2(\mathbf{R}).$$

(3.13.4) Exercice. *L'action* $g : X \mapsto gX{}^t\overline{g}$ *de* $g \in SL_2(\mathbf{C})$ *sur* $V = \{X \in M_2(\mathbf{C}) \mid \overline{X} = {}^tX\}$ *induit un homomorphisme de groupes* $SL_2(\mathbf{C}) \longrightarrow O(V, \det)$ *et un isomorphisme* $SL_2(\mathbf{C})/\{\pm I\} \xrightarrow{\sim} SO^+(1,3)$.

3.14 Linéarisation (= l'algèbre de Lie) de $O(f), U(f), Sp(f)$

(3.14.1) Sous-groupes à un paramètre. (i) L'application

$$\mathbf{R} \longrightarrow SO(2), \qquad t \mapsto R(t) = \begin{pmatrix} \cos(t) & -\sin(t) \\ \sin(t) & \cos(t) \end{pmatrix}$$

est un homomorphisme de groupes (i.e. $R(s+t) = R(s)\,R(t)$) différentiable : on a

$$R'(t) = \begin{pmatrix} -\sin(t) & -\cos(t) \\ \cos(t) & -\sin(t) \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} R(t), \qquad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = R'(0).$$

(ii) En général, un **sous-groupe à un paramètre** de $GL_n(\mathbf{C})$ est un homomorphisme de groupes différentiable $U : \mathbf{R} \longrightarrow GL_n(\mathbf{C})$, c'est à dire une aplication différentiable qui vérifie $U(s+t) = U(s)\,U(t)$ (pour tous $s, t \in \mathbf{R}$). On appelle la matrice $U'(0) \in M_n(\mathbf{C})$ le **générateur infinitésimal** de U.

Pour toute matrice $X \in M_n(\mathbf{C})$, il existe un unique sous-groupe à un paramètre $U : \mathbf{R} \longrightarrow GL_n(\mathbf{C})$ vérifiant $U'(0) = X$. En effet, l'équation $U(s+t) = U(s)\,U(t)$ entraîne

$$U'(t) = \left.\frac{\partial U(s+t)}{\partial s}\right|_{s=0} = \left.\frac{\partial (U(s)\,U(t))}{\partial s}\right|_{s=0} = U'(0)\,U(t) = X\,U(t), \qquad U(0) = I.$$

Cette équation différentielle a une unique solution, à savoir

$$U(t) = e^{tX}\,U(0) = e^{tX} = \sum_{k=0}^{\infty} X^k \frac{t^k}{k!} \qquad\qquad (X^0 = I),$$

où la série est absolument convergente.

(3.14.2) Exemples : (i) Si la matrice X est diagonale, e^X l'est aussi :

$$X = \begin{pmatrix} a_{11} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix}, \qquad e^X = \begin{pmatrix} e^{a_{11}} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{a_{nn}} \end{pmatrix}$$

(ii) Si la matrice X est triangulaire, e^X l'est aussi :

$$X = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ 0 & \cdots & a_{nn} \end{pmatrix}, \qquad e^X = \begin{pmatrix} e^{a_{11}} & \cdots & * \\ \vdots & \ddots & \vdots \\ 0 & \cdots & e^{a_{nn}} \end{pmatrix}$$

(iii) Si $g \in GL_n(\mathbf{C})$, alors on a $(gXg^{-1})^k = gX^kg^{-1}$ $(k \geq 0)$, d'où

$$e^{(gXg^{-1})} = g(e^X)g^{-1}.$$

(iv) Si $X, Y \in M_n(\mathbf{C})$ commutent, i.e. si $XY = YX$, alors on a $e^{X+Y} = e^X e^Y = e^Y e^X$. En particulier, si $Y = -X$, on obtient $e^{-X} = (e^X)^{-1}$ (donc $e^X \in GL_n(\mathbf{C})$).

