Notes du cours de géométrie

Daniele Faenzi

17 septembre 2017

TABLE DES MATIÈRES

CHAPITRE 1

GÉOMÉTRIE AFFINE

Ce chapitre est fortement inspiré de [**Aud06**].

1.I. Espaces affines

Fixons un corps $\mathbb{K}$.

1.I.A. Espaces affines et direction. —

Définition 1.I.1. — Un *espace affine* $\mathcal{E}$ est un ensemble sur lequel un espace vectoriel E, appelé *direction* de $\mathcal{E}$ opère simplement transitivement. Si $\dim(E) = n$, on note $\dim(\mathcal{E}) = n$. On note $\vec{v}$ les éléments de E, y compris l'élément neutre, $\vec{0}$. Parfois on écrit $\vec{\mathcal{E}}$ pour la direction E de $\mathcal{E}$.

On note l'opération par une somme, étant donné $P \in \mathcal{E}$ et $\vec{v} \in E$, $P + \vec{v}$ le point de $\mathcal{E}$ résultat de $\vec{v}$ qui opère sur P.

Soit $P, Q \in \mathcal{E}$. Alors il existe un et un seul vecteur de E qui amène P sur Q, on le note $\overrightarrow{PQ}$. On appelle $\overrightarrow{PQ}$ le *vecteur libre* de P à Q. Bien sûr $P + \overrightarrow{PQ} = Q$ et $\overrightarrow{PQ} = -\overrightarrow{QP}$, $\overrightarrow{PP} = \vec{0}$. Les axiomes d'opération de groupe disent que, pour tout $\vec{u}, \vec{v} \in E$ et $P \in \mathcal{E}$:

$$P + (\vec{u} + \vec{v}) = (P + \vec{u}) + \vec{v},$$

où bien entendu tous les signes + n'ont pas la même signification !

L'application $\mathcal{E} \times \mathcal{E} \to E$ qui à (P, Q) associe $\overrightarrow{PQ}$ est bijective à P fixé, ou à Q fixé.

Exemple 1.I.2. — L'exemple de base est $\mathcal{E} = E$. L'opération est l'opération de somme si $u \in E$ et $v \in E$, alors $u + v$ est la somme de u et v dans E. On appelle $\mathcal{E}$ la *structure canonique d'espace affine*, en faisant opérer E sur lui-même par addition. On a alors, si $\overrightarrow{uv} = v - u$.

Remarque 1.I.3. — On a la *règle du parallélogramme*, qui affirme que, si A, A', B, B' sont des points d'un espace affine $\mathcal{E}$, alors $\overrightarrow{AA'} = \overrightarrow{BB'}$ si et seulement si $\overrightarrow{AB} = \overrightarrow{A'B'}$.

Démonstration. — On a $\overrightarrow{AB'} = \overrightarrow{AA'} + \overrightarrow{A'B'} = \overrightarrow{AB} + \overrightarrow{BB'}$. Ainsi, $\overrightarrow{AA'} = \overrightarrow{BB'}$ implique $\overrightarrow{AB} = \overrightarrow{A'B'}$, et réciproquement. □

Définition 1.I.4. — *Vectorialiser* un espace affine $\mathcal{E}$ de direction E en un point $O \in \mathcal{E}$ consiste à considérer la bijection $\Theta_O : \mathcal{E} \to E$ qui envoie P en $\overrightarrow{OP}$.

On voit que $\mathcal{E}$, vectorialisé en O, possède une structure de $\mathbb{K}$-espace vectoriel, avec O, identifié à $\overrightarrow{OO} = \vec{0}$ comme origine.

Exercice 1.I.5. — Si on considère la structure canonique d'espace affine sur un espace vectoriel E, et $u \in E$, alors pour $w \in E$ on a $\Theta_u(w) = \{w - u \mid w \in E\}$.

1.I.B. Sous espaces affines. —

1.I.B.1. Sous espaces affines et vectoriels. —

Définition 1.I.6. — Une partie $\mathcal{F}$ d'un espace affine $\mathcal{E}$ est un *sous espace affine* s'il existe $P \in \mathcal{F}$ tel que $\Theta_P(\mathcal{F})$ est un sous espace vectoriel de E.

On pourra remarquer que, pour tout $P, Q \in \mathcal{F}$, on a :

$$\Theta_Q(\mathcal{F}) = \{\overrightarrow{QM} \mid M \in \mathcal{F}\} = \overrightarrow{QP} + \{\overrightarrow{PM} \mid M \in \mathcal{F}\} = \overrightarrow{QP} + \Theta_P(\mathcal{F}).$$

Or, si $\Theta_P(\mathcal{F})$ est un sous espace vectoriel de E, comme $\overrightarrow{QP} = -\overrightarrow{PQ}$ appartient à $\Theta_P(\mathcal{F})$: on trouve alors $\Theta_Q(\mathcal{F}) = \Theta_P(\mathcal{F})$. Ainsi, pour vérifier si $\mathcal{F}$ est un sous espace affine, on peut choisir n'importe quel point P est vérifier si $\Theta_P(\mathcal{F})$ est un sous espace vectoriel de E.

Exemple 1.I.7. — On se donne un système linéaire dans $\mathbb{K}^n$ de la forme :

$$\begin{cases} a_{1,1}x_1 + \cdots + a_{1,n}x_n = b_1 \\ \vdots \\ a_{m,1}x_1 + \cdots + a_{m,n}x_n = b_m \end{cases}$$

Les solutions $x = (x_1, \ldots, x_n)$ du système sont de la forme $x = x' + y$ où x' est une solution fixée du système de départ et $y = (y_1, \ldots, y_n)$ est solution du système homogène :

$$\begin{cases} a_{1,1}y_1 + \cdots + a_{1,n}y_n = 0 \\ \vdots \\ a_{m,1}y_1 + \cdots + a_{m,n}y_n = 0 \end{cases}$$

Il s'agit d'un sous espace affine de $\mathbb{K}^n$, de la forme $x' + E$, où E est le sous espace linéaire de $\mathbb{K}^n$ des solutions du système homogène.

Exemple 1.I.8. — Si $f : E \to F$ est une application linéaire de E vers F, $\mathbb{K}$-espaces vectoriels, alors pour $v \in \mathrm{Im}(f)$, la *fibre* $E_v = f^{-1}(v)$ est un sous espace affine de E, muni de sa structure canonique d'espace affine. En effet, il existe $u \in E_v$ puisque $v \in \mathrm{Im}(f)$. On vectorialise E_v en u, donc :

$$\Theta_u(E_v) = \{w - u \mid f(w) = v\} = \{z \mid f(z) = 0\} = \ker(f),$$

parce que $z = w - v$ satisfait $f(z) = 0$ si et seulement si $f(w) = 0$. Le sous espace E_v est donc dirigé par $\ker(f)$.

