Plan de cours détaillé
ELM42 Algèbre 3, L2 S3 2009/2010

David Vauclair

27 avril 2010

Table des matières

1 Dualité dans les espaces vectoriels de dimension finie

K désigne un corps (dans les exemples, ce sera toujours $\mathbb{R}, \mathbb{C}$ ou $\mathbb{Q}$), E, F des espaces vectoriels de dimension finie. L'ensemble des applications linéaires $E \to F$ est noté $Hom_K(E, F)$. Le sous-espace vectoriel de E engendré par une partie $S \subset E$ est noté $< S >$. Par "base de E", on entend "n-uplet de vecteurs dont la famille sous-jacente est libre et engendre E".

1.1 Espace dual

Rappel 1.1 *1. L'ensemble $Hom_K(E, F)$ est un espace vectoriel pour les opérations suivantes :*

(i) Si $\phi, \psi : E \to F$ sont deux applications linéaires, alors $\phi+\psi : E \to F$ désigne l'application $x \mapsto \phi(x) + \psi(x)$; c'est une application linéaire.

(ii) Si $\phi : E \to F$ est une application linéaire et $\lambda \in K$ un scalaire, alors $\lambda\phi : E \to F$ désigne l'application $x \mapsto \lambda\phi(x)$; c'est une forme linéaire.

2. L'espace vectoriel $E^* := Hom_K(E, K)$ s'appelle l'espace dual de E. Ses éléments s'appellent des formes linéaires sur E.

Exemple 1.2 *(i) Soit $\underline{e} = (e_1, \ldots, e_n)$ une base de E. Si $x \in E$, alors il existe un unique n-uplet de scalaires $(\lambda_1, \ldots, \lambda_n)$ tels que $x = \lambda_1 e_1 + \ldots + \lambda_n e_n$. Pour i fixé, le scalaire λ_i dépend de x ; notons-le $e_i^*(x)$. On a ainsi défini une application $E \to K$, $x \mapsto e_i^*(x)$. C'est l'application "$i$ème coordonnée par rapport à la base $\underline{e}$". On vérifie sans peine que e_i^* est une forme linéaire.*

(ii) On vient de voir comment associer n formes linéaires $e_1^*, \ldots, e_n^*$ à une base $\underline{e}$ donnée. Comme toute forme linéaire, e_i^* est caractérisée par les valeurs qu'elle prend en les vecteurs de la base $\underline{e}$. Celles-ci sont facile à retenir : $e_i^*(e_j) = 0$ si $j \neq i$ et 1 si $j = i$.

Exercice 1.3 *Soit $\underline{e} = ((1, 1, 0), (0, 1, 1), (1, 0, 0))$. Calculer $e_i^*((x, y, z))$ pour $i = 1, 2, 3$.*

Solution : $y - z, z, x - y + z$.

Proposition 1.4 *Soit $\underline{e} = (e_1, \ldots, e_n)$ une base de E. Alors $\underline{e}^* := (e_1^*, \ldots, e_n^*)$ est une base de E^*. On l'appelle la base duale à $\underline{e}$.*

Preuve. Liberté : si $\lambda_1 e_1^* + \ldots + \lambda_n e_n^* = 0$ est une égalité dans E^*, on obtient $\lambda_i = 0$ en l'évaluant en e_i.

Génération : Si $\phi \in E^*$, alors $\phi = \phi(e_1)e_1^* + \ldots + \phi(e_n)e_n^*$.

Remarque 1.5 *1. On voit donc que si E est de dimension n, alors E^* aussi.*

2. On prendra garde que e_i^* dépend de la base $\underline{e}$ tout entière, et pas seulement de e_i.

Exercice 1.6 *Soit $\phi : \mathbb{R}^3 \to \mathbb{R}$, $(x, y, z) \mapsto \phi((x, y, z) = x+2y+3z$. Vérifier que $\phi \in E^*$ et exprimer ses coordonnées par rapport à la base $\underline{e}^*$ de l'exercice 1.3.*

Solution : $e_1^* + 3e_2^* + 5e_3^*$.

Proposition 1.7 *Soient $\underline{e}$ et $\underline{f}$ deux bases de E et P la matrice de passage de $\underline{e}$ à $\underline{f}$. Alors ${}^tP$ est la matrice de passage de $\underline{f}^*$ à $\underline{e}^*$.*

Preuve. Si $P = (p_{i,j})$, il s'agit de montrer que $e_i^* = \sum p_{i,j} f_j^*$. Pour le vérifier, il suffit d'évaluer en f_j, $i = 1, \ldots, n$ (exprimer f_j dans la base $\underline{e}$ pour évaluer le premier membre).

1.2 Espace bidual

Définition 1.8 *$E^{**} := (E^*)^*$ s'appelle l'espace bidual de E. C'est un espace vectoriel de même dimension que E^*, et donc que E.*

Proposition 1.9 *Pour $x \in E$ et $\phi \in E^*$, notons $ev_x(\phi) := \phi(x)$.*

(i) L'application $ev_x : E^* \to K$ est linéaire, ie. $ev_x \in E^*$.

(ii) L'application $ev : E \to E^{**}$, $x \mapsto ev_x$ est linéaire. Mieux, c'est un isomorphisme d'espace vectoriels.

Preuve. Pour l'injectivité de ev, choisir une base $\underline{e}$ de E et remarquer que $x \in Ker\, ev \Rightarrow \forall i, e_i^*(x) = 0$. La bijectivité s'en déduit par le théorème du rang.

Exercice 1.10 *Si $\underline{e}$ est une base de E, et $\underline{\phi} = \underline{e}^*$ est sa base duale. Quelle est la base duale $\underline{\phi}^*$ de $\underline{\phi}$?*

Remarque 1.11 *Pour la proposition 1.9, il est crucial que la dimension soit finie. C'est un bon exercice de montrer que pour un espace vectoriel de dimension quelconque, l'application linéaire ev est toujours injective et qu'elle est surjective si et seulement si* $\dim E < \infty$.

1.3 Restriction à un sous-espace vectoriel

Soit F un sous-espace vectoriel de E.

Définition 1.12 *Si $\phi \in E^*$, on note $\phi_{|F}$, ou $res_F^E \phi$ l'application $F \to K$, $x \mapsto \phi(x)$. C'est une forme linéaire.*

Proposition 1.13 *L'application $res_F^E : E^* \to F^*$, $\phi \mapsto \phi_{|F}$ est une application linéaire surjective, dont le noyau est de dimension* $\dim E - \dim F$.

Preuve. Pour la surjectivité, il suffit de choisir une base $\underline{f} = (f_1, \ldots, f_k)$ de F, et de montrer que les éléments f_i^* de sa base duale sont dans l'image. Pour cela, on complète $\underline{f}$ en un base $\underline{e} = (f_1, \ldots, f_k, e_{k+1}, \ldots, e_n)$ de E, et on remarque que pour $i \leq k$, $res_F^E e_i^* = f_i^*$.

Pour la dimension du noyau, on peut au choix utiliser le théorème du rang ou remarquer que $\phi \in Ker\, res_E^F$ si et seulement ses k premières coordonnées dans la base $\underline{e}^*$ sont nulles, ie ssi $x \in < e_{k+1}^*, \ldots, e_n^* >$.

Exercice 1.14 *Soit $f : E \to F$ une application linéaire, et notons $f^* : F^* \to E^*$, $\phi \mapsto \phi \circ f$.*

(i) Montrer que $\phi \in Ker\, f^* \Leftrightarrow Im\, f \subset Ker\, \phi$.

(ii) Montrer que $\psi \in Im\, f^* \Leftrightarrow Ker\, f \subset Ker\, \psi$ (on pourra introduire un supplémentaire de $Ker\, f$ dans E).

2 Formes bilinéaires

2.1 Généralités

2.1.1 Définition

Définition 2.1 *Une forme bilinéaire sur $E \times F$ est une application $E \times F \to K$ vérifiant les propriétés suivantes :*
- (linéarité à droite) $\forall x \in E$, $y \mapsto b(x, y)$ est linéaire.
- (linéarité à gauche) $\forall y \in F$, $x \mapsto b(x, y)$ est linéaire.

Exemple 2.2 *1. $b : K \times K \to K$, $(x, y) \mapsto xy$.*
2. Pour $(a_{i,j}) \in M_{n\times m}(K)$, $b : K^n \times K^m \to K$, $(x, y) \mapsto \sum a_{i,j}x_iy_j$.
3. (le même) Pour $A \in M_{n\times m}(K)$, $b : M_{n\times 1}(K) \times M_{m\times 1}(K)$, $(X, Y) \mapsto {}^tXAY$.
4. Si A est une K-algèbre et $\phi \in A^*$, $b : A \times A \to K$, $(x, y) \mapsto \phi(xy)$.

Définition 2.3 *Soit b une forme bilinéaire sur $E \times F$, $\underline{e}$ une base de E et $\underline{f}$ une base de F. On définit la matrice de b par rapport aux bases $\underline{e}$ et $\underline{f}$ comme suit :*

$$Mat(b, \underline{e}, \underline{f}) := (b(e_i, f_j))_{i,j}$$

Proposition 2.4 *Soit $\underline{e} = (e_1, \dots, e_n)$ une base de E et $\underline{f} = (f_1, \dots, f_m)$ une base de F. Si $x \in E$ (resp. $y \in F$) on note $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ (resp. $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$) le vecteur des coordonnées de x (resp. y) par rapport à la base $\underline{e}$ (resp. $\underline{f}$).*

(i) Si b est une forme bilinéaire sur $E \times F$, alors $Mat(b, \underline{e}, \underline{f})$ est l'unique matrice B telle que $\forall (x, y) \in E \times F$, $b(x, y) = {}^tXBY$.