(v)

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad (\forall k > 1) \quad X^k = 0, \qquad e^{tX} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}.$$

(vi)

$$X = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad X^{2k} = (-1)^k I, \qquad X^{2k+1} = (-1)^k X,$$

$$e^{tX} = \sum_{k=0}^{\infty} \frac{(-1)^k t^{2k}}{(2k)!} I + \sum_{k=0}^{\infty} \frac{(-1)^k t^{2k+1}}{(2k+1)!} X = (\cos(t))I + (\sin(t))X = R(t) \in SO(2).$$

(vii)

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad X^{2k} = I, \qquad X^{2k+1} = X,$$

$$e^{tX} = \sum_{k=0}^{\infty} \frac{t^{2k}}{(2k)!} I + \sum_{k=0}^{\infty} \frac{t^{2k+1}}{(2k+1)!} X = (\mathrm{ch}(t))I + (\mathrm{sh}(t))X = \begin{pmatrix} \mathrm{ch}(t) & \mathrm{sh}(t) \\ \mathrm{sh}(t) & \mathrm{ch}(t) \end{pmatrix} \in SO(1,1).$$

(viii)

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad X + Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

$$e^{tX} = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \qquad e^{tY} = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, \qquad e^{t(X+Y)} = \begin{pmatrix} \mathrm{ch}(t) & \mathrm{sh}(t) \\ \mathrm{sh}(t) & \mathrm{ch}(t) \end{pmatrix} \neq e^{tX}e^{tY},\ e^{tY}e^{tX}.$$

(ix) Si $X \in M_n(\mathbf{C})$ est une matrice nilpotente (c'est-à-dire que s'il existe un entier $N \geq 1$ tel que $X^N = 0$ $\Longleftrightarrow$ toutes les valeurs propres de X sont égales à 0), alors on a $X^n = 0$, d'où

$$U := e^X = I + X + \cdots X^{n-1}/(n-1)!, \qquad (U - I)^n = 0.$$

Réciproquement, si $U \in GL_n(\mathbf{C})$ est unipotente ($\Longleftrightarrow$ il existe un entier $N \geq 1$ tel que $(U - I)^N = 0$ $\Longleftrightarrow$ toutes les valeurs propres de X sont égales à 1 $\Longleftrightarrow$ $(U - I)^n = 0$), alors la matrice

$$X := \log(I + (U - I)) = (U - I) - (U - I)^2/2 + \cdots + (-1)^{n-1}(U - I)^{n-1}/(n-1) \in M_n(\mathbf{C})$$

vérifie $X^n = 0$ et $e^X = U$.
(x) Plus précisement, si $X \in M_n(\mathbf{C})$ est une matrice nilpotente, alors il existe $g \in GL_n(\mathbf{C})$ telle que $X = gYg^{-1}$, où

$$Y = \begin{pmatrix} Y_{n_1} & 0 & \cdots & 0 \\ 0 & Y_{n_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & Y_{n_k} \end{pmatrix}, \qquad Y_m = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \in M_m(\mathbf{C}), \qquad \sum_{j=1}^{k} n_j = n;$$

L'exponentielle de tY_m est égale à

$$e^{tY_m} = \begin{pmatrix} 1 & t & t^2/2 & \cdots & t^m/m! \\ 0 & 1 & t & \cdots & t^{m-1}/(m-1)! \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & t \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

(3.14.3) Exercice. (i) *Si* $X \in M_n(\mathbf{C})$, *alors* $\det(e^X) = e^{\mathrm{Tr}(X)}$.
(ii) *Si* $X \in GL_n(\mathbf{C})$, *alors il existe* $Y \in M_n(\mathbf{C})$ *vérifiant* $e^Y = X$.
[Utiliser 3.14.2(ii),(iii).]
(iii) *Si* $X \in \mathrm{Herm}_n(\mathbf{C})$, *alors* $e^{iX} \in U(n)$. *Réciproquement, si* $U \in U(n)$, *alors il existe* $X \in \mathrm{Herm}_n(\mathbf{C})$ *vérifiant* $e^{iX} = U$.

(3.14.4) Définition. *Soient* $K = \mathbf{R}$ *ou* $\mathbf{C}$, $\sigma = \mathrm{id}$ *ou la conjugaison complexe,* f *une forme* σ*-sesquilinéaire non-dégénérée sur* K^n, *soit hermitienne, soit bilinéaire symétrique, soit bilinéaire antisymétrique. Soit* $G = GL_n(K)$, $SL_n(K)$, $U(f)$, $SU(f)$, $O(f)$, $SO(f)$ *ou* $Sp(f)$. *On définit*

$$\mathrm{Lie}(G) := \{X \in M_n(K) \mid (\forall t \in \mathbf{R})\ \ e^{tX} \in G\}.$$