1.I.B.2. Sous espaces affine engendré par une partie. —

Définition 1.I.9. — Si $A \neq \varnothing$ est une partie de $\mathcal{E}$, on appelle *espace affine engendré par* A les plus petit sous espace affine de $\mathcal{E}$ contenant A. On le note $\mathrm{aff}(A)$.

Remarque 1.I.10. — Si $(\mathcal{F}_i)_{i\in I}$ est une famille de sous espaces affine de $\mathcal{E}$ et $\mathcal{F} = \cap_{i\in I}\mathcal{F}_i \neq \varnothing$, alors $\mathcal{F}$ est un sous espace affine de $\mathcal{E}$, dirigé par $\cap_{i\in I}\vec{\mathcal{F}}_i$.

Démonstration. — Étant donné $O \in \mathcal{F}$, on a $F_i = \Theta_O(\mathcal{F}_i)$ sous espace vectoriel de $\mathcal{E}$, donc $F = \cap_{i\in I}F_i$ est un sous espace vectoriel de $\mathcal{E}$ et $F = \Theta_O(\mathcal{F})$ du fait que Θ_O est bijective. □

Remarque 1.I.11. — Pour $A \subset \mathcal{E}$, $\mathrm{aff}(A)$ est l'intersection des sous espaces affine de $\mathcal{E}$ contenant A. Si $O \in A$, on a $\mathrm{aff}(A) = O + \mathrm{vect}(\Theta_O(A))$.

Démonstration. — On sait que cette intersection, notée $\mathcal{F}$, est un sous espace affine de $\mathcal{E}$ qui contient A. Pour voir qu'elle est minimale, on prend un espace affine $\mathcal{F}'$ contenant A, donc $\mathcal{F} \subset \mathcal{F}'$ puisque $\mathcal{F}'$ fait partie de la famille de sous espaces dont l'intersection est $\mathcal{F}$. □

1.I.B.3. Intersection d'espaces affines. —

Proposition 1.I.12. *— Soit $\mathcal{F}$ et $\mathcal{G}$ sous espaces affines de $\mathcal{E}$, dirigés par F et G. Alors $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ si et seulement si, étant donnés $P \in \mathcal{F}$ et $Q \in \mathcal{G}$, on a $\overrightarrow{PQ} \in F + G$. En particulier, si $F + G = E$, on a $\mathcal{F} \cap \mathcal{G} \neq \emptyset$.*

Dans la proposition, il suffit de vérifier qu'il existe $P \in \mathcal{F}$ et $Q \in \mathcal{G}$ tels que $\overrightarrow{PQ} \in F + G$ pour conclure $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. On aura alors que, pour tout $P \in \mathcal{F}$ et $Q \in \mathcal{G}$, le vecteur $\overrightarrow{PQ}$ appartient à $\in F + G$.

Démonstration. — Si $M \in \mathcal{F} \cap \mathcal{G}$, alors $\overrightarrow{PM} \in F$ et $\overrightarrow{QM} \in G$ donc $\overrightarrow{PQ} = \overrightarrow{PM} - \overrightarrow{QM} \in F + G$. Réciproquement, si $\overrightarrow{PQ} \in F + G$ alors $\overrightarrow{PQ}$ s'exprime comme somme de vecteurs F et de G. Ces vecteurs ont la forme $\overrightarrow{PM}$ et $-\overrightarrow{QN}$, pour $M \in \mathcal{F}$ et $N \in \mathcal{G}$. Mais $\overrightarrow{PQ} = \overrightarrow{PM} - \overrightarrow{QN}$ implique $\vec{0} = \overrightarrow{PM} - \overrightarrow{NP}$ donc $N = M$ et $\mathcal{F} \cap \mathcal{G}$ contient $M = N$. □

1.I.C. Parallélisme. —

Définition 1.I.13. *— Soit $\mathcal{F}$ et $\mathcal{G}$ sous espaces affines d'un espace affine $\mathcal{E}$. On dit que $\mathcal{F}$ et $\mathcal{G}$ sont *parallèles* si $\vec{\mathcal{F}} = \vec{\mathcal{G}}$.*

Exemple 1.I.14. *— Dans l'exemple 1.I.8, quelque soient $u, v \in F$, les sous espaces E_u et E_v sont parallèles.*

Remarque 1.I.15. *— Si $\mathcal{F}$ et $\mathcal{G}$ sont parallèles, $\mathcal{F} = \mathcal{G}$ ou alors $\mathcal{F} \cap \mathcal{G} = \emptyset$.*

Démonstration. — S'il existe $P \in \mathcal{F} \cap \mathcal{G}$, alors $\mathcal{F} = P + \vec{\mathcal{F}} = P + \vec{\mathcal{G}} = \mathcal{G}$. □

Remarque 1.I.16. *— Soit $P \in \mathcal{E}$ et $\mathcal{F}$ un sous espace affine de $\mathcal{E}$. Alors il existe un et un seul sous espace affine $\mathcal{G}$ de $\mathcal{E}$ parallèle à $\mathcal{F}$ et passant par P.*

Démonstration. — Le sous espace $P + \vec{\mathcal{F}}$ parallèle à $\mathcal{F}$ et passe par P. Si $\mathcal{G}$ est un autre sous espace par P et parallèle à $\mathcal{F}$, on a $\vec{\mathcal{G}} = \vec{\mathcal{F}}$ et $P \in \mathcal{G}$ donc $\mathcal{G} = F + \vec{\mathcal{F}}$. □

Corollaire 1.I.17. *— Soit $\mathcal{F}$ sous espace affine de $\mathcal{E}$, de direction $F \subset E$. Soit G un supplémentaire de F dans E. Alors tout sous espace affine de $\mathcal{E}$ dirigé par G rencontre $\mathcal{F}$ en un et un seul point.*

Démonstration. — Soit $\mathcal{G}$ sous espace affine de $\mathcal{E}$ dirigé par G. La proposition 1.I.12 dit que $\mathcal{G} \cap \mathcal{F}$ n'est pas vide car $E = F + G$. Il s'agit donc d'un sous espace affine de $\mathcal{E}$, dirigé par $F \cap G = \{0\}$. Cet espace consiste donc d'un seul point. □