(ii) Si $B \in M_{n\times m}(K)$, alors il existe une unique forme bilinéaire b sur $E \times F$ telle que $Mat(b, \underline{e}, \underline{f}) = B$.

Preuve : (i) La formule s'obtient en développant $b(\sum x_ie_i, \sum y_ij)$. Pour l'unicité, on retrouve $Mat(b, \underline{e}, \underline{f})$ à partir de la formule en appliquant celle-ci avec $x = e_i$ et $y = f_j$.

(ii) Pour l'existence, il suffit de remarquer que $(x, y) \mapsto {}^tXBY$ est une forme bilinéaire.

Exemple 2.5 *Considérons $b : \mathbb{R}^2 \times \mathbb{R}^3$, $(x, y) \mapsto x_1y_1 + 3x_1y_3 - 2x_2y_2$.*

(i) Si $\underline{e}$ et $\underline{f}$ sont les bases canoniques respectives de $\mathbb{R}^2$ et $\mathbb{R}^3$, alors

$$Mat(b, \underline{e}, \underline{f}) = \begin{pmatrix} 1 & 0 & 1 \\ 0 & -2 & 0 \end{pmatrix}$$

(ii) Si $\underline{e}' = ((1, 0), (1, 1))$ et $\underline{f}' = ((-1, 0, 0), (1, 1, -1), (0, 1, 0))$, alors

$$Mat(b, \underline{e}, \underline{f}) = \begin{pmatrix} -1 & 0 & 1 \\ -1 & -1 & -2 \end{pmatrix}$$

Proposition 2.6 *Notons P (resp. Q) la matrice de passage de $\underline{e}$ (resp. $\underline{f}$) à $\underline{e}'$ (resp. $\underline{f}'$). Si $B = Mat(b, \underline{e}, \underline{f})$ et $B' = Mat(b, \underline{e}', \underline{f}')$, alors*

$$B' = {}^tPBQ$$

Preuve : Comme $Coord(x, \underline{e}) = P\,Coord(x, \underline{e}')$ et $Coord(y, \underline{f}) = Q\,Coord(y, \underline{f}')$, il suffit d'utiliser la caractérisation de $Mat(b, \underline{e}', \underline{f}')$ par la formule de la proposition précédente.

2.1.2 Orthogonalité

Définition 2.7 *Soit b une forme bilinéaire sur $E \times F$.*

1. *Soit $y \in F$ (resp. $Y \subset F$).*
   - *(i) On dit que x est orthogonal à gauche à y (resp. Y) pour b si $b(x,y) = 0$ (resp. si $b(x,y) = 0$ pour tout $y \in Y$).*
   - *(ii) On note ${}^{\perp}y$ ou ${}^{\perp b}y$ (resp. ${}^{\perp}Y$ ou ${}^{\perp b}Y$) l'ensemble des vecteurs de E qui sont orthogonaux à gauche à y (resp. à Y).*
2. *Soit $x \in E$ (resp. $X \subset E$).*
   - *(i) On dit que y est orthogonal à droite à x (resp. X) pour b si $b(x,y) = 0$ (resp. si $b(x,y) = 0$ pour tout $x \in X$).*
   - *(ii) On note $x^{\perp}$ ou $x^{\perp b}$ (resp. $X^{\perp}$ ou $X^{\perp b}$) l'ensemble des vecteurs de E qui sont orthogonaux à droite à x (resp. à X).*

Proposition 2.8 *Soit b une forme bilinéaire sur $E \times F$, et $X \subset E$, $X' \subset E$, $Y \subset F$ et $Y' \subset F$.*

- *(i) $X \subset {}^{\perp}Y \Leftrightarrow Y \subset X^{\perp}$.*
- *(ii) $Y \subset ({}^{\perp}Y)^{\perp}$ et $X \subset {}^{\perp}(X^{\perp})$.*
- *(iii) ${}^{\perp}Y$ et $X^{\perp}$ sont des sous-espaces vectoriels.*
- *(iv) ${}^{\perp}Y = {}^{\perp} < Y >$ et $X^{\perp} =< X >^{\perp}$.*
- *(v) ${}^{\perp}Y \cap {}^{\perp}Y' = {}^{\perp}(Y \cup Y') = {}^{\perp}(< Y > + < Y' >)$*
  et $X^{\perp} \cap X'^{\perp} = (X \cup X')^{\perp} = (< X > + < X' >)^{\perp}$.
- *(vi) ${}^{\perp}(< Y > + < Y' >) = {}^{\perp}(Y \cup Y') \subset {}^{\perp}(Y \cap Y')$*
  et $(< X > + < X' >)^{\perp} = (X \cup X')^{\perp} \subset X^{\perp} \cap X'^{\perp}$.

Preuve : il suffit d'écrire les définitions.

Définition 2.9 *On dit que b est non dégénérée si ${}^{\perp}F = 0$ et $E^{\perp} = 0$.*

Exercice 2.10 *Soient $\underline{e} = (e_1, e_2, e_3)$ une base de E et $\underline{f}$ une base de F. Montrer que la forme bilinéaire de matrice $\begin{pmatrix} 1 & 0 & 1 \\ 0 & -1 & 0 \\ -1 & 1 & 1 \end{pmatrix}$ par rapport aux bases $\underline{e}$ et $\underline{f}$ est non dégénérée.*

2.1.3 Applications linéaires associées à une formes bilinéaire

Fixons une application bilinéaire b sur $E \times F$.

Définition 2.11 *(i) Si $x \in E$, on note $b_*(x)$, ou $b(x,*)$, l'application $F \to K$, $y \mapsto b(x,y)$.*

(ii) Si $y \in F$, on note $b_*(y)$, ou $b(y,*)$ l'application $E \to K$, $x \mapsto b(x,y)$.

Proposition 2.12 *1. (i) Pour tout $x \in E$, $b_*(x)$ est une forme linéaire sur F.*

(ii) Pour tout $y \in F$, ${}_*b(y)$ est une forme linéaire sur E.

2. (i) *L'application* $b_* : E \to F^*$ *est linéaire.*

   (ii) *L'application* ${}_*b : F \to E^*$ *est linéaire.*

Preuve : On utilise la bilinéarité de b.

Lemme 2.13 1. (i) $Kerb_* = {}^\perp F$.

   (ii) $Ker_*b = E^\perp$.

2. (i) *Si* F' *est un sev de* F, $Ker\, res_{F'} \circ b_* = {}^\perp F'$.

   (ii) *Si* E' *est un sev de* E, *alors* $Ker\, res_{E'} \circ {}_*b = E'^\perp$.

Preuve : il suffit d'écrire les définitions.

Corollaire 2.14 *Soient* $E' \leq E$ *et* $F' \leq F$ *deux sev.*

(i) $dim\, E'^\perp \geq dim\, F - \dim E'$.

(ii) $dim\, F'^\perp \geq dim\, E - \dim F'$.

Preuve : Il s'agit simplement d'écrire le théorème du rang pour les applications linéaires $res_{E'} \circ {}_*b$ et $res_{F'} \circ b_*$.

Remarque 2.15 *Si* b *est non dégénérée, le corollaire appliqué au cas où* $E' = E$ *et* $F' = F$ *donne deux inégalités contraires, et donc* $dim\, F - \dim E = 0$.

Proposition 2.16 *Soit* $\underline{e}$ *(resp.* $\underline{f}$*) une base de* E *(resp.* F*) et* $\underline{e}^*$ *(resp.* $\underline{f}^*$*) sa base duale. Si* $B = Mat(b, \underline{e}, \underline{f})$, *alors*

(i) $Mat(b_*, \underline{e}, \underline{f}^*) = {}^tB$.

(ii) $Mat({}_*b, \underline{f}, \underline{e}^*) = B$.

2.1.4 Formes bilinéaires non dégénérées

On suppose désormais que E et F ont même dimension.

Proposition 2.17 *Soient* $\underline{e}$, *underlinef des bases respectives de* E *et* F.
Sont équivalents :

(i) b *est non dégénérée.*

(ii) b_* *est un isomorphisme.*

(iii) ${}_*b$ *est un isomorphisme.*

(iv) $Mat(b, \underline{e}, \underline{f})$ *est inversible.*

Preuve : pour $(i) \Leftrightarrow (ii)$ (resp. $(i) \Leftrightarrow (iii)$) on applique le théorème du rang à b_* (resp. ${}_*b$). La dernière équivalence résulte de ce que $Mat({}_*b, \underline{f}, \underline{e}^*) = Mat(b, \underline{e}, \underline{f})$.

Remarque 2.18 *La proposition précédente montre que l'inversibilité de la matrice* $Mat(b, \underline{e}, \underline{f})$ *ne dépend pas du choix des bases* $\underline{e}$ *et* $\underline{f}$. *C'est cohérent avec la formule de changement de base.*

Exemple 2.19 *Crochet de dualité. Soit $b : F^* \times F$, $b(\phi, y) = \phi(y)$. Dans ce cas :*

- $b(\phi, *) = \phi$, ie. $b_* : F^* \to F^*$ est l'application identique. La forme bilinéaire b est donc non dégénérée.