(3.14.5) Moralement, $\mathrm{Lie}(G)$ est la linéarisation du groupe G dans un voisinage de l'identité $I \in G$, puisqu'on a

$$e^{tX} = I + tX + O(t^2).$$

(3.14.6) Théorème. (i) $\mathrm{Lie}(G) \subset M_n(K)$ *est un* $\mathbf{R}$*-espace vectoriel.*
(ii) *Pour tous* $X, Y \in \mathrm{Lie}(G)$, *leur* **commutateur** $[X,Y] := XY - YX$ *est contenu dans* $\mathrm{Lie}(G)$ *(on dit que* $\mathrm{Lie}(G)$ *est une* **algèbre de Lie réelle***).*
(iii) *L'exponentielle*

$$\exp : \mathrm{Lie}(G) \longrightarrow G, \qquad X \mapsto e^X$$

définit une bijection entre un voisinage convenable $\mathscr{U}$ *de* $\vec{0} \in \mathrm{Lie}(G)$ *et son image* $\exp(\mathscr{U}) \subset G$. *En fait,* G *est muni d'une structure canonique de variété différentiable et la restriction de* $\exp$ *à* $\mathscr{U}$ *est un difféomorphisme* $\mathscr{U} \xrightarrow{\sim} \exp(\mathscr{U})$. *En particulier, la dimension (réelle) de* G *est égale à* $\dim_{\mathbf{R}}(\mathrm{Lie}(G))$.
(iv) *(Campbell-Hausdorff) Il existe une série universelle*

$$F(X,Y) = X + Y + \frac{1}{2}[X,Y] + \frac{1}{12}[X,[X,Y]] + \cdots$$

(qui ne contient que des commutateurs itérés de X *et* Y *à coefficients rationnels), qui converge absolument pour tous* $X, Y \in M_n(\mathbf{C})$ *et vérifie*

$$e^{F(X,Y)} = e^X e^Y.$$

En particulier, la multiplication dans $\exp(\mathscr{U})$ *est déterminée par* $\mathrm{Lie}(G)$.

(3.14.7) Proposition. *Soit* $K = \mathbf{R}$ *ou* $\mathbf{C}$.
(i) $gl_n(K) := \mathrm{Lie}(GL_n(K)) = M_n(K)$.
(ii) $sl_n(K) := \mathrm{Lie}(SL_n(K)) = \{X \in M_n(K) \mid \mathrm{Tr}(X) = 0\}$.
(iii) *Si* $f(x,y) = {}^t x A\, {}^\sigma y$ *et* $G = U(f)$ *ou* $O(f)$ *ou* $Sp(f)$, *alors on a*

$$\mathrm{Lie}(G) = \{X \in M_n(K) \mid {}^t X A + A\, {}^\sigma X = 0\}.$$

Preuve. (i) Trivial. (ii) Pour tout $X \in M_n(K)$, on a :

$$(\forall t \in \mathbf{R}) \quad 1 = \det(e^{tX}) = e^{t\,\mathrm{Tr}(X)} \iff (\forall t \in \mathbf{R}) \quad t\,\mathrm{Tr}(X) \in 2\pi i \mathbf{Z} \iff \mathrm{Tr}(X) = 0.$$

(iii) On a

$$G = \{U \in GL_n(K) \mid {}^t U A\, {}^\sigma U = A\}.$$

On fixe $X \in M_n(K)$ et on définit

$$f : \mathbf{R} \longrightarrow M_n(K), \qquad t \mapsto {}^t(e^{tX}) A\, {}^\sigma(e^{tX}).$$

La fonction f est diférentiable; elle vérifie $f(0) = A$ et

$$f'(t) = {}^t(e^{tX})\,{}^tXA\,{}^{\sigma}(e^{tX}) + {}^t(e^{tX})A\,{}^{\sigma}X\,{}^{\sigma}(e^{tX}) = {}^t(e^{tX})({}^tXA + A\,{}^{\sigma}X)\,{}^{\sigma}(e^{tX}),$$

d'où

$$X \in \mathrm{Lie}(G) \iff (\forall t \in \mathbf{R}) \quad f(t) = A \iff (\forall t \in \mathbf{R}) \quad f'(t) = 0 \iff {}^tXA + A\,{}^{\sigma}X = 0.$$

(3.14.8) On peut reformuler 3.14.4 en utilisant les **nombres duaux**

$$K[\varepsilon] = \{a + \varepsilon b \mid a, b \in K,\ \varepsilon^2 = 0\}$$

et les matrices à coefficients à $K[\varepsilon]$:

$$M_n(K[\varepsilon]) = \{A + \varepsilon B \mid A, B \in M_n(K),\ \varepsilon^2 = 0\}.$$