1.I.D. Barycentres. —

1.I.D.1. Définition de barycentre. —

Définition 1.I.18. *— Soit $\mathcal{E}$ un espace affine et $(A_1, \ldots, A_k)$ points de $\mathcal{E}$. Soit $(\lambda_1, \ldots, \lambda_k) \in \mathbb{K}^k$, avec :*

$$\sum_{i=1}^{k} \lambda_i \neq 0.$$

Alors il existe un et un seul point G de $\mathcal{E}$, le barycentre de la famille de points pondérés $(A_i, \lambda_i)_{i \in [\![1,k]\!]}$ tel que :

$$\sum_{i=1}^{k} \lambda_i \overrightarrow{GA_i} = \vec{0}. \tag{1}$$

Posons $\lambda = \sum_{i=1}^{k} \lambda_i$. Alors, quelque soit $O \in \mathcal{E}$, on a :

$$\lambda \overrightarrow{OG} = \sum_{i=1}^{k} \lambda_i \overrightarrow{OA_i}. \tag{2}$$

On note $G = \mathrm{Bary}(A_i, \lambda_i)_{i\in[\![1,k]\!]}$.

On démontre que la définition est bien posée. Pour montrer que G existe, nous prenons $Q \in \mathcal{E}$ et, comme $\lambda \neq 0$ nous pouvons poser :

$$G = Q + \frac{1}{\lambda}\sum_{i=1}^{k} \lambda_i \overrightarrow{QA_i}.$$

Donc la relation (2) est valide si $O = Q$. Montrons qu'elle reste alors valide quelque soit O. On écrit :

$$\lambda\overrightarrow{OG} = \lambda\overrightarrow{OQ} + \lambda\overrightarrow{QG} = \lambda\overrightarrow{OQ} + \sum_{i=1}^{k}\lambda_i\overrightarrow{QA_i} = \sum_{i=1}^{k}\lambda_i(\overrightarrow{OQ} + \overrightarrow{QA_i}) = \sum_{i=1}^{k}\lambda_i\overrightarrow{OA_i}.$$

On peut enfin déduire (1). En effet, comme (2) est valide pour tout O, elle est valide aussi pour $O = G$, auquel cas l'équation devient (1).

1.I.D.2. Associativité du barycentre. — Soit $k_1, \ldots, k_s$ entiers et, pour tout $i \in [\![1, s]\!]$, considérons des familles de points pondérés $(A_{i,j}, \lambda_{i,j})_{j\in[\![1,k_i]\!]}$ de $\mathcal{E}$ avec :

$$\mu_i := \sum_{j=1}^{k_i} \lambda_{i,j} \neq 0.$$

Posons $B_i = \mathrm{Bary}(A_{i,j}, \lambda_{i,j})_{j\in[\![1,k_i]\!]}$. Notons $I = \{(i,j) \mid \forall i \in [\![1,s]\!],\, j \in [\![1,k_i]\!]\}$.

Proposition 1.I.19. — *On a* $\mathrm{Bary}(B_i, \mu_i)_{i\in[\![1,s]\!]} = \mathrm{Bary}(A_{i,j}, \lambda_{i,j})_{(i,j)\in I}$.

Démonstration. — Posons $G = \mathrm{Bary}(B_i, \mu_i)_{i\in[\![1,s]\!]}$ et $G' = \mathrm{Bary}(A_{i,j}, \lambda_{i,j})_{(i,j)\in I}$. Pour $i \in [\![1,s]\!]$ on a $\sum_{j\in[\![1,k_i]\!]} \lambda_{i,j}\overrightarrow{B_iA_{i,j}} = \vec{0}$. Aussi nous avons $\sum_{i\in[\![1,s]\!]} \mu_i\overrightarrow{GB_i} = \vec{0}$. Donc :

$$\begin{aligned}\sum_{(i,j)\in I}\lambda_{i,j}\overrightarrow{GA_{i,j}} &= \sum_{i\in[\![1,s]\!]}\sum_{j\in[\![1,k_i]\!]}\lambda_{i,j}\overrightarrow{GA_{i,j}} = \sum_{i\in[\![1,s]\!]}\sum_{j\in[\![1,k_i]\!]}\lambda_{i,j}(\overrightarrow{GB_i} + \overrightarrow{B_iA_{i,j}})\\ &= \sum_{i\in[\![1,s]\!]}\left(\sum_{j\in[\![1,k_i]\!]}\lambda_{i,j}\right)\overrightarrow{GB_i} + \sum_{i\in[\![1,s]\!]}\sum_{j\in[\![1,k_i]\!]}\lambda_{i,j}\overrightarrow{B_iA_{i,j}} =\\ &= \sum_{i\in[\![1,s]\!]}\mu_i\overrightarrow{GB_i} = \vec{0}.\end{aligned}$$

Donc $G = G'$. □

1.I.E. Repères et coordonnées. —

1.I.E.1. Repères cartésiens. —

Définition 1.I.20. — Soit $\mathcal{E}$ un espace affine de direction E et dimension $n < \infty$ et soit $O \in \mathcal{E}$ et $\mathcal{B} = (\vec{e_1}, \ldots, \vec{e_n})$ une base de E. On dit que $\mathcal{R} = (O, \mathcal{B})$ est un *repère cartésien sur* $\mathcal{E}$. Pour tout $P \in \mathcal{E}$, il existe un et un seul vecteur colonne $X = (x_1, \ldots, x_n)^t \in \mathbb{K}^n$ tel que $P = O + x_1\vec{e_1} + \cdots + x_n\vec{e_n}$. On dit que x est le *vecteur des coordonnées cartésiennes de* P en le repère $\mathcal{R}$.

Remarque 1.I.21. — Soit $\mathcal{R} = (O, \mathcal{B})$ et $\mathcal{R}' = (O', \mathcal{B}')$ repères cartésiens de $\mathcal{E}$. Alors, pour $i, j \in [\![1, n]\!]$, il existe $a_{i,j} \in \mathbb{K}$ et $c_i \in \mathbb{K}$ tels que :

$$\vec{e_j}' = \sum_{i=1}^{n} a_{i,j}\vec{e_i}, \qquad \overrightarrow{OO'} = \sum_{i=1}^{n} c_i\vec{e_i}.$$