- $b(*, y) = ev_y$, ie. $b^* : F \to F^{**}$ est l'application de bidualité. On retombe sur le fait (déjà établi au chapitre sur la dualité) que c'est un isomorphisme.

Proposition 2.20 *Si b une forme bilinéaire non dégénérée sur $E \times F$, et si $E' \leq E$ et $F' \leq F$ deux sev, alors :*

(i) $dim\, E'^{\perp} = dim\, F - \dim E'$.

(ii) $dim\, F'^{\perp} = dim\, E - \dim F'$.

Preuve : Comme b_* est ici un isomorphisme, ces égalités découlent des formules pour la dimension du noyau de la restriction (cf. chapitre dualité).

Exercice 2.21 *Soit $f : E \to F^*$ une application linéaire quelconque. Existe-t-il une forme bilinéaire b sur $E \times F$ telle que ${}_*b = f$?*

2.2 Formes bilinéaires symétriques

On se restreint désormais au cas $E = F$ et on dit "forme bilinéaire sur E" au lieu de "forme bilinéaire sur $E \times E$". Aussi si $\underline{e}$ base de E, on note simplement $Mat(b, \underline{e})$ pour $Mat(b, \underline{e}, \underline{e})$.

Définition 2.22 *Soit b une forme bilinéaire sur E. On dit que*

(i) b est symétrique si $b(x, y) = b(y, x)$ pour tout $x, y \in E$.

(ii) b est antisymétrique si $b(x, y) = -b(y, x)$ pour tout $x, y \in E$.

(iii) b est alternée si $b(x, x) = 0$ pour tout $x \in E$.

Exercice 2.23 *Si b est alternée, alors b est antisymétrique. Montrer que si dans K, on a $2 \neq 0$, alors la réciproque est vraie aussi.*

Proposition 2.24 *Soit une forme bilinéaire sur E et $\underline{e}$ une base de E. Sont alors équivalents :*

(i) b est symétrique.

(ii) $b_* = {}_*b$.

(iii) $Mat(b, \underline{e})$ est symétrique.

De même que

(i) b est antisymétrique.

(ii) $b_* = -{}_*b$.

(iii) $Mat(b, \underline{e})$ est antisymétrique.

Preuve : Dans les deux cas, $(i) \Leftrightarrow (ii)$ est immédiat et $(ii) \Leftrightarrow (iii)$ résulte de l'interprétation matricielle de b_* et ${}_*b$.

Remarque 2.25 *Si b est soit symétrique soit antisymétrique, alors pour tout $X \subset E$, on a égalité entre $X^{\perp}$ et ${}^{\perp}X$.*

Dans **toute la suite de ce chapitre** on s'intéresse exclusivement au cas des **formes bilinéaires symétriques** (fbs).

2.2.1 Matrice et invariants d'une fbs

Fixons une fbs b sur E.

Proposition 2.26 *Si P est la matrice de passage d'une base $\underline{e}$ de E à une autre $\underline{e}'$ et si l'on note $B = Mat(b, \underline{e})$, $B' = Mat(b, \underline{e}')$, alors*

$$B' = {}^tPBP$$

Définition 2.27 *Soient B et B' deux matrices carrées. On dit que B' est congruente à B s'il existe P inversible telle que $B' = {}^tPBP$.*

Exercice 2.28 *Montrer que la relation "B' est congruente à B" est une relation d'équivalence sur $M_n(K)$.*

Définition 2.29 *Soient $\delta, \delta' \in K$. On dit que δ' est congru à d modulo un carré de $K^\times$ et l'on note $\delta \equiv \delta' \mathrm{mod}\ K^{\times 2}$ s'il existe $\alpha \in K$ tel que $\delta' = \delta x^2$.*

Exemple 2.30 *Si $K = \mathbb{R}$, alors $3 \equiv 28 \mathrm{mod}\ K^{\times 2}$. En effet, $3 = 28\alpha^2$ avec par exemple $\alpha = \frac{1}{2\sqrt{7}}$. Par contre $3 \not\equiv 0 \mathrm{mod}\ K^{\times 2}$, puisque l'on ne peut pas écrire $3 = 0\alpha^2$ avec $\alpha \in \mathbb{R}$.*

Lemme 2.31

(i) La relation "$\delta \equiv \delta' \mathrm{mod}\ K^{\times 2}$" est une relation d'équivalence.

(ii) Si $K = \mathbb{C}$, deux nombres non nuls sont toujours congrus mod $K^{\times 2}$. Aussi, les classes de congruences mod $K^{\times 2}$ sont $\{\overline{0}, \overline{1}\}$.

(iii) Si $K = \mathbb{R}$, deux nombres non nuls sont congrus mod $K^{\times 2}$ si et seulement s'il sont de même signe. Aussi, les classes de congruences mod $K^{\times 2}$ sont $\{\overline{-1}, \overline{0}, \overline{1}\}$.

(iv) Si $K = \mathbb{Q}$, deux nombres x et y non nuls sont congrus mod $K^{\times 2}$ si et seulement s'ils on même signe et si leurs décomposition en facteur premiers $x = \prod p_p^n$, $y = \prod p_p^m$ vérifient $n_p \equiv m_p \mathrm{mod}\ (2)$. En particulier, les classes de congruences de K mod K^2 sont $\{\overline{0}\} \cup \{\overline{\epsilon p_1 \dots p_k}, \epsilon \in \{\pm 1\}, k \geq 0, p_1, \dots, p_k$ premiers$\}$.

Preuve : (i) Il s'agit de vérifier que pour $\delta, \delta', \delta'' \in K$, on a toujours
- $\delta \equiv \delta \mathrm{mod}\ K^{\times 2}$.
- $\delta' \equiv \delta \mathrm{mod}\ K^{\times 2} \Rightarrow \delta \equiv \delta' \mathrm{mod}\ K^{\times 2}$.
- $(\delta' \equiv \delta \mathrm{mod}\ K^{\times 2}$ et $\delta'' \equiv \delta' \mathrm{mod}\ K^{\times 2}) \Rightarrow \delta' \equiv \delta \mathrm{mod}\ K^{\times 2}$.

C'est très facile.

(ii) vient du fait que tous les nombres complexes sont des carrés et (iii) vient du fait qu'un nombre réel est le carré d'un nombre réel si et seulement s'il est positif. Quant à (iv), il suffit de constater qu'un nombre rationnel est le carré d'un nombres rationnel si et seulement si sa décomposition en facteurs premier d'un nombre rationnel est de la forme $\prod p_p^n$ où tous les n_p sont pairs.

Proposition 2.32 *(i) Si B et B' sont congruentes, alors $\det B \equiv \det B \mathrm{mod}\ K^{\times 2}$.*

(ii) La classe de $\det Mat(b, \underline{e})$ modulo $K^{\times 2}$ ne dépend pas de $\underline{e}$. On l'appelle le discriminant de b.

(iii) b est non dégénérée si et seulement si $\mathrm{disc}\, b \neq \overline{0}$.

Définition 2.33 *Soit* $b_* : E \to E^*$ *l'application linéaire attachée à* b*. On convient d'appeler*

- *"Le noyau de* b*" celui de* b_**. On notera aussi* $Ker\, b := Ker\, b_*$*.*
- *"Le rang de* b*" celui de* b_**. On notera aussi* $rg\, b := rg\, b_*$*.*

Cette terminologie est troublante à première vue, car b n'est pas une application linéaire donc ne possède ni noyau ni rang. Il faut bien comprendre qu'il s'agit simplement d'une convention, d'un abus de langage bien commode.

Proposition 2.34 $rg\, b + \dim Ker\, b = \dim E$.

Preuve : c'est juste le théorème du rang appliqué à l'application linéaire $b_* : E \to E^*$.

Remarque 2.35 *De manière plus explicite, on a* $Ker\, b_* = \{x, \forall y \in E,\, b(x,y) = 0\}$*. En d'autres termes* $Ker\, b = E^{\perp}$*.*

La proposition suivante découle immédiatement de l'interprétation matricielle de b_*.

Proposition 2.36 *Soit* $\underline{e}$ *une base de* E *et* $B = Mat(b, \underline{e})$*.*

(i) $rg\, b = rg\, B$*.*

(ii) Si $X = Coord(x, \underline{e})$*, alors* $x \in Ker\, b \Leftrightarrow AX = 0$*.*

2.2.2 Isotropie et non dégénérescence

Ici encore, b désigne systématiquement une fbs sur E.