Si l'on définit $G(K[\varepsilon])$ comme l'ensemble de matrices $g \in M_n(K[\varepsilon])$ qui vérifient les équations qui définissent G, alors on a

$$\mathrm{Lie}(G) = \{X \in M_n(K) \mid I + \varepsilon X \in G(K[\varepsilon])\}.$$

Exemples : (1) $G = SL_2(K) = \{g \in GL_2(K) \mid \det(g) = 1\}$, ce qui entraîne que $X \in M_2(K)$ appartient à $\mathrm{Lie}(SL_2(K))$ si et seulement si

$$1 = \det(I + \varepsilon X) = \begin{vmatrix} 1 + \varepsilon X_{11} & \varepsilon X_{12} \\ \varepsilon X_{21} & 1 + \varepsilon X_{22} \end{vmatrix} = 1 + \varepsilon(X_{11} + X_{22}) + \varepsilon^2(X_{11}X_{22} - X_{12}X_{21}) = 1 + \varepsilon(X_{11} + X_{22}),$$

ce qui équivaut à $\mathrm{Tr}(X) = X_{11} + X_{22} = 0$.
(2) Sous les hypothèses de 3.14.7(iii), on a

$$G = \{g \in M_n(K) \mid {}^tgA\,{}^{\sigma}g = A\},$$

ce qui entraîne que $X \in M_n(K)$ appartient à $\mathrm{Lie}(G)$ si et seulement si l'on a

$$A = {}^t(I + \varepsilon X)A\,{}^{\sigma}(I + \varepsilon X) = A + \varepsilon({}^tXA + A\,{}^{\sigma}X) + \varepsilon^2({}^tXA\,{}^{\sigma}X) = A + \varepsilon({}^tXA + A\,{}^{\sigma}X),$$

d'où

$$\mathrm{Lie}(G) = \{X \in M_n(K) \mid {}^tXA + A\,{}^{\sigma}X = 0\}.$$

(3.14.9) Exemples : (i) $G = O_n(K)$: on a $\sigma = \mathrm{id}$ et $A = I_n$, donc

$$o_n(K) := \mathrm{Lie}(O_n(K)) = \{X \in M_n(K) \mid {}^tX + X = 0\}$$
$$so_n(K) := \mathrm{Lie}(SO_n(K)) = o_n(K) \cap sl_n(K) = o_n(K)$$

et

$$\dim_K(o_n(K)) = 1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

(ii) $G = U_n(\mathbf{C}) = U(n)$: on a $\sigma(u + iv) = u - iv$ et $A = I_n$, donc

$$u_n(\mathbf{C}) := \mathrm{Lie}(U_n(\mathbf{C})) = \{X \in M_n(\mathbf{C}) \mid {}^tX + \overline{X} = 0\}$$
$$\dim_{\mathbf{R}} u_n(\mathbf{C}) = n + 2(1 + 2 + \cdots + (n-1)) = n^2.$$

(iii) $G = SU_n(\mathbf{C}) = SU(n) = U_n(\mathbf{C}) \cap SL_n(\mathbf{C})$: on a

$$su_n(\mathbf{C}) := \mathrm{Lie}(SU_n(\mathbf{C})) = u_n(\mathbf{C}) \cap sl_n(\mathbf{C}) = \{X \in M_n(\mathbf{C}) \mid {}^tX + \overline{X} = 0,\ \mathrm{Tr}(X) = 0\}$$
$$\dim_{\mathbf{R}} su_n(\mathbf{C}) = n^2 - 1.$$

(3.14.10) Exercice. *Déterminer les algèbres de Lie* $\mathrm{Lie}(O(r,s))$, $\mathrm{Lie}(U(r,s))$, $\mathrm{Lie}(Sp(2n,K))$ *et leurs dimensions.*

(3.14.11) Exercice. *Définir et déterminer* $\mathrm{Lie}(GO(n))$, $\mathrm{Lie}(GU(n))$, $\mathrm{Lie}(GSp(2n,K))$ *et* $\mathrm{Lie}(GA_n(K))$.