On écrit la matrice $P = (a_{i,j})$, autrement dit

$$P = \mathrm{Mat}_{\mathcal{B},\mathcal{B}'}(\mathrm{id}_E),$$

et $c = (c_1, \dots, c_n)^t$. Les équations deviennent $\mathcal{B}' = \mathcal{B}P$ et $\overrightarrow{OO'} = \mathcal{B}c$. On trouve donc $P = O + \mathcal{B}x = O + \overrightarrow{OO'} + \mathcal{B}'x' = O + \mathcal{B}c + \mathcal{B}Px'$, ce qui implique :

$$x = c + Px'.$$

Bien sûr on trouve :

$$x' = P^{-1}x - P^{-1}c.$$

On utilisera parfois la convention $\mathrm{Mat}_{\mathcal{R}}(P) = (1, x_1, \dots, x_n)^t$ au lieu de $(x_1, \dots, x_n)$. Dans ce cas, la formule de passage de base devient :

$$\mathrm{Mat}_{\mathcal{R}}(P) = \mathrm{Mat}_{\mathcal{R},\mathcal{R}'}(\mathrm{id}_{\mathcal{E}})\mathrm{Mat}_{\mathcal{R}'}(P), \qquad \text{où} \qquad \mathrm{Mat}_{\mathcal{R},\mathcal{R}'}(\mathrm{id}_{\mathcal{E}}) = \begin{pmatrix} 1 & 0 \\ c & P \end{pmatrix}.$$

On retrouve :

$$\mathrm{Mat}_{\mathcal{R}',\mathcal{R}}(\mathrm{id}_{\mathcal{E}}) = \mathrm{Mat}_{\mathcal{R},\mathcal{R}'}(\mathrm{id}_{\mathcal{E}})^{-1} = \begin{pmatrix} 1 & 0 \\ -P^{-1}c & P^{-1} \end{pmatrix}.$$

1.I.E.2. Coordonnées barycentriques. — Soit $\dim(\mathcal{E}) = n < \infty$ et prenons $A_0, \dots, A_k$ points de $\mathcal{E}$, avec $k \leq n$. Notons, pour $i \in [\![1, k]\!]$, $\overrightarrow{e_i} = \overrightarrow{A_0A_i}$. On a

$$\mathrm{aff}(A_0, \dots, A_k) = A_0 + \mathrm{vect}(\overrightarrow{e_1}, \dots, \overrightarrow{e_k}),$$

donc $\dim(\mathrm{aff}(A_0, \dots, A_k)) \leq k$, l'égalité étant atteinte si i seulement si $(\overrightarrow{e_1}, \dots, \overrightarrow{e_k})$ est une famille libre dans E. Il est clair que ceci ne dépend du choix de 0 comme indice privilégié, ainsi cela est équivalent à ce que, quelque soit $i \in [\![0, k]\!]$, la famille suivante soit libre :

$$(\overrightarrow{A_iA_0}, \dots, \overrightarrow{A_iA_{i-1}}, \overrightarrow{A_iA_{i+1}}, \dots, \overrightarrow{A_iA_k}).$$

Remarque 1.I.22. — L'ensemble des barycentres de $A_0, \dots, A_k$ est $\mathrm{aff}(A_0, \dots, A_k)$.

Démonstration. — Qu'un point P soit l'un de ces barycentres veut dire $P = \mathrm{Bary}((A_i, \lambda_i)_{i \in [\![0,k]\!]})$ pour certains $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ avec $\lambda = \lambda_1 + \cdots + \lambda_k \neq 0$. Ceci arrive si et seulement si

$$\lambda\overrightarrow{A_0P} = \sum_{i=1}^{k} \lambda_i \overrightarrow{A_0A_i}.$$

Comme les $\lambda_1, \dots, \lambda_k$ sont arbitraires et $\lambda \neq 0$, ceci arrive si et seulement si $P \in A_0 + \mathrm{vect}(\overrightarrow{e_1}, \dots, \overrightarrow{e_k}) = \mathrm{aff}(A_0, \dots, A_k)$. □

Définition 1.I.23. — Soit $(A_0, \dots, A_n)$ points de $\mathcal{E}$ tels que $\mathrm{aff}(A_0, \dots, A_n) = \mathcal{E}$. Alors on dit que $(A_0, \dots, A_n)$ est un *repère affine* de $\mathcal{E}$.

Remarque 1.I.24. — Soit $\mathcal{R} = (A_0, \dots, A_n)$ un repère affine de $\mathcal{E}$ et $P \in \mathcal{E}$. Alors il existe un et un seul vecteur $\lambda = (\lambda_0, \dots, \lambda_n)^t \in \mathbb{K}^{n+1}$ tel que $\sum_{i=0}^{n} \lambda_i = 1$ et $P = \mathrm{Bary}((A_i, \lambda_i)_{i \in [\![0,n]\!]})$.

Démonstration. — On a déjà vu l'existence. Quant à l'unicité, si $(\lambda'_0, \dots, \lambda'_n)$ satisfait aussi les conditions, on a :

$$\sum_{i=1}^{n} \lambda_i \overrightarrow{A_0A_i} = \left(\sum_{i=0}^{n} \lambda_i\right) \overrightarrow{A_0P} = \overrightarrow{A_0P} = \sum_{i=1}^{n} \lambda'_i \overrightarrow{A_0A_i},$$

donc $\lambda_i = \lambda'_i$ pour tout $i \in [\![1, n]\!]$, puis aussi $\lambda_0 = \lambda'_0$ grâce à la condition $\sum_{i=0}^{n} \lambda_i = 1 = \sum_{i=0}^{n} \lambda'_i$. □

Définition 1.I.25. — On appelle λ de la remarque précédente le vecteur des *coordonnés barycentriques* de P en le repère $\mathcal{R}$, noté $\mathrm{Mat}_{\mathcal{R}}(P) = (\lambda_0, \dots, \lambda_n)^t$.

1.I.E.3. Passage entre coordonnées cartésiennes et barycentriques. — Soit $\mathcal{B} = (\overrightarrow{e_1}, \dots, \overrightarrow{e_n})$ une base de E et $O \in \mathcal{E}$. Alors $\mathcal{R} = (O, \mathcal{B})$ est un repère cartésien de $\mathcal{E}$. De plus $\mathcal{S} = (O, O+\overrightarrow{e_1}, \dots, O+\overrightarrow{e_n})$ est un repère affine de $\mathcal{E}$. Soit $P \in \mathcal{E}$.

Remarque 1.I.26. — Soit $\mathrm{Mat}_{\mathcal{R}} = (1, x_1, \dots, x_n)^t$ et $\mathrm{Mat}_{\mathcal{S}} = (\lambda_0, \dots, \lambda_n)^t$. Alors

$$(\lambda_0, \dots, \lambda_n) = (1 - \sum_{i=1}^{n} x_i, x_1, \dots, x_n),$$

$$(1, x_1, \dots, x_n) = (\sum_{i=0}^{n} \lambda_i, \lambda_0, \dots, \lambda_n).$$

1.I.F. Convexes. — Ici, nous prenons $\mathbb{K} = \mathbb{R}$.