Définition 2.37 *L'ensemble* $\{x, \in E, b(x,x) = 0\}$ *s'appelle le cône isotrope de* b*. Ses éléments s'appellent les vecteurs isotropes de* b*.*

Exercice 2.38 *Dessiner le cone isot de* $x_1y_1 + x_2y_2 - x_3y_3$*, et en particulier dessiner les sections* $x_3 = 1$*,* $x_3 = x_2 + 2$*,* $x_2 = 1$*.*

Définition 2.39

1. *(i) On dit que* b *est totalement isotrope si tous ses vecteurs sont isotropes.*

   (ii) On dit que b *est anistrope si* 0 *est son unique vecteur isotrope.*

2. *On dit d'un sev* F *de* E *qu'il est totalement isotrope (resp. anisotrope) si la restriction de* b *à* F *l'est. Concrètement, "*F *totalement isotrope" signifie "*$x \in F \Rightarrow b(x,x) = 0$*", tandis que* F *anisotrope signifie "*$x \in F,\, x \neq 0 \Rightarrow b(x,x) \neq 0$*".*

Lemme 2.40 *Si* $2 \neq 0$*, alors il n'y a pas de fbs totalement isotrope autre que la forme nulle.*

Remarque 2.41 *L'anisotropie est liée au corps* K *: ex :* $x_1y_1 + x_2y_2$ *est anisotrope si* $K = \mathbb{R}$ *mais pas si* $K = \mathbb{C}$ *;* $x_1y_1 - 2x_2y_2$ *est anisotrope si* $K = \mathbb{R}$ *mais pas si* $K = \mathbb{Q}$*.*

Lemme 2.42 *Supposons* b *anisotrope, alors*

(i) b *est non dégénérée.*

(ii) La restriction de b *à tout sev est encore anisotrope.*

Preuve : Pour (i), constater que le cone isotrope contient le noyau.

Bien sûr, (i) ne possède pas de réciproque : par exemple $x_1y_2+x_2y_1$ est non dégénérée, bien que non anisotrope (dessiner son cône isotrope). Cependant :

Proposition 2.43 *Une fbs b est anisotrope si et seulement si sa restriction à tout sev F de E est non dégénérée.*

Preuve : Si b est anisotrope, il résulte du lemme précédent que sa restriction à n'importe quel F est anisotrope, et donc non dégénérée, *a fortiori*. Si b n'est pas anisotrope, il y a un $x \in E$ non nul vérifiant $b(x,x)=0$; mais alors b_F est non dégénérée (en fait, c'est la forme nulle !) pour $F =< x >$.

2.2.3 Orthogonalité et non dégénérescence

Comme auparavant, b désigne une fbs sur E.

Définition 2.44 *(i) On dit d'une décomposition de E en somme directe $E = E_1 \oplus E_2$ qu'elle est orthogonale si $E_1 \subset E_2^{\perp}$. On la note alors $E = E_1 \perp^b E_2$ (ou simplement $E = E_1 \perp E_2$).*

(ii) On dit de E_2 que c'est un supplémentaire orthogonal de E_1 si $E = E_1 \perp E_2$.

Remarque 2.45 *- Considérons une décomposition en somme orthogonale $E = F \oplus G$, ainsi que $\underline{f} = (f_1,\ldots,f_k)$, $\underline{g} = (g_1,\ldots,g_{n-k})$ des bases de F et G et $\underline{e} = (f_1,\ldots,f_k,g_1,\ldots,g_{n-k})$ celle de E qui s'en déduit. Alors $E = E_1 \perp E_2$ si et seulement si $mat(b,\underline{e})$ est de la forme $\begin{pmatrix} mat(b_{|F},\underline{f}) & 0 \\ 0 & mat(b_{|G},\underline{g}) \end{pmatrix}$.*

- Il arrive qu'un sev E_1 de E ne possède aucun supplémentaire orthogonal. C'est notamment le cas lorsque $E_1 =< x >$, si x est un vecteur isotrope non nul de b.

Proposition 2.46 *(i) $Ker\, b_{|F} = F \cap F^{\perp b}$.*

(ii) Sont équivalents :

- $b_{|F}$ est non dégénérée.
- $E = F \perp F^{\perp}$.
- $E = F \oplus F^{\perp}$.

Exercice 2.47 *Montrer que tout supplémentaire G de $F = Ker\, b$ est un supplémentaire orthogonal et que $b_{|G}$ est systématiquement non dégénérée.*

Proposition 2.48 *Si $E = E_1 \perp^b E_2$, alors*

(i) $Ker\, b = Ker\, b_{|E_1} \perp Ker\, b_{|E_2}$.

(ii) $rg\, b = rg\, b_{|E_1} + rg\, b_{|E_2}$.

(iii) $disc\, b = disc\, b_{|E_1} disc\, b_{|E_1}$.

Explication de (iii) : la classe de ab mod $K^{\times 2}$ ne dépend que de celle de a et de celle de b ; on convient de la noter $\overline{a}\overline{b}$.

Preuve de la proposition : Pour (i), il suffit de montrer que $Ker\, b \subset Ker\, b_{|E_1} + Ker\, b_{|E_2}$ ce qui est immédiat. (ii) s'en déduit par le théorème du rang. Pour (iii), on calcule le déterminant par blocs.

Remarque 2.49 *(i) et (ii) peuvent aussi se voir matriciellement.*

Corollaire 2.50 *Si $E = E_1 \perp^b E_2$, alors b est non dégénérée si et seulement si $b_{|E_1}$ et $b_{|E_2}$ le sont.*

Définition 2.51 *Une famille $\{e_1, \ldots, e_k\}$ est dite orthogonale si $i \neq j \Rightarrow b(e_i, e_j) = 0$. Une base $\underline{e}$ est dite orthogonale si sa famille sous jacente l'est.*

Remarque 2.52 *Soit $\underline{e}$ une base orthogonale de E. - $mat(b, \underline{e})$ est diagonale.*
- si $F =< e_1, \ldots, e_k >$ et $G =< e_1, \ldots, e_{n-k} >$, alors $E = F \perp^b G$.

Proposition 2.53 *Si b est une fbs sur E, alors il existe une base orthogonale.*

Preuve : On raisonne par récurrence sur le rang : si celui-ci est non nul, c'est que b est non nulle, donc non totalement isotrope. Choisir un vecteur x anisotrope et contempler la décomposition orthogonale $E =< x >\perp x^\perp$ qui en résulte donne le résultat.

2.3 Formes quadratiques

On suppose désormais que $2 \neq 0$ dans K.

2.3.1 Definition

Si q est une application $E \to K$, on note $b_q : E \times E \to K$ l'application définie par $b_q(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$. Si maintenant b est une application $E \times E \to K$, on note $q^b : E \to K$ l'application définie par $q^b(x) = b(x, x)$.

Définition 2.54 *Considérons une application $q : E \to K$. On dit que q est une forme quadratique si :*
- $\forall x \in E$, $\forall \lambda \in K$, $q(\lambda x) = \lambda^2 q(x)$.
- b_q est une fbs.

Si $FQ(E)$ et $FBS(E)$ désignent respectivement l'ensemble des formes quadratiques sur E et $FBS(E)$ celui des formes bilinéaires symétriques sur E, l'application $q \to b_q$ induit donc

$$FQ(E) \to FBS(E)$$

Proposition 2.55 *L'application ci-dessus est bijective, et son application réciproque est donnée par $b \mapsto q^b$.*

preuve : on vérifie simplement que $b_{q^b} = b$ et $q^{b_q} = q$.

2.3.2 Polynômes quadratiques

Définition 2.56 *Considérons deux n-uplets de variables* $X = (X_1, \ldots, X_n)$ *et* $Y = (Y_1, \ldots, Y_n)$*. - Un polynôme linéaire* $L(X)$ *est une expression du type* $L(X) = \sum a_i X_i$*.*

- Un polynôme bilinéaire symétrique $B(X, Y)$ *est une expression du type* $B(X, Y) = \sum_{i,j} b_{i,j} X_i Y_j$ *vérifiant* $b_{i,j} = b_{j,i}$*. On note* $PoLBS(n)$ *l'ensemble des tels polynômes.*

- Un polynôme quadratique $Q(X)$ *est une expression du type* $Q(X) = \sum c_i X_i^2 + \sum_{i<j} c_{i,j} X_i X_j$*. On note* $PoLQ(n)$ *l'ensemble de tels polynômes.*

Proposition 2.57 *- Si* $B(X, Y) = \sum_{i,j} b_{i,j} X_i Y_j \in PolB(n)$*, alors* $Q^B(X) := B(X, X) = \sum_i b_{i,i} X_i^2 + 2 \sum_{i<j} b_{i,j} X_i X_j$ *est dans* $PolQ(n)$*.*

- Si $Q(X) \in PolQ(n)$*, alors* $B_Q(X, Y) := \frac{1}{2}(q(X+Y) - q(X) - q(X)) = \sum_{i,j} b_{i,j} X_i Y_j$ *est dans* $PolBS(n)$*. Ici,* $b_{i,j} = \left| \begin{array}{ll} c_i & si\ i = j \\ \frac{1}{2} c_{i,j} & si\ i < j \\ \frac{1}{2} c_{j,i} & si\ j < i \end{array} \right.$

Les applications $B(X, Y) \mapsto Q^B(X)$ *et* $Q(X) \mapsto B_Q(X, Y)$ *sont réciproques, et réalisent donc une bijection*

$$PolQ(n) \leftrightarrow PolBS(n)$$

.

Preuve : il suffit de l'écrire.