(3.14.12) Les algèbres de Lie de tous les groupes que l'on a considérés en 3.14.4 sont assez simples : par exemple, les commutateurs dans $sl_2(K) = \mathrm{Lie}(SL_2(K))$ s'écrivent

$$[X,Y] = H, \qquad [H,X] = 2X, \qquad [H,Y] = -2Y,$$

où

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

(3.14.13) Représentation adjointe. Si, sous les hypothèses de 3.14.4, $g \in G$ et $X \in \mathrm{Lie}(G)$, alors on a

$$(\forall t \in \mathbf{R}) \qquad e^{t(gXg^{-1})} = g\, e^{tX} g^{-1} \in G \implies gXg^{-1} \in \mathrm{Lie}(G).$$

Les applications

$$\mathrm{Ad}(g) : \mathrm{Lie}(G) \longrightarrow \mathrm{Lie}(G), \qquad X \mapsto gXg^{-1}$$

ainsi définies forment alors la **représentation adjointe**

$$\mathrm{Ad} : G \longrightarrow GL_{\mathbf{R}}(\mathrm{Lie}(G)).$$

Si $G = SL_2(\mathbf{R})$, on a $\mathrm{Lie}(G) = M_2(\mathbf{R})^0$, donc on obtient l'homomorphisme qui intervient dans la seconde colonne de 3.13.1.

(3.14.14) Exercice. (i) *Si $\lambda \in \mathbf{C}$ est une valeur propre de $X \in M_n(\mathbf{C})$, alors e^λ est une valeur propre de e^X. La réciproque est-elle vraie?*
(ii) *L'exponentielle* $\exp : sl_2(\mathbf{R}) \longrightarrow SL_2(\mathbf{R})$ *n'est pas surjective. Plus précisement, on a*

$$(\forall X \in M_2(\mathbf{R})) \qquad e^X \neq \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

(iii) *L'exponentielle* $\exp : sl_2(\mathbf{C}) \longrightarrow SL_2(\mathbf{C})$ *est surjective.*
(iv) *Si $G = SO(n), U(n)$ ou $SU(n)$, alors l'exponentielle* $\mathrm{Lie}(G) \longrightarrow G$ *est surjective.*
(v) *Déterminer l'image de l'exponentielle* $\exp : \mathrm{Lie}(O(1,1)) \longrightarrow O(1,1)$.

(3.14.15) Exercice. (i) *Montrer que l'on a* $SU(1,1) = \left\{ \begin{pmatrix} a & \bar{c} \\ c & \bar{a} \end{pmatrix} \,\middle|\, a, c \in \mathbf{C},\ |a|^2 - |c|^2 = 1 \right\}$.
(ii) *Existe-t-il $U \in SU(1,1)$ qui n'est pas diagonalisable ?*
(iii) *Déterminer* $su(1,1) = \mathrm{Lie}(SU(1,1))$.
(iv) *Existe-t-il $X \in su(1,1)$ vérifiant $X^2 = 0$, $X \neq 0$?*

(3.14.16) Exercice. *Soit $f : \mathbf{C}^2 \times \mathbf{C}^2 \longrightarrow \mathbf{C}$ la forme hermitienne* $f\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}\right) = i(x_1\overline{y_2} - x_2\overline{y_1})$.
(i) *Déterminer* $su(f) = \mathrm{Lie}(SU(f))$.
(ii) *Déterminer* $SU(f)$.

(iii) *Trouver une base de* $\mathbf{C}^2$ *qui soit orthogonale par rapport à* f.
(iv) *Trouver un changement de coordonnées qui transforme* f *à une forme standard*

$$x_1\overline{y_1} + \cdots + x_r\overline{y_r} - x_{r+1}\overline{y_{r+1}} - \cdots - x_{r+s}\overline{y_{r+s}}.$$

(v) *Trouver une matrice* $g \in GL_2(\mathbf{C})$ *telle que* $gSU(f)g^{-1} = SU(r,s)$.

(3.14.17) Exercice. (i) *Montrer que le groupe* $G = SO(n)$ *agit naturellement sur la sphère* $S^{n-1} = \{x \in \mathbf{R}^n \mid \|x\| = 1\}$ *de telle façon que l'orbite (resp., le stabilisateur) d'un point est égale à* S^{n-1} *(resp., à* $SO(n-1)$*). En déduire que*

$$\dim(SO(n)) = \dim(SO(n-1)) + (n-1) = (n-1) + \cdots + 2 + 1 = n(n-1)/2.$$

(ii) *De même pour* $U(n)$ *agissant sur* $S^{2n-1} = \{z \in \mathbf{C}^n \mid \|z\|^2 = |z_1|^2 + \cdots + |z_n|^2 = 1\}$*; dans ce cas, on a*