Définition 1.I.27. — Une partie $\mathcal{C}$ d'un espace affine $\mathcal{E}$ est *convexe* si, pour tout $P, Q \in A$, le segment $[P,Q] = \{P + t\overrightarrow{PQ} \mid t \in [0,1]\}$ est contenu dans $\mathcal{C}$.

Remarque 1.I.28. — Si $(\mathcal{C}_i)_{i\in I}$ sont convexes, alors $\mathcal{C} = \cap_{i\in I}\mathcal{C}_i$ est convexe.

Démonstration. — Soit $P, Q \in A$. Alors $[P,Q]$ est contenu dans tous $\mathcal{C}_i$ car $\mathcal{C}_i$ est convexe. Ainsi $[P,Q]$ est contenu dans $\mathcal{C}$. □

Définition 1.I.29. — Soit A une partie de $\mathcal{E}$. L'enveloppe convexe de A, notée $\mathrm{conv}(A)$, est le plus petit convexe de $\mathcal{A}$ contenant A.

Proposition 1.I.30. — *On a* $\mathrm{conv}(A) = \{\mathrm{Bary}(A_i, \lambda_i)_{i\in[\![1,k]\!]} \mid \lambda_i \geq 0, k \geq 1, \exists \lambda_i > 0\}$.

Démonstration. — Soit $\mathcal{C} = \{\mathrm{Bary}(A_i, \lambda_i)_{i\in[\![1,k]\!]} \mid \lambda_i \geq 0, k \geq 1, \exists \lambda_i > 0\}$.

Pour montrer $\mathcal{C} \subset \mathrm{conv}(A)$, il faut montrer que $\mathcal{C}$ est contenu dans tout convexe $\mathcal{D}$ contenant A. Pour le faire, on doit montrer que tout barycentre $G = \mathrm{Bary}(A_i, \lambda_i)_{i\in[\![1,k]\!]}$ appartient à $\mathcal{D}$. Faisons-le par récurrence sur k. Si $k = 1$, c'est clair car alors $G \in A \subset \mathcal{D}$. Supposons alors que tout barycentre à coefficients positifs de $k-1$ points de A soit dans $\mathcal{D}$ et considérons $G = \mathrm{Bary}(A_i, \lambda_i)_{i\in[\![1,k]\!]}$. Il existe $i \in [\![1,k]\!]$ tel que $\lambda_i > 0$, disons $i = k$ quitte à permuter les indices. Si $\lambda_i = 0$ pour tout $i \in [\![1, k-1]\!]$ en fait $G = A_k$ et l'énoncé est valide. Sinon on peut appliquer à $G' = \mathrm{Bary}(A_i, \lambda_i)_{i\in[\![1,k-1]\!]}$ l'hypothèse de récurrence pour conclure que $G' \in \mathcal{D}$. Alors $G = \mathrm{Bary}((G', \lambda'), (A_k, \lambda_k))$ par associativité des barycentres, où $\lambda' = \sum_{i=1}^{k-1} \lambda_i \geq 0$. Donc $G \in [G', A_k]$ appartient à $\mathcal{D}$ par convexité de $\mathcal{D}$.

Réciproquement, on peut montrer que $\mathcal{C}$ est convexe pour conclure que, comme il contient évidemment A, il contient $\mathrm{conv}(A)$. On prend donc deux points de $\mathcal{C}$, i.e. deux barycentres G et G' à coefficients positifs de points de A. Un point de $[GG']$ étant un barycentre à coefficients positifs de G et G', par associativité il est encore un barycentre à coefficients positifs de points de A, donc un élément de $\mathcal{C}$. □

1.II. Applications affines

Nous noterons toujours $\mathcal{E}$ et $\mathcal{F}$ espaces affines de directions E et F.

1.II.A. Applications affines et linéaires. —

1.II.A.1. Partie linéaire d'une application affine. —

Définition 1.II.1. — Soit $\varphi : \mathcal{E} \to \mathcal{F}$ une application. On dit que φ est *affine* s'il existe $O \in \mathcal{E}$ et $f : E \to F$ linéaire tels que $\varphi(P) = \varphi(O) + f(\overrightarrow{OP})$, quelque soit $P \in \mathcal{E}$.

On peut écrire l'égalité $\varphi(P) = \varphi(O) + f(\overrightarrow{OP})$ aussi $f(\overrightarrow{OM}) = \overrightarrow{\varphi(O)\varphi(M)}$.

Remarque 1.II.2. — L'application f ne dépend pas de O. On la note $\vec{\varphi}$ et on l'appelle la *partie linéaire de* φ.

Démonstration. — Soit $Q \in \mathcal{E}$ et $g : E \to F$ linéaire tels que $\varphi(P) = \varphi(Q) + g(\overrightarrow{QP})$, quelque soit $P \in \mathcal{E}$. Alors $g(\overrightarrow{QP}) = \overrightarrow{\varphi(Q)\varphi(P)}$. Par ailleurs:

$$f(\overrightarrow{QP}) = f(\overrightarrow{QO} + \overrightarrow{OP}) = f(\overrightarrow{QO}) + f(\overrightarrow{OP}) = \overrightarrow{\varphi(O)\varphi(P)} - \overrightarrow{\varphi(O)\varphi(Q)} = \overrightarrow{\varphi(Q)\varphi(P)},$$

donc $f(\overrightarrow{QP}) = g(\overrightarrow{QP})$, ce qui implique $f = g$. □

Remarque 1.II.3. — Soit $\varphi : \mathcal{E} \to \mathcal{F}$ affine et $O \in \mathcal{E}$. Alors $\Theta_{\varphi(O)} \circ \varphi \circ \Theta_O^{-1} : E \to F$ est linéaire.

1.II.A.2. Translations. —

Définition 1.II.4. — Si $\vec{v} \in E$, la *translation* $t_{\vec{v}} : \mathcal{E} \to \mathcal{E}$ est l'application $P \mapsto P + \vec{v}$. Il s'agit d'une bijection affine de $\mathcal{E}$, d'inverse $t_{-\vec{v}}$.