2.3.3 Classification

Les différentes incarnations de la notion de fbs sont récapitulées par le diagramme suivant, dans lequel $MatS(n)$ désigne l'ensemble des matrices symétriques de taille n, et l'indice "base" indique que la bijection en question dépend du choix d'une base alors que l'indice "can" indique qu'il en est indépendant.

$$\begin{tikzcd}
FBS(E) \arrow[r, leftrightarrow, "\text{base}"] \arrow[d, leftrightarrow, "\text{can}"] & MatS(n) \arrow[r, leftrightarrow, "\text{can}"] & PolB(n) \arrow[d, leftrightarrow, "\text{can}"] \\
FQ(E) & & PolQ(n)
\end{tikzcd}$$

Exercice 2.58 *Faire le tour du diagramme, et écrire les preuves qui ne l'ont pas encore été.*

Proposition 2.59 *Fixons une base* $\underline{e}$ *de* E *(resp.* $\underline{e}'$ *de* E'*) et notons* $b, q, B, B(X, Y), Q(X)$ *(resp.* $b', q', B', B'(X, Y), Q'(X)$*) les* 5 *incarnations d'une forme bilinéaire sur* E'*.*

Soit $u : E \to E'$ *un isomorphisme,* $A = (a_{i,j}) = Mat(u, \underline{e}, \underline{e}')$*, et* $L_1(X) = \sum_j a_{1,j} X_i$*, ... ,* $L_1(X) = \sum_j a_{1,j} X_i$ *la famille libre de polynômes linéaires correspondante. Si* $x = \sum x_i e_i$ *et* $y = \sum y_i$*.*

Les assertions suivantes sont équivalentes :

(i) $b(x, y) = b'(u(x), u(y))$*.*

(ii) $q(x) = q'(u(x))$*.*

(iii) $B(x_1, \ldots, x_n, y_1, \ldots, y_n)$
$= B'(L_1(x_1, \ldots, x_n), \ldots, L_n(x_1, \ldots, x_n), L_1(y_1, \ldots, y_n), \ldots, L_n(y_1, \ldots, y_n))$

(iv) $Q(x_1,\dots,x_n)=Q'(L_1(x_1,\dots,x_n),\dots,L_n(x_1,\dots,x_n))$.

(v) $${}^t\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} B \begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} = {}^t\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} {}^tAB'A \begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}.$$

En pratique, on est souvent intéressé par le cas suivant : $E=E'$ et $u=id_E$; dans ce cas, A est l'inverse de la matrice de passage de $\underline{e}$ vers $\underline{e}'$ et (v) correspond à l'égalité $B'={}^tPBP$, avec $P=A^{-1}=Pass(\underline{e},\underline{e}')$. L'équivalence entre les points (iv) et (v) est le point de départ de la méthode de Gauss (cf TD) pour trouver une base orthogonale.

Définition 2.60 *(i) On dit d'une fbs b (resp. fq. q) sur E qu'elle est isomorphe à la fbs b' (resp. fq. q') sur E' s'il existe u inversible comme ci-dessus.*

(ii) On dit d'un polynôme bilinéaire symétrique $B(X,Y)$ (resp. quadratique $Q(X)$) qu'il est isomorphe à $B'(X,Y)$ s'il existe une famille libre de polynômes linéaires $L_1'(X),\dots,L_n'(X)$ comme ci-dessus.

Dans les quatre cas de cette définition, la relation "$*$ est isomorphe à $*'$ " est une relation d'équivalence. La proposition précédente montre que ces quatre relations d'équivalences sont compatibles entre elles, mais aussi avec la relation de congruence pour les matrices.

Théorème 2.61 *Soit $K=\mathbb{C}$. Si $B\in MatS(n)$, alors il existe un unique $r\le n$ tel que B soit congruente à la matrice $\begin{pmatrix} I_r & 0_{r,n-r}\\ 0_{n-r,r} & 0_{n-r}\end{pmatrix}$. Le nombre r est le rang de B.*

Preuve. L'unicité est claire (deux matrices congruentes ont même rang). Pour l'existence, on considère la fbs b sur $\mathbb{C}^n$ correspondant à B via la base canonique $\underline{e}$. On sait déjà qu'il existe une base orthogonale $\underline{e}'$ pour b. Après renumérotation et normalisation, on obtient une base $\underline{e}''$ dans laquelle la matrice de b est celle de l'énoncé.

Pour $K=\mathbb{R}$, il faut travailler un peu plus.

Définition 2.62 *Soit $K=\mathbb{R}$ et q une fq sur E.*

- On dit que $F\subset E$ est un sous-espace positif (ou que $q_{|F}$) positive) si $x\in F\Rightarrow$ $q(x)\ge 0$.

- On dit que F (ou $q_{|F}$) est défini(e) positif(/ve) si de plus F (ou $q_{|F}$) est anisotrope.

Proposition 2.63 *Soit n fixé. Pour $p\le r\le n$ et $q=r-p$, on note*

$$A_{p,q}=\begin{pmatrix} I_p & 0_{p,q} & 0_{p,n-r}\\ 0_{q,p} & -I_q & 0_{q,n-r}\\ 0_{n-r,p} & 0_{n-r,q} & 0_{n-r}\end{pmatrix}$$

Si $(p,q)\ne(p',q')$, alors $A_{p,q}$ et $A_{p',q'}$ ne sont pas congruentes.

Preuve : Si elle l'étaient, on pourrait trouver deux bases $\underline{e}$, $\underline{e}'$ de $E=\mathbb{R}^n$ par rapport auxquelles elles représenteraient respectivement la même fbs b sur E. Mais alors, on devrait avoir :

- $rg\,A_{p,q}=rg\,A_{p',q'}$, ie. $r=r'$.

- $< e_1, \ldots, e_p > \cap < e'_{p'+1}, \ldots, e'_n >= \{0\}$ car le premier sous-espace est défini positif pour b, alors que le second est négatif. Aussi, $p + (n - p') \leq n$

- $< e_{p+1}, \ldots, e_n > \cap < e'_1, \ldots, e'_{p'} >= \{0\}$ car le premier sous-espace est négatif alors que le second est défini positif. Aussi, $(n - p) + p' \leq n$.

Et finalement, $(p, r) = (p', r')$, ce qui termine la preuve.

Théorème 2.64 *Soit $K = \mathbb{R}$. Si $B \in MatS(n)$, alors il existe un unique couple (p, q) avec $p + q \leq n$ tel que B soit congruente à la matrice $A_{p,q}$. Le couple (p, q) s'appelle la signature de B et le nombre $r = p + q$ est le rang de B.*

Preuve : L'unicité relève de la proposition précédente. Pour l'existence, on procède comme pour $K = \mathbb{C}$, sauf au moment de normaliser : pour $k \leq r$, on pose $e''_k := \frac{e'_k}{\sqrt{|q_b(e'k)|}}$.

Remarque 2.65 *Soit b une fbs sur E alors b est positive (resp. définie positive) si et seulement si $q = 0$ (resp. $p = n$).*

3 Espaces euclidiens

3.1 La structure euclidienne

Définition 3.1 *Un espace euclidien est un espace vectoriel de dimension finie sur $\mathbb{R}$ muni d'une forme bilinéaire symétrique définie positive fixée, appelée produit scalaire, et notée $< -, - >: E \times E \to \mathbb{R}$.*

L'exemple standard d'espace euclidien est $\mathbb{R}^n$ muni du produit scalaire usuel $< x, y >= \sum x_i y_i$. Le théorème de classification du chapitre précédent montre qu'en fait tout espace euclidien y est (non canoniquement) isomorphe.

Remarque 3.2 *Par définition, le produit scalaire est non dégénéré et réalise donc une bijection $E \simeq E^*$, $x \mapsto < x, - >$.*

On fixe désormais un espace euclidien $(E, < -, - >)$.

Proposition 3.3 *Pour $x \in E$, notons $||x|| = \sqrt{< x, x >}$. L'application $|| - || : E \to [0, +\infty[$ ainsi définie est une norme, ie. vérifie les propriétés suivantes :*

- $||x|| = 0 \Leftrightarrow x = 0$.

- $||\lambda x|| = |\lambda| \, ||x||$ pour tout $\lambda \in \mathbb{R}$.

- (inégalité triangulaire) $||x + y|| \leq ||x|| + ||y||$.

On dit de $(E, || - ||)$ que c'est un espace normé.

Exercice 3.4 *Montrer que dans un espace normé, on a toujours $| \, ||x|| - ||y|| \, | \leq ||x - y||$.*

Pour prouver l'inégalité triangulaire, on a besoin d'un résultat préliminaire.

Lemme 3.5 *(Cauchy-Schwartz) Si $x, y \in E$, alors $| < x, y > | \leq ||x|| \, ||y||$ et l'égalité a lieu si et seulement si x et y sont colinéaires.*

Preuve du lemme : Le cas non trivial est celui où x et y sont non colinéaires. Dans celui-ci, observons la fonction polynômiale de degré 2 suivante : $\lambda \mapsto ||x+\lambda y||^2$. Comme elle ne s'annule pas, le discriminant doit être strictement positif et cela donne le résultat sans valeur absolue lorsqu'on l'explicite. Les valeurs absolues viennent en remplaçant au besoin x par $-x$.

Preuve de l'inégalité triangulaire : $||x+y||^2 = ||x||^2 + 2 < x, y > +||y||^2 \leq ||x||^2 + 2||x||\,||y|| + ||y||^2 = (||x|| + ||y||)^2$.

Remarque 3.6 *(i) Si $||-||$ est une norme, alors l'application $d(-,-) : E \times E \to]0, +\infty[$ est une distance, ie. vérifie les propriétés suivantes :*

- $d(x, y) = 0 \Leftrightarrow x = y$.

- $d(x, y) = d(y, x)$.

- $d(x, z) \leq d(x, y) + d(y, z)$.

On dit alors que (E, d) est un espace métrique.