$$\dim(U(n)) = \dim(U(n-1)) + (2n-1) = (2n-1) + \cdots + 3 + 1 = n^2.$$

(3.14.18) Exercice. (i) *Montrer : si* $U \in O(n) = O_n(\mathbf{R})$ $(n \geq 1)$ *et* $(U-I)^2 = 0$*, alors* $U = I$.
(ii) *Montrer : si* $X \in o_3(\mathbf{C}) = \mathrm{Lie}(O_3(\mathbf{C}))$ *et* $X^2 = 0$*, alors* $X = 0$.
(iii) *Montrer : si* $U \in O_3(\mathbf{C})$ *et* $(U-I)^2 = 0$*, alors* $U = I$.
iv) *Déterminer l'ensemble de matrices*

$$\{X \in o_3(\mathbf{C}) \mid X^3 = 0\} \subset M_3(\mathbf{C}).$$

(v) *Y a-t-il* $U \in O_3(\mathbf{C})$*,* $U \neq I$*, telle que l'on ait* $(U-I)^3 = 0$ *?*

3.15 Isométries affines

(3.15.1) Définition. *Un* **espace affine euclidien** *est un espace affine réel* X *dont l'espace de directions* $\vec{X}$ *est un espace euclidien. La* **distance** *de deux points* $x, y \in X$ *est* $d(x,y) = \|\overrightarrow{xy}\|$*. Une* **isométrie** *de* X *est une application* $f : X \longrightarrow X$ *telle que*

$$(\forall x, y \in X) \qquad d(f(x), f(y)) = d(x,y).$$

(3.15.2) Proposition. *Soit* X *un espace affine euclidien. Une application* $f : X \longrightarrow X$ *est une isométrie de* X $\iff$ f *est affine et* $\vec{f} \in O(\vec{X})$.

Preuve. Si f est affine et $\vec{f} \in O(\vec{X})$, alors on a

$$d(f(x), f(y)) = \|\overrightarrow{f(x)f(y)}\| = \|\vec{f}(\overrightarrow{xy})\| = \|\overrightarrow{xy}\| = d(x,y),$$

pour tous $x, y \in X$. Réciproquement, soit $f : X \longrightarrow X$ une isométrie. On fixe une origine $x_0 \in X$; la translation $t(\vec{a})$ par n'importe quel vecteur $\vec{a} \in \vec{X}$ étant une isométrie, la composée $g = t(\overrightarrow{f(x_0)x_0}) \circ f : X \longrightarrow X$ est une isométrie qui fixe x_0. On identifie X à $\vec{X}$ à l'aide de x_0; on considère donc g comme une application $g : \vec{X} \longrightarrow \vec{X}$ qui vérifie $g(\vec{0}) = \vec{0}$ et

$$\begin{aligned} d(g(x), g(y))^2 = \|g(y) - g(x)\|^2 = (g(y) \mid g(y)) + (g(x) \mid g(x)) - 2(g(y) \mid g(x)) = \\ = d(x,y)^2 = \|x - y\|^2 = (y \mid y) + (x \mid x) - 2(y \mid x), \end{aligned}$$

pour tous $x, y \in \vec{X}$. Si l'on prend $y = \vec{0}$, on obtient $(g(x) \mid g(x)) = (x \mid x)$ (et de même pour y), d'où

$$\forall x, y \in \vec{X} \qquad (g(y) \mid g(x)) = (y \mid x),$$

ce qui entraîne que l'application g est linéaire et appartient à $O(\vec{X})$ (d'après 3.4.3.4).

(3.15.3) Il résulte de 3.15.2 que les isométries de X s'écrivent dans les coordonnées cartésiennes associées à n'importe quel choix d'origine $x_0 \in X$ et n'importe quel choix de base **orthonormée** de $\vec{X}$ de la façon suivante :

$$f(x) = Ax + a \qquad\qquad (A \in O(n),\ u \in \mathbf{R}^n).$$

On sait, d'après 3.10.24, que le vecteur $a \in \mathbf{R}^n$ admet une unique décomposition

$$a = (I - A)b + c, \qquad (I - A)c = 0, \qquad b, c \in \mathbf{R}^n$$

($c \in \mathbf{R}^n$ est unique, mais b ne l'est pas, en général). Ceci entraîne que l'on a

$$f(x) = Ax + (I - A)b + c = A(x - b) + b + c, \qquad f(x + b) = Ax + b + c, \qquad Ac = c.$$

En particulier, si l'on remplace les coordonnées cartésiennes x par $x' = x + b$ ($\iff$ si l'on remplace l'origine x_0 par son translaté par $-b$), alors l'application f s'écrit dans les coordonnées x'

$$f'(x') = Ax' + c, \qquad Ac = c.$$

On a aussi

$$f(x) = g(x) + c = g(x + c), \qquad g(x) = A(x - b) + b, \qquad \mathrm{Fix}(g) = \{x \in X \mid g(x) = x\} = b + \mathrm{Ker}(I - A).$$

Voici une version abstraite du même calcul.