Proposition 1.II.5. — *Une application affine $\varphi : \mathcal{E} \to \mathcal{E}$ est une translation si et seulement si on a $\vec{\varphi} = \mathrm{id}_E$.*

Démonstration. — Soit $O, P \in \mathcal{E}$. On regarde les points $O, \varphi(O), P, \varphi(P)$. On sait que φ est une translation ssi $\varphi(P) = P + \vec{v}$ pour un certain $v \in E$ fixé, i.e. ssi pour tout $O, P \in \mathcal{E}$:

$$\overrightarrow{P\varphi(P)} = \vec{v} = \overrightarrow{O\varphi(O)}, \qquad \text{donc ssi} \qquad \overrightarrow{OP} = \overrightarrow{\varphi(O)\varphi(P)} = \vec{\varphi}(\overrightarrow{OP}),$$

d'après la règle du parallélogramme. Ceci est donc équivalent à ce que $\vec{\varphi} = \mathrm{id}_E$. □

1.II.A.3. Projections. — Soit $\mathcal{F}$ un sous espace affine de $\mathcal{E}$ et G un supplémentaire de $F = \vec{\mathcal{F}}$ dans $E = \vec{\mathcal{E}}$. On définit la projection.

Définition 1.II.6. — La *projection* de $\mathcal{E}$ sur $\mathcal{F}$ parallèle à G est l'application $\pi : \mathcal{E} \to \mathcal{F}$ qui, à chaque point $P \in \mathcal{E}$, associe $\mathcal{F} \cap \mathcal{G}_P$, où $\mathcal{G}_P$ est le sous espace affine de $\mathcal{E}$ parallèle à G et passant par P.

La définition est bien posée d'après la proposition 1.I.17.

Proposition 1.II.7. — *La projection π est une application affine, dont la partie linéaire $\vec{\pi}$ est la projection $p : E \to F$ parallèle à G.*

Démonstration. — Fixons $O \in \mathcal{F}$. On a $\pi(O) = O$ car $O = \mathcal{G}_O \cap \mathcal{F}$. Soit maintenant $P \in \mathcal{E}$. On écrit de manière unique $\overrightarrow{OP} = \vec{u} + \vec{v}$ avec $\vec{u} = p(\overrightarrow{OP}) \in F$ et $\vec{v} \in G$, donc $O + \vec{u} \in \mathcal{F}$. De plus, $O + \vec{u} = O + \overrightarrow{OP} - \vec{v} = P - \vec{v}$, ce qui appartient à $\mathcal{G}_P = P + G$.

Donc $\pi(P) = O + \vec{u} = O + p(\overrightarrow{OP})$ et comme $O = \pi(O)$ aussi $\pi(P) = O + \vec{\pi}(\overrightarrow{OP})$, autrement dit $\vec{\pi} = p$, ce qui montre les deux énoncés. □

1.II.A.4. Symétries. — Soit $\mathcal{F}$ un sous espace affine de $\mathcal{E}$ et G un supplémentaire de $F = \vec{\mathcal{F}}$ dans $E = \vec{\mathcal{E}}$.

Définition 1.II.8. — La *symétrie* $\sigma : \mathcal{E} \to \mathcal{E}$ d'axe $\mathcal{F}$ parallèle à G est l'application qui, à chaque point $P \in \mathcal{E}$, associe $\sigma(P) = P + 2\overrightarrow{P\pi(P)}$.

Proposition 1.II.9. — *La symétrie σ est une application affine, dont la partie linéaire $\vec{\sigma}$ est la symétrie $s : E \to E$ d'axe F parallèle à G.*

Démonstration. — Fixons $O \in \mathcal{F}$, donc $\sigma(O) = O$. Soit $P \in \mathcal{E}$. On écrit, comme dans la preuve de la proposition 1.II.7, $\overrightarrow{OP} = \vec{u} + \vec{v}$ avec $\vec{u} = p(\overrightarrow{OP}) \in F$ et $\vec{v} \in G$, et on rappelle $\pi(P) = P - \vec{v}$, donc $\overrightarrow{P\pi P} = -\vec{v}$ et $\overrightarrow{P\sigma(P)} = -2\vec{v}$. On écrit :

$$\vec{\sigma}(\overrightarrow{OP}) = \overrightarrow{O\sigma(P)} = \overrightarrow{OP} + \overrightarrow{P\sigma(P)} = \vec{u} + \vec{v} - 2\vec{v} = \vec{u} - \vec{v} = s(\overrightarrow{OP}),$$

ce qui achève la démonstration. □

1.II.A.5. Composition d'applications affines. —

Remarque 1.II.10. — La composition de deux applications affines ψ et φ l'est aussi, et
$$\overrightarrow{\psi \circ \varphi} = \overrightarrow{\psi} \circ \overrightarrow{\varphi}.$$

Démonstration. — Soit $\varphi : \mathcal{E} \to \mathcal{F}$ et $\psi\mathcal{F} \to \mathcal{G}$ applications affines et choisissons $O \in \mathcal{E}$. On a donc, pour $P \in \mathcal{E}$, $Q \in \mathcal{F}$, $\varphi(P) = \varphi(O) + \overrightarrow{\varphi}(\overrightarrow{OP})$ et $\psi(Q) = \psi(\varphi(O)) + \overrightarrow{\psi}(\overrightarrow{\varphi(O)Q})$. Donc:
$$\psi(\varphi(P)) = \psi(\varphi(O)) + \overrightarrow{\psi}(\overrightarrow{\varphi(O)\varphi(P)}) = \psi(\varphi(O)) + \overrightarrow{\psi}(\overrightarrow{\varphi}(\overrightarrow{OP})),$$
donc, $\overrightarrow{\psi} \circ \overrightarrow{\varphi}$ étant linéaire, on a $\psi \circ \varphi$ affine. Nous avons montré que $\overrightarrow{\psi \circ \varphi} = \overrightarrow{\psi} \circ \overrightarrow{\varphi}$. □

1.II.A.6. Applications affines et translations. —

Remarque 1.II.11. — Soit $\varphi : \mathcal{E} \to \mathcal{E}$ affine et $O \in \mathcal{E}$. Alors il existe unique $(\psi, \overrightarrow{u})$ avec $\psi : \mathcal{E} \to \mathcal{E}$ affine qui fixe O et $\varphi = t_{\overrightarrow{u}} \circ \psi$.

Démonstration. — On prend $\overrightarrow{u} = \overrightarrow{O\varphi(O)}$ puis $\psi = t_{-\overrightarrow{u}} \circ \varphi$. On trouve $\psi(O) = \varphi(O) - \overrightarrow{u} = O$, donc ψ fixe O. Pour l'unicité, si $t_{\overrightarrow{u}} \circ \psi = t_{\overrightarrow{u}'} \circ \psi'$ alors ψ et ψ' ont même partie linéaire, donc elles sont égales puisqu'elles fixent O toutes les deux. Par conséquent, $\overrightarrow{u} = \overrightarrow{u}'$. □

1.II.A.7. Homothéties. —

Définition 1.II.12. — L'*homothétie affine* de centre $O \in \mathcal{E}$ et rapport $\lambda \in \mathbb{K}^*$ est l'application affine $\varphi : \mathcal{E} \to \mathcal{E}$ définie par $\varphi(P) = O + \lambda\overrightarrow{OP}$.