(ii) Si $< -, - >$ est un produit scalaire, alors l'inégalité de Cauchy-Schwartz montre que la quantité $\left(\frac{<x,y>}{||x||\,||y||}\right)$ est toujours ≤ 1. On définit alors l'angle non orienté formé par x et y de la manière suivante : $angle(x, y) = \arccos\left(\frac{<x,y>}{||x||\,||y||}\right)$.

Définition 3.7 *Une famille de vecteurs est dite orthonormée si elle est orthogonale et si ses vecteurs ont tous norme 1.*

Exercice 3.8 *Toute famille orthonormée est libre.*

Récapitulons en une proposition quelques reformulations possibles de cette définition.

Proposition 3.9 *Si $\underline{e}$ est une base de E, les assertions suivantes sont équivalentes :*

(i) $\underline{e}$ est orthonormée.

(ii) $mat(< -, - >, \underline{e}) = I$.

(iii) $\forall i$, $< e_i, - >= e_i^*$, où $\underline{e}^*$ désigne la base duale de $\underline{e}$.

(iv) $\forall x \in E$, $Coord(x, \underline{e}) = \begin{pmatrix} < e_1, x > \\ \vdots \\ < e_n, x > \end{pmatrix}$

D'après le chapitre précédent, on sait déjà qu'un espace euclidien possède toujours des bases orthonormées. Pour en fabriquer, on dispose de l'algorithme de Gram-Schmidt, qui consiste à transformer une base donnée $\underline{e} = (e_1, \ldots, e_n)$ en une base orthonormée $\underline{f} = (f_1, \ldots, f_n)$. Ceci en n étapes, dont voici la k-ième :

Proposition 3.10 *Supposons que $\underline{(}f_1, \ldots, f_{k-1}, e_k, \ldots, e_n)$ soit une base de E, et que la famille $\{f_1, \ldots, f_{k-1}\}$ soit orthonormée.*

Le vecteur $f_k' = e_k - \sum_{i=1}^{k-1} < e_k, f_i > f_i$ est nécessairement non nul. Si l'on note $f_k = \frac{f_k'}{||f_k'||}$, alors la famille $\{f_1, \ldots, f_k\}$ est orthonormée. De plus, elle engendre le même sev que $\{f_1, \ldots, f_{k-1}, e_k\}$ si bien que $(f_1, \ldots, f_k, e_{k+1}, \ldots, e_n)$ est aussi une base de E.

Preuve : La non nullité de f_k résulte de la liberté de la famille $\{f_1, \ldots, f_{k-1}, e_k\}$ et l'égalité de sev $< f_1, \ldots, f_{k-1}, e_k >=< f_1, \ldots, f_k >$ est évidente. Le point essentiel consiste donc à vérifier que la famille $\{f_1, \ldots, f_{k-1}, f'_k\}$ est orthogonale, ce qui est immédiat.

On rappelle que le produit scalaire est anisotrope, si bien que tout sev F possède un unique supplémentaire orthogonal, qui est $F^\perp$.

Proposition 3.11 *Soit F un sev de E.*

(i) Si $x \in E$, alors il existe un unique $y \in F$ dont la distance à x soit minimale, ie vérifiant $z \in F \Rightarrow ||x - z|| \geq ||x - y||$. On le note $y = p_F(x)$.

(ii) L'application $p_F : x \mapsto p_F(x)$ est linéaire et c'est une projection (ie. vérifie $p_F^2 = p_F$). On l'appelle la projection orthogonale sur F.

Preuve : Si $x = x_1 + x_2$, $x_1 \in F$, $x_2 \in F^\perp$ est la décomposition de x correspondant à la somme orthogonale $E = F \perp F^\perp$ et si $z \in F$, alors $||x - z||^2 = ||x_1 - z||^2 + ||x_2||^2 > ||x_2||^2 = ||x - x_1||^2$, sauf si $z = x_1$. La fonction $z \mapsto ||x - z||$ atteint donc un minimum strict (donc unique) en $y = x_1$ ce qui prouve (i). Le point (ii) est clair.

Si $(e_1, \ldots, e_k)$ est une base de F et $(e_{k+1}, \ldots, e_n)$ une base de $F^\perp$, alors $mat(p_F, \underline{e}) = \begin{pmatrix} I_k & 0_{k,n-k} \\ 0_{n-k,k} & 0_k \end{pmatrix}$. L'application linéaire $s_F := 2p_F - id_E$ (dont la matrice par rapport à la même base est donc $\begin{pmatrix} I_k & 0_{k,n-k} \\ 0_{n-k,k} & -I_k \end{pmatrix}$) s'appelle la symétrie orthogonale par rapport à F.

Remarque 3.12 *Si $(e_1, \ldots, e_k)$ est une base orthogonale de F et $x \in E$, alors $p_F(x) = \sum_{i=1}^k < x, e_i > e_i$.*

3.2 Le groupe orthogonal

$(E, < -, - >)$ désigne désormais un espace euclidien fixé.

3.2.1 Endomorphismes orthogonaux

Définition 3.13 *Un endomorphisme u de E est dit orthogonal s'il conserve le produit scalaire, ie. si $< u(x), u(y) >=< x, y >$ pour tous $x, y \in E$.*

Proposition 3.14 *u est othogonal si et seulement s'il conserve la norme, ie. si $||u(x)|| = ||x||$ pour tout $x \in E$.*

Preuve : La coïncidence des fbs $(x, y) \mapsto < (u)x, u(y) >$ et $(x, y) \mapsto < x, y >$ équivaut à celle des formes quadratiques $x \mapsto ||u(x)||^2$ et $x \mapsto ||x||^2$.

Remarque 3.15 *Si u est orthogonal, alors u est inversible et u^{-1} est automatiquement orthogonal.*

Exemple 3.16 *Si F est un sev strict de E, alors s_F (la symétrie orthogonale par rapport à F) est un endomorphisme orthogonal de E. Ce n'est bien sûr pas le cas de p_F (la projection orthogonale par rapport à F).*

Proposition 3.17 *Soit u un endomorphisme de E et $\underline{e}$ une bon fixée de E. Si l'on note $e'_i = u(e_i)$, $i = 1, \ldots, n$, alors les assertions suivantes sont équivalentes :*

(i) u est orthogonal.

(ii) $\underline{e}'$ est une base de E et $P := Pass(\underline{e}, \underline{e}')$ vérifie $P^{-1} = {}^tP$.

(iii) u est inversible et $A := Mat(u, \underline{e})$ vérifie $A^{-1} = {}^tA$.

(iv) $\underline{e}'$ est une bon de E.

Preuve : Il faut commencer par remarquer que si u est orthogonal, alors $\underline{e}'$ est une base de E puisque u est inversible. Les équivalences de l'énoncé résultent alors des égalités matricielles suivantes : $A = P$ et $Mat(< -, - >, \underline{e}') = Mat(< u(-), u(-) >, \underline{e}) = {}^tPP$.

Définition 3.18 *On dit d'une matrice $A \in M_n(\mathbb{R})$ qu'elle est orthogonale si ${}^tAA = I$.*

Corollaire 3.19 *Si u est orthogonal, alors $\det u = 1$.*

Exercice 3.20 *Trouver une base (non orthonormée !) de $\mathbb{R}^2$ dans laquelle la matrice de la symétrie orthogonale par rapport à $< (1, 0) >$ n'est pas orthogonale.*

Définition 3.21 *On adopte les notations suivantes :*
- *$O(E) \subset GL(E)$ désigne l'ensemble des endomorphismes orthogonaux de E.*
- *$SO(E) \subset O(E)$ désigne l'ensemble de ceux qui sont en plus de déterminant 1.*
- *$O_n(\mathbb{R}) \subset GL_n(R)$ désigne l'ensemble des matrices orthogonales de taille n.*
- *$SO_n(\mathbb{R}) \subset O_n(\mathbb{R})$ désigne l'ensemble de ceux qui sont en plus de déterminant 1.*

Les deux premiers (resp. derniers) sont des sous-groupes de $GL(E)$ (resp. $GL_n(\mathbb{R})$). Le choix d'une bon de E induit trois isomorphismes de groupes compatibles

$$GL(E) \sim GL_n(\mathbb{R}) \qquad O(E) \sim O_n(\mathbb{R}) \qquad SO(E) \sim SO_n(\mathbb{R})$$

3.2.2 Orientation et produit vectoriel dans $E = \mathbb{R}^n$

Dans ce paragraphe, $(E, < -, - >)$ désigne $\mathbb{R}^n$ muni de sa structure euclidienne usuelle. Rappelons que l'on dispose d'une application n-linéaire canonique $det : E^n :\rightarrow \mathbb{R}$, caractérisée par les propriétés suivantes :

- soit $\underline{e} = (e_1, \ldots, e_n)$ la base canonique de E, alors $det(e_1, \ldots, e_n) = 1$.

- soit $(x_1, \ldots, x_n)$ un n-uplet quelconque de E, alors $det(x_1, \ldots, x_n) = 0$ ssi la famille de vecteurs $\{x_1, \ldots, x_n\}$ est liée.

Si $P = (p_{i,j})$ et $x_j = \sum_{i=1}^n p_{i,j} e_i$ alors $det(x_1, \ldots, x_n)$ est aussi noté $det(P)$. L'application $det : M_n(\mathbb{R}) \rightarrow \mathbb{R}$ ainsi définie est multiplicative.