(3.15.4) Proposition. *Soit $f : X \longrightarrow X$ une isométrie affine d'un espace affine euclidien. Alors il existe une unique décomposition $f = t(\vec{c}) \circ g = g \circ t(\vec{c})$, où $g : X \longrightarrow X$ est une isométrie affine dont l'ensemble de points fixes $\mathrm{Fix}(g) = \{x \in X \mid g(x) = x\}$ est non vide et $\vec{c} \in \overrightarrow{\mathrm{Fix}(g)} = \mathrm{Ker}(\vec{g} - \mathrm{id}) = \mathrm{Ker}(\vec{f} - \mathrm{id})$ (comme $\mathrm{Fix}(g)$ n'est pas vide, c'est un sous-espace affine de X).*

Preuve. Soit $x_0 \in X$. D'après 3.10.24, le vecteur $\overrightarrow{x_0 f(x_0)} \in \vec{X}$ admet une unique décomposition

$$\overrightarrow{x_0 f(x_0)} = \vec{c} + (\vec{b} - \vec{f}(\vec{b})), \qquad \vec{f}(\vec{c}) = \vec{c}, \qquad \vec{b} \in \vec{X}.$$

On pose $x_1 = x_0 + \vec{b}$; comme

$$f(x_1) = f(x_0) + \vec{f}(\vec{b}) = x_0 + \vec{c} + \vec{b} - \vec{f}(\vec{b}) + \vec{f}(\vec{b}) = x_0 + \vec{c} + \vec{b} = x_1 + \vec{c},$$

l'isométrie $g := t(-\vec{c}) \circ f$ vérifie $g(x_1) = x_1$. Il en résulte que $g(x) = x \iff \vec{g}(\overrightarrow{x_1 x}) = \overrightarrow{x_1 x}$, donc $\mathrm{Fix}(g)$ est un sous-espace affine de X de direction $\overrightarrow{\mathrm{Fix}(g)} = \mathrm{Ker}(\vec{g} - \mathrm{id}) = \mathrm{Ker}(\vec{f} - \mathrm{id})$. On a aussi $f \circ t(-\vec{c})(x) = f(x - \vec{c}) = f(x) - \vec{f}(\vec{c}) = f(x) - \vec{c} = t(-\vec{c}) \circ f(x)$, d'où $f = t(\vec{c}) \circ g = g \circ t(\vec{c})$. L'unicité résulte de 3.10.24.

(3.15.5) Exemple ($\dim(X) = 2$) : Soit $f : X \longrightarrow X$ une isométrie affine d'un plan affine euclidien.
(i) Si $\vec{f} = \mathrm{id}$, alors $f = t(\vec{c})$ est une **translation**, $g = \mathrm{id}$ et $\mathrm{Fix}(g) = X$.
(ii) Si $\vec{f} \in O^+(\vec{X})$ est une rotation ($\vec{f} \neq \mathrm{id}$), alors $\mathrm{Ker}(\vec{f} - \mathrm{id}) = 0$, $\vec{c} = \vec{0}$ et $f = g$ admet un unique point fixe P (f est une **rotation** autour de P).
(iii) Si $\vec{f} \in O^-(\vec{X})$ est une réflexion, alors $f = t(\vec{c}) \circ g = g \circ t(\vec{c})$, où g est une réflexion affine par rapport à une droite affine $d \subset X$ de direction $\vec{d} = \mathrm{Ker}(\vec{f} - \mathrm{id})$, et $\vec{c} \in \vec{d}$ est parallèle à d. On dit que f est une **symétrie glissée**.

(3.15.6) Exercice. *Classifier les isométries affines en dimension* 3.