Remarque 1.II.13. — On a les propriétés suivantes.

i) Une application affine φ est une homothétie de rapport λ si et seulement si φ possède un point fixe et $\overrightarrow{\varphi} = \lambda \mathrm{id}_E$.

ii) Si φ est une homothétie de centre O et rapport λ et ψ est une transformation affine, alors $\psi\varphi\psi^{-1}$ est une homothétie de centre $\psi(O)$ et rapport λ.

iii) Une application affine φ est composition d'une homothétie de rapport λ et d'une translation si et seulement si $\overrightarrow{\varphi} = \lambda \mathrm{id}_E$.

iv) La composition d'homothéties $\varphi_1, \ldots, \varphi_r$ et translations $t_1, \ldots, t_s$ est de la forme $t \circ \varphi$, avec t translation et φ homothétie.

Démonstration. — Le premier énoncé est clair.

Pour le deuxième, soit O le centre de φ et $Q = \psi(O)$. On calcule $\psi\varphi\psi^{-1}(Q) = \psi(\varphi(O)) = Q$. Aussi, on voit que $\overrightarrow{\psi} = \lambda \mathrm{id}_E$, ce qui prouve l'énoncé.

Ensuite, la composition φ d'une homothétie de centre rapport λ et d'une translation satisfait évidemment $\overrightarrow{\varphi} = \lambda \mathrm{id}_E$. Réciproquement, on fixe $O \in \mathcal{E}$ et on écrit $\varphi = t_{\overrightarrow{u}} \circ \psi$ avec $\psi(O) = O$, alors $\overrightarrow{\psi} = \lambda \mathrm{id}_E$ donc ψ est une homothétie de rapport λ et centre O.

Pour le dernier énoncé, la composition φ en question satisfait $\overrightarrow{\varphi} = \lambda_1 \ldots \lambda_s \mathrm{id}_E$, où λ_i est le rapport d'homothétie de φ_i, c'est donc la composition d'une translation et d'une homothétie. □

1.II.B. Points fixes. —

Proposition 1.II.14. — *Soit $\varphi : \mathcal{E} \to \mathcal{E}$ affine. Alors* $\mathrm{Fix}(\varphi)$ *est soit vide, soit un sous espace affine de $\mathcal{E}$ dirigé par l'espace propre de la valeur propre* 1 *de $\overrightarrow{\varphi}$.*

Démonstration. — Supposons $\mathrm{Fix}(\varphi)$ non vide donc soit $O \in \mathrm{Fix}(\varphi)$. Prenons $P \in \mathcal{E}$ et utilisons que $O = \varphi(O)$ pour écrire $\varphi(P) = O + \overrightarrow{\varphi}(\overrightarrow{OP})$. Alors P appartient à $\mathrm{Fix}(\varphi)$ ssi $P = O + \overrightarrow{\varphi}(\overrightarrow{OP})$, i.e. ssi $\overrightarrow{OP} = \overrightarrow{\varphi}(\overrightarrow{OP})$. Ceci équivaut à $\overrightarrow{OP} \in \ker(\overrightarrow{\varphi} - \mathrm{id}_E)$, l'espace propre de $\overrightarrow{\varphi}$ de la valeur propre 1. □

Théorème 1.II.15. — *Soit $\varphi : \mathcal{E} \to \mathcal{E}$ affine et supposons $E = \ker(\overrightarrow{\varphi} - \mathrm{id}_E) \oplus \mathrm{Im}(\overrightarrow{\varphi} - \mathrm{id}_E)$. Alors φ s'écrit uniquement sous la forme $\varphi = t_{\overrightarrow{u}} \circ \psi = \psi \circ t_{\overrightarrow{u}}$, où $\psi : \mathcal{E} \to \mathcal{E}$ est affine à point fixe et $\overrightarrow{u} \in \ker(\overrightarrow{\varphi} - \mathrm{id}_E)$.*

Démonstration. — Nous commençons avec un point O de $\mathcal{E}$. On écrit :

$$\overrightarrow{O\varphi(O)} = \overrightarrow{u} + \overrightarrow{\varphi}(\overrightarrow{v}) - \overrightarrow{v}, \qquad \text{pour certains } \overrightarrow{v}, \overrightarrow{u} \in E \text{ où } \overrightarrow{u} \in \ker(\overrightarrow{\varphi} - \mathrm{id}_E).$$

On considère $Q \in \mathcal{E}$ tel que $Q + \overrightarrow{v} = O$ i.e. $Q = O - \overrightarrow{v}$. Donc $\overrightarrow{OQ} = -\overrightarrow{v}$. Ainsi :

$$\overrightarrow{Q\varphi(Q)} = \overrightarrow{QO} + \overrightarrow{O\varphi(O)} + \overrightarrow{\varphi(O)\varphi(Q)} = \overrightarrow{v} + \overrightarrow{u} + \overrightarrow{\varphi}(\overrightarrow{v}) - \overrightarrow{v} - \overrightarrow{\varphi}(\overrightarrow{v}) = \overrightarrow{u}.$$

On prend $\psi = t_{-\overrightarrow{u}} \circ \varphi$. On trouve $\varphi = t_{\overrightarrow{u}} \circ \psi$ et $Q \in \mathrm{Fix}(\psi)$ car :

$$\overrightarrow{Q\psi(Q)} = \overrightarrow{Q\varphi(Q)} - \overrightarrow{u} = \overrightarrow{0}.$$

On obtient aussi $\varphi = \psi \circ t_{\overrightarrow{u}}$ car, si $P \in \mathcal{E}$, on calcule :

$$\psi \circ t_{\overrightarrow{u}}(P) = \psi(P + \overrightarrow{u}) = \varphi(O) + \overrightarrow{\varphi}(\overrightarrow{OP} + \overrightarrow{u}) - \overrightarrow{u} = \varphi(O) + \overrightarrow{\varphi}(\overrightarrow{OP}) = \varphi(P).$$