Définition 3.22 *Soit $\underline{e}$ la base canonique de $E := \mathbb{R}^n$. On dit d'une base $\underline{f}$ de E qu'elle est directe (resp. indirecte) si la matrice $P = Pass(\underline{e}, \underline{f})$ a un déterminant positif (resp. négatif).*

Remarque 3.23 *Echanger deux vecteurs d'une base ou en multiplier un par un scalaire négatif transforme une base positive en une base négative et réciproquement.*

Définition 3.24 *Si $(x_1,\ldots,x_{n-1})$ est un $(n-1)$-uplet de vecteurs de $\mathbb{R}^n$, on note $x_1 \wedge \ldots \wedge x_{n-1}$ l'unique vecteur vérifiant $< x_1 \wedge \ldots \wedge x_{n-1}, y >= det(x_1,\ldots,x_{n-1},y)$ pour tout $y \in \mathbb{R}^n$.*

NB : pour donner un sens à la définition précédente, il faut remarquer que l'application $det(x_1,\ldots,x_{n-1},-)$ est une forme linéaire, donc de la forme $< z, - >$ pour un unique $z \in \mathbb{R}^n$.

Proposition 3.25 *Le produit vectoriel $E^{n-1} \to E$, $(x_1,\ldots,x_{n-1}) \mapsto x_1 \wedge \ldots \wedge x_{n-1}$ est une application $(n-1)$-linéaire et vérifie la propriété suivante : $x_1 \wedge \ldots \wedge x_{n-1} = 0$ si et seulement si la famille $\{x_1,\ldots,x_n\}$ est liée.*

Proposition 3.26 *Si $x_j = \begin{pmatrix} x_{1,j} \\ \vdots \\ x_{n,j} \end{pmatrix}$ et si M_i désigne la matrice obtenue en effaceant la ième ligne de $\begin{pmatrix} x_{1,1} & \ldots & x_{1,n-1} \\ \vdots & & \vdots \\ x_{n,1} & \ldots & x_{n,n-1} \end{pmatrix}$ alors $x_1 \wedge \ldots \wedge x_{n-1} = \begin{pmatrix} (-1)^{n+1}det(M_1) \\ \vdots \\ (-1)^{n+n}det(M_n) \end{pmatrix}$.*

Preuve : Le $i$ème coefficient du vecteur $x_1 \wedge \ldots \wedge x_{n-1}$ est $< x_1 \wedge \ldots \wedge x_{n-1}, e_i >= det(x_1,\ldots,x_{n-1},e_n)$. D'où la formule de l'énoncé en développant la déterminant matriciel correspondant par rapport à la dernière colonne.

Remarque 3.27 *Soit $\underline{f} = (f_1,\ldots,f_n)$ une bon de E. En calculant $< f_1 \wedge \ldots \wedge f_{n-1}, f_i >$, on voit que $f_1 \wedge \ldots \wedge f_{n-1} = \pm f_n$, suivant que $\underline{f}$ est directe ou non.*

3.2.3 Description de $O_n(\mathbb{R})$

- $O^+(\mathbb{R}^2)$ (rotations dans le plan) :

Proposition 3.28 *Pour $\theta \in \mathbb{R}$, notons $R_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$. Cette famille de matrices vérifie les propriétés suivantes :*
- $R_\theta \in SO_2(\mathbb{R})$.
- $R_{\theta+\theta'} = R_\theta R_{\theta'}$.

Remarque 3.29 $R_\theta^{-1} = R_{-\theta}$.

Proposition 3.30 *Si $\underline{e} = (e_1, e_2)$ et $\underline{f} = (f_1, f_2)$ désignent respectivement la base canonique et une bon de directe de $\mathbb{R}^2$, alors il existe un unique $\theta \in [0, 2\pi[$ tel que $R_\theta = Pass(\underline{e}, \underline{f})$.*

Preuve : Il y a un unique θ tel que $f_1 = (\cos\theta, \sin\theta)$. Le vecteur $(-\sin\theta, \cos\theta)$ est alors l'unique vecteur complétant f_1 en une bon directe de $\mathbb{R}^2$: c'est f_2.

Corollaire 3.31 *(i) Si $u \in SO(\mathbb{R}^2)$, alors $\exists!\theta \in [0, 2\pi[$, $mat(u, \underline{e}) = R_\theta$. On note $u = \rho_\theta$.*

(ii) $SO_2(\mathbb{R}) = \{R_\theta,\, \theta \in [0, 2\pi[\}$.

Exercice 3.32 *Soit $\underline{f}$ une bon quelconque de $E = \mathbb{R}^2$. Montrer que $mat(\rho_\theta, \underline{f}) = R_\theta$ ou $R_{-\theta}$, suivant que $\underline{f}$ est directe ou non.*

Exercice 3.33 *Pour tout $x \in \mathbb{R}^2$, $< x, \rho_\theta(x) >= \theta$.*

- $O^-(\mathbb{R}^2)$ (symétries dans le plan) :

Définition 3.34 *Pour x non nul dans $\mathbb{R}^2$, on note s_x la symétrie orthogonale par rapport à $< x >$.*

Remarque 3.35 *Si $\underline{e} = (e_1, e_2)$ est une bon de E avec $x \in < e_1 >$, alors*

$$Mat(s_x, \underline{e}) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Lemme 3.36 *s_x est l'unique endomorphisme orthogonal indirect qui laisse x fixe.*

Preuve : Examiner la matrice de u dans une bon comme ci-dessus.

Lemme 3.37 $s_{e_1}\rho_\theta = s_{\rho_{\frac{-\theta}{2}} e_1}$.

Il suffit de vérifier que $\rho_{\frac{-\theta}{2}} e_1$ est laissé fixe par $s_{e_1}\rho_\theta$, ce qui est clair : $s_{e_1}\rho_\theta\rho_{\frac{-\theta}{2}} e_1 = s_{e_1}\rho_{\frac{\theta}{2}} e_1 = s_{e_1}(\cos\frac{\theta}{2}, \sin\frac{\theta}{2}) = (\cos\frac{\theta}{2}, -\sin\frac{\theta}{2}) = \rho_{\frac{-\theta}{2}} e_1$.

Proposition 3.38 *Tout $u \in O^-(\mathbb{R}^2)$ est de la forme s_x. De plus, on peut toujours choisir x de la forme $\rho_{\frac{-\theta}{2}}(e_1)$, auquel cas*

$$Mat(s_x, \underline{e}) = \begin{pmatrix} \cos\theta & -\sin\theta \\ -\sin\theta & -\cos\theta \end{pmatrix}$$

Preuve : Comme $s_{e_1}u \in O^+(\mathbb{R}^2)$, il est de la forme ρ_θ. Mais alors $u = s_{e_1}\rho_\theta = \rho_{\frac{-\theta}{2x}}$, puisque $s_{e_1}^{-1} = s_{e_1}$.

Exercice 3.39 *(relation dihédrale) Montrer que $s_x\rho_\theta s_x = \rho_\theta^{-1}$.*

- $O(\mathbb{R}^n)$:

Commençons par quelques rappels généraux.

- Dans l'anneau $K[X]$, tout polynôme possède une décomposition en produit de puissances de polynômes irréductibles. Si $K = \mathbb{C}$, les polynômes irréductibles sont tous de degré ≤ 1. Si $K = \mathbb{R}$, ils sont tous de degré ≤ 2.

- Si E est un ev de dim finie sur K et $u \in End_K(E)$, le polynôme irréductible et le polynôme minimal de u possèdent les mêmes facteurs irréductibles. Si $P(X)$ est l'un d'entre eux, alors E possède un sev F de dimension $d = deg\, P(X)$ avec les propriétés suivantes : F est stable par u et l'endomorphisme $P(u)$ vaut 0 sur F.

Lemme 3.40 *Soit u orth. Si F est stable par u, alors $F^\perp$ aussi.*

Lemme 3.41 *les vp réelles d'un endom orth sont* ± 1.

Exercice 3.42 *En utilisant la conjugaison complexe, montrer qu'en fait, toutes les valeurs propres d'une matrice orthogonale sont de module* 1.

Proposition 3.43 *Soit* u *orth, alors il existe une bon de* E *dans laquelle la matrice de* u *est la matrice par bloc suivante*

$$\begin{pmatrix} R_{\theta_1} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ & \ddots & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & R_{\theta_k} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Preuve : Par récurrence sur la dimension.

- $O^+(\mathbb{R}^3)$ (Rotations dans l'espace)

Un endomorphisme orthogonal positif possède une description géométrique, qu'on explique maintenant.

Lemme 3.44 *Si* $u \in O^+(\mathbb{R}^3)$, *alors* 1 *est valeur propre de* u.

Preuve : le produit des valeurs propres doit valoir 1. Comme elles sont toutes de module 1, on conclut facilement en examinant les cas. Autre possibilité : calculer directement le déterminant de la matrice donné par le théorème de réduction.

Corollaire 3.45 *Si* $u \in O^+(\mathbb{R}^3)$, *alors il existe une bon directe de* $\underline{f} = (f_1, f_2, f_3)$ *de* $\mathbb{R}^3$ *dans laquelle* u *a pour matrice*

$$\begin{pmatrix} 1 & 0 \\ 0 & R_\theta \end{pmatrix}$$

Preuve : l'existence d'une bon est donnée par le théorème général. On en trouve une directe en changeant éventuellement le signe d'un des vecteurs.

Proposition 3.46 *Soient* u *et* $\underline{f}$ *comme dans la proposition précédente. Si* $\underline{g}$ *est une autre bon. directe telle que* $g_1 = f_1$, *alors* $Mat(u, \underline{g}) = Mat(u, \underline{f})$.