(3.15.7) Exercice. *Soient*

$$A = \frac{1}{3}\begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}, \qquad a = \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}.$$

(i) *Montrer que l'application* $x \mapsto Ax$ $(x \in \mathbf{R}^3)$ *est une isométrie de* $\mathbf{R}^3$ *(où* $\mathbf{R}^3$ *est muni du produit scalaire usuel).*
(ii) *Déterminer les sous-espaces* $E_\pm = \{x \in \mathbf{R}^3 \mid Ax = \pm x\}$.
(iii) *Décrire géometriquement l'isométrie* $x \mapsto Ax$ $(x \in \mathbf{R}^3)$.
(iv) *Écrire l'isométrie affine* $f(x) = Ax + a$ $(x \in \mathbf{R}^3)$ *comme* $f = g \circ t(b) = t(b) \circ g$, *où* g *est une isométrie affine dont l'ensemble de points fixes* $\mathrm{Fix}(g) = \{x \in \mathbf{R}^3 \mid g(x) = x\}$ *n'est pas vide, et* $t(b)$ *est la translation par un vecteur* $b \in \mathbf{R}^3$ *qui est faiblement parallèle à* $\mathrm{Fix}(g)$.
(v) *Décrire géometriquement l'isométrie affine* g.

(3.15.8) Exercice. *On considère* $\mathbf{R}^3$ *muni du produit scalaire usuel. Soient*

$$P_1 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix}, \quad P_2 = \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix}, \quad P_3 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} 5/3 \\ -2/3 \\ 1/3 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 1 \\ 0 \\ 3 \end{pmatrix}, \quad Q_3 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}.$$

(i) *Déterminer toutes les isométries affines* $f(x) = Ax + a$ *de* $\mathbf{R}^3$ *(où* $A \in O(3)$ *et* $a \in \mathbf{R}^3$*) telles que* $\forall j = 1, 2, 3 \quad f(P_j) = P_j$.
(ii) *Déterminer toutes les isométries affines* $g(x) = Bx + b$ *de* $\mathbf{R}^3$ *(où* $B \in O(3)$ *et* $b \in \mathbf{R}^3$*) telles que* $\forall j = 1, 2, 3 \quad g(P_j) = Q_j$.
(iii) *Si* $B \in SO(3)$, *alors on a* $g = h \circ t = t \circ h$, *où* h *est une rotation d'angle* β *autour une droite affine* d *et* t *est une translation par un vecteur* $\overrightarrow{c}$ *parallèle à* d*; déterminer* d, $\cos(\beta)$ *et* $\overrightarrow{c}$.
(iv) *Si* $x \mapsto Bx$ *est une réflexion, alors on a* $g = h' \circ t' = t' \circ h'$, *où* h' *est une réflexion par rapport à un hyperplan affine* H' *et* t' *est une translation par un vecteur* $\overrightarrow{c}'$ *parallèle à* H'*; déterminer* H' *et* $\overrightarrow{c}'$.

(3.15.9) Exercice. *Soit* $n \geq 2$ *un entier.*
(i) *Déterminer l'image de l'application exponentielle* $\exp : o(n) \longrightarrow O(n)$.
(ii) *Soit*

$$G_n = \{x \mapsto Ax + a \mid A \in O(n),\, a \in \mathbf{R}^n\} = \left\{ \begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix} \,\middle|\, A \in O(n),\, a \in \mathbf{R}^n \right\} \subset GL_{n+1}(\mathbf{R})$$

$(x \in \mathbf{R}^n)$ *le groupe des isométries affines de* $\mathbf{R}^n$. *On sait que l'on a*

$$\mathrm{Lie}(G_n) = \left\{ \begin{pmatrix} B & b \\ 0 & 0 \end{pmatrix} \,\middle|\, B \in o(n),\, b \in \mathbf{R}^n \right\} \subset M_{n+1}(\mathbf{R}).$$

Déterminer l'image de l'application exponentielle $\exp : \mathrm{Lie}(G_n) \longrightarrow G_n$.
(iii) *Pour* $n = 2$ *et* 3, *décrire géométriquement les orbites des sous-groupes à un paramètre de* G_n *agissant sur* $\mathbf{R}^n$, *à savoir les ensembles*

$$\{(e^{tX})(x) \mid t \in \mathbf{R}\},$$

où $X \in \mathrm{Lie}(G_n)$, $x \in \mathbf{R}^n$ *et où l'on a noté*

$$\begin{pmatrix} A & a \\ 0 & 1 \end{pmatrix}(x) = Ax + a.$$

VERSION 9/10/2008

Bibliographie

[L] Y. Ladegaillerie, *Géométrie - Affine, projective, euclidienne et anallagmatique*, Ellipses, Paris, 2003.

[N] J. Nekovář, *Formes Quadratiques et Géométrie*, polycopié du cours LM 223, disponible à http://www.math.jussieu.fr/∼nekovar/co/q/

[P] D. Perrin, *Cours d'algèbre*, Ellipses, Paris, 1995.

[B] M. Berger, *Géométrie*, CEDIC, Paris, 1977.