Preuve : Comme $\underline{f}$ et $\underline{g}$ sont deux bon directe, $Pass(\underline{f}, \underline{g})$ est nécessairement de la forme $\begin{pmatrix} 1 & 0 \\ 0 & R_{\theta'} \end{pmatrix}$. D'où le résulat, en écrivant la formule de changement de base.

Le couple (f_1, θ) caractérise donc l'endomorphisme u. On dit que u est la rotation d'angle θ, d'axe dirigé par f_1.

Exercice 3.47 *Soit* u *(resp.* u'*) la rotation d'angle* θ *(resp.* θ'*), d'axe dirigé par* f_1 *(resp.* f_1'*). Montrer que* $u = u'$ *si et seulement si* $e_1 = e_1'$ *et* $\theta = \theta' mod\ 2\pi\mathbb{Z}$ *ou* $e_1 = -e_1'$ *et* $\theta = -\theta' mod\ 2\pi\mathbb{Z}$.

3.3 Le groupe symétrique

Comme dans le paragraphe précédent, $(E, < -, - >)$ désigne une espace euclidien fixé.

Définition 3.48 *Un endomorphisme u de E est dit symétrique si pour tout $x, y, \in E$, $< u(x), y >=< x, u(y) >$.*

Proposition 3.49 *Soit $\underline{e}$ une bon de E. L'endomorphisme u est symétrique si et seulement si $Mat(u, \underline{e})$ l'est.*

Preuve : u est symétrique si et seulement si les formes bilinéaires $(x, y) \mapsto < u(x), y >$ et $< x, u(y) >$ coincident. D'où le résultat en écrivant la matrice de ces dernières par rapport à la base $\underline{e}$.

Proposition 3.50 *Soit u un endomorphisme symétrique. Si $F \subset E$ est un sous-espace stable par u, alors $F^\perp$ aussi.*

Proposition 3.51 *Soit $A \in M_n(\mathbb{R})$ une matrice réelle et notons $\chi(X) \in K[X]$ son polynôme caractéristique. Si A est symétrique, alors les racines complexes de χ sont toutes réelles.*

Preuve : Si λ est une racine complexe de χ, alors il existe $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{C}^n$ non nul tel que $AX = \lambda X$. Mais alors on trouve que $\lambda \sum |x_i|^2 = {}^t(AX)\overline{X} = {}^tX\overline{AX} = \overline{\lambda} \sum |x_i|^2$, ce si bien que $\lambda = \overline{\lambda}$.

Théorème 3.52 *Si u est un endomorphisme symétrique, alors u est diagonalisable. De plus, E possède une base orthonormée de vecteurs propres (pour u).*

Preuve : Par récurrence sur la dimension, à l'aide des deux propositions précédentes.

Corollaire 3.53 *Si A est une matrice symétrique, alors il existe P orthogonale telle que ${}^tPAP = P^{-1}AP$ soit diagonale.*

Preuve : On applique le théorème précédent à l'espace $\mathbb{R}^n$ muni de sa structure euclidienne canonique et à l'endomorphisme u dont la matrice vaut A dans la base base canonique.

Corollaire 3.54 *Soient b_1, b_2 deux formes bilinéaires symétriques sur un espace vectoriel F. Si b_1 est définie positive, alors E possède une base qui soit simultanément orthogonale pour b_1 et b_2.*

Preuve : On applique le corollaire précédent à la matrice $A = mat(b_2, \underline{f})$ où $\underline{f}$ est une base orthonormée pour b_1.

Exercice 3.55 *Déduire directement le corollaire ci-dessus du théorème, en l'appliquant à l'espace euclidien (F, b_1) et à l'endomorphisme $u = (b_{1*})^{-1}b_{2*}$, dont on vérifiera qu'il est symétrique (pour b_1).*

Corollaire 3.56 *Soit $\underline{e}$ une base orthogonale de E, u un endomorphisme symétrique et b la forme bilinéaire symétrique sur E telle que $A = Mat(u, \underline{e}) = Mat(b, \underline{e})$. Sont équivalents :*
(i) b est définie positive.
(ii) les valeurs propres de u sont toutes strictement positives.
Par abus de langage on parle d'endomorphisme symétrique défini positif.

Preuve : Soit $P = Pass(\underline{e}, \underline{f})$ où $\underline{f}$ est une bon de vp pour u. Les valeurs propres de u ainsi que la signature de b se lisent sur la matrice $Mat(u, \underline{f}) = P^{-1}AP = {}^tPAP = Mat(b, \underline{f})$.

3.4 La décomposition polaire

Commençons par de nouveaux rappels d'algèbre linéaire. Pour ceux-ci, E désigne un espace vectoriel de dimension finie sur un corps K quelconque.

- Un endomorphisme u de E est diagonalisable si et seulement si son polynôme minimal - notons-le $min_u(X)$ - est scindé dans K, ie. si toutes ses racines sont simples et vivent dans K.

- Soit u un endomorphisme diagonalisable de E. Si $F \subset E$ est un sous-espace stable par u, alors $u_{|F}$ est diagonalisable puisque $min_{u_F}(X) \mid min_u(X)$.

Proposition 3.57 *Si u et v sont deux endomorphismes diagonalisables d'un même espace vectoriel E et si $u \circ v = v \circ u$, alors E possède une base dont les vecteurs sont propres pour u et v simultanément.*

Preuve : Considérons la décomposition de E suivant les valeurs propres de u, disons $E = \oplus E_{u,\lambda_i}$ avec $\lambda_1, \ldots, \lambda_k$ deux à deux distinctes. Puisque u et v commutent, on voit tout de suite que les E_{u,λ_i} sont stables par v. D'après les rappels ci-dessus, chaque restriction $v_{|E_{u,\lambda_i}}$ est diagonalisable. Si pour chaque i, $(e_{i,1}, \ldots, e_{i,l_i})$ est une base de E_{u,λ_i} diagonalisant la restriction de v, alors $(e_{1,1}, \ldots, e_{1,l_1}, \ldots, e_{k,1}, \ldots, e_{k,l_k})$ est une base de E dont les vecteurs sont propres pour u et v simultanément.

Proposition 3.58 *Soit u un endomorphisme symétrique défini positif, alors il existe un unique endomorphisme symétrique défini positif w tel que $u = w^2$.*

Preuve : Existence : Soit $\underline{e}$ un bon de vecteurs propres. Comme la matrice $U = Mat(u, \underline{e})$ est diagonale à termes positifs, il existe W tel que $W^2 = U$. Mais alors l'endomorphisme w tel que $Mat(w, \underline{e}) = W$ est symétrique (car W l'est et $\underline{e}$ est orthonormée) défini positif. On remarque que u et w possèdent exactement les mêmes sous-espaces propres (car $\lambda_i \neq \lambda_j \Leftrightarrow \sqrt{\lambda_i} \neq \sqrt{\lambda_j}$). En particulier, la matrice de u dans une base donnée est diagonale si et seulement si celle de w l'est.

Unicité : Soit v un endomorphisme symétrique défini positif tel que $v^2 = u$. Alors v est diagonalisable, et commute avec u (en effet $v \circ u = v \circ v^2 = v^3 = v^2 \circ v = u \circ v$). Il existe donc une base $\underline{f}$ telle que $V' = Mat(v, \underline{f})$ et $U' = Mat(u, \underline{f})$ soient diagonales. D'après la remarque précédente, $W' = Mat(w, \underline{f})$ est diagonale aussi. Comme W' et V' sont diagonales à terme positifs et de carrés égaux, c'est qu'en fait $V' = W'$, ie. $v = w$.

Corollaire 3.59 *Si A est une matrice symétrique définie positive, alors il existe une unique matrice symétrique définie positive P vérifiant $P^2 = A$. On la note $P = \sqrt{A}$.*

Corollaire 3.60 *Soit $A \in M_n(\mathbb{R})$, alors A est symétrique définie positive si et seulement s'il existe $B \in GL_n(\mathbb{R})$ telle que ${}^tBB = A$.*

Preuve : Si A est symétrique définie positive, on peut toujours prendre pour P la matrice S donnée par le corollaire précédent. Reste donc à remarquer que pour $B \in GL_n(\mathbb{R})$, la matrice ${}^tBB$ est toujours définie positive ; en effet, c'est la matrice du produit scalaire canonique de $\mathbb{R}^n$ par rapport à la base donnée par les vecteurs collonnes de B.

Remarque 3.61 *Il n'y bien sûr pas unicité, puisque si O est orthogonale, on a ${}^t(OB)OB = {}^tBB$.*

Théorème 3.62 *Pour tout $A \in GL_n(\mathbb{R})$, il existe un unique couple (P, O) vérifiant $A = PO$ avec P symétrique définie positive et O orthogonale.*

Preuve : Existence : Soit P la matrice symétrique définie positive $\sqrt{A^tA}$ et notons $O = P^{-1}A$. On a alors $O^tO = P^{-1}A^tA^tP^{-1} = P^{-1}P^2P^{-1} = I$, si bien que O est orthogonale.

Unicité : Si $A = PO = P'O'$, alors $A^tA = P^2 = P'^2$, si bien que $P = P' = \sqrt{A^tA}$, puisque P et P' sont symétriques définies positives. Du coup, $O = P^{-1}A = P'^{-1}A = O'$.