Montrons enfin que $\overrightarrow{u}$ et ψ sont uniques. Soient $\overrightarrow{u}' \in \ker(\overrightarrow{\varphi} - \mathrm{id}_E)$ et ψ' ayant un point fixe Q' avec $t_{\overrightarrow{u}'} \circ \psi' = \varphi$. On écrit $\varphi(Q') = Q' + \overrightarrow{u}'$ et $\varphi(Q) = Q + \overrightarrow{u}$ donc :

$$\overrightarrow{QQ'} = \overrightarrow{Q\varphi(Q)} + \overrightarrow{\varphi(Q)\varphi(Q')} + \overrightarrow{\varphi(Q')Q'} = \overrightarrow{u} + \overrightarrow{\varphi}(\overrightarrow{QQ'}) - \overrightarrow{u}'.$$

Ainsi :

$$\ker(\overrightarrow{\varphi} - \mathrm{id}_E) \ni \overrightarrow{u} - \overrightarrow{u}' = \overrightarrow{QQ'} - \overrightarrow{\varphi}(\overrightarrow{QQ'}) \in \mathrm{Im}(\overrightarrow{\varphi} - \mathrm{id}_E).$$

On en déduit que $\overrightarrow{u} = \overrightarrow{u}'$ et par conséquent $\psi = \psi'$. □

Pour l'unicité, nous n'avons pas utilisé la condition que ψ et $t_{\overrightarrow{u}}$ commutent. Mais si $\varphi = t_{\overrightarrow{u}} \circ \psi$ et $\overrightarrow{u} \in \ker(\overrightarrow{\varphi} - \mathrm{id}_E)$ alors nécessairement ψ et $t_{\overrightarrow{u}}$ commutent.

Remarque 1.II.16. — Dans la proposition précédente, φ possède un point fixe ssi $\overrightarrow{u} = \overrightarrow{0}$.

Démonstration. — Si $\overrightarrow{u} = 0$ alors $\varphi = \psi$ et φ possède un point fixe. Si φ possède un point fixe, les conditions de la proposition sont satisfaites si on choisit $\psi = \varphi$ et $\overrightarrow{u} = \overrightarrow{0}$, mais ce choix est le seul possible, par l'unicité de ψ et $\overrightarrow{u}$. □

1.II.C. Applications affines et barycentres. — Considérons $\mathcal{E}$ et $\mathcal{F}$ espaces affines.

Proposition 1.II.17. — *Soit $\varphi : \mathcal{E} \to \mathcal{F}$ une application affine. Alors, pour tout choix de $P_1, \dots, P_k$ points de $\mathcal{E}$ et $\lambda_1, \dots, \lambda_k \in \mathbb{K}$ avec $\lambda = \sum_{i=1}^k \lambda_i \neq 0$ on a :*

$$\varphi(\mathrm{Bary}((P_i, \lambda_i)_{i \in [\![1,k]\!]})) = \mathrm{Bary}((\varphi(P_i), \lambda_i)_{i \in [\![1,k]\!]}).$$

Démonstration. — Soit $G = \mathrm{Bary}((P_i, \lambda_i)_{i \in [\![1,k]\!]})$. On a donc :

$$\sum_{i=1}^k \lambda_i \overrightarrow{GP_i} = \overrightarrow{0}.$$

Ainsi, grâce à la linéarité de $\overrightarrow{\varphi}$, on trouve :

$$\sum_{i=1}^k \lambda_i \overrightarrow{\varphi(G)\varphi(P_i)} = \sum_{i=1}^k \lambda_i \overrightarrow{\varphi}(\overrightarrow{GP_i}) = \overrightarrow{0},$$

ce qui exprime $\varphi(G) = \mathrm{Bary}((\varphi(P_i), \lambda_i)_{i \in [\![1,k]\!]})$. □

Théorème 1.II.18. — *Soit $\mathbb{K}$ de caractéristique différente de 2 et soit $\varphi : \mathcal{E} \to \mathcal{F}$ une application telle que, pour tout $\lambda \in \mathbb{K}$ et tout $P, Q \in \mathcal{E}$ on ait:*

$$\varphi(\mathrm{Bary}((P, \lambda), (Q, 1 - \lambda))) = \mathrm{Bary}((\varphi(P), \lambda), (\varphi(Q), 1 - \lambda)).$$

Alors φ est affine.

Démonstration. — Fixons $O \in \mathcal{E}$. Nous définissons $\vec{\varphi}$ par $\vec{\varphi}(\overrightarrow{OP}) = \overrightarrow{\varphi(O)\varphi(P)}$. Il s'agit de montrer que $\vec{\varphi}$ est linéaire. Déjà on a $\varphi(\overrightarrow{OO}) = \vec{0}$.

Montrons d'abord que, si $\lambda \in \mathbb{K}$, on a $\vec{\varphi}(\lambda\overrightarrow{OP}) = \lambda\vec{\varphi}(\overrightarrow{OP})$. On considère

$$G = \mathrm{Bary}((O, 1-\lambda), (P, \lambda)).$$

On a $\overrightarrow{OG} = (1-\lambda)\overrightarrow{OO} + \lambda\overrightarrow{OP} = \lambda\overrightarrow{OP}$ et $\varphi(G) = \mathrm{Bary}((\varphi(O), 1-\lambda), (\varphi(P), \lambda))$. Ainsi:

$$\vec{\varphi}(\lambda\overrightarrow{OP}) = \vec{\varphi}(\overrightarrow{OG}) = \overrightarrow{\varphi(O)\varphi(G)} = (1-\lambda)\overrightarrow{\varphi(O)\varphi(O)} + \lambda\overrightarrow{\varphi(O)\varphi(P)} = \lambda\overrightarrow{\varphi(O)\varphi(P)},$$

donc $\vec{\varphi}(\lambda\overrightarrow{OP}) = \lambda\vec{\varphi}(\overrightarrow{OP})$, comme on voulait.

Vérifions maintenant que, pour tout $P, Q \in \mathcal{E}$, on a $\vec{\varphi}(\overrightarrow{OP} + \overrightarrow{OQ}) = \vec{\varphi}(\overrightarrow{OP}) + \vec{\varphi}(\overrightarrow{OQ}) =$. Comme $\mathbb{K}$ n'est pas de caractéristique 2, on peut considérer:

$$G = \mathrm{Bary}((P, 1/2), (Q, 1/2)),$$

et utiliser :

$$\varphi(G) = \mathrm{Bary}((\varphi(P), 1/2), (\varphi(Q), 1/2)).$$

On a $\overrightarrow{OG} = 1/2\overrightarrow{OP} + 1/2\overrightarrow{OQ}$ et $\overrightarrow{\varphi(O)\varphi(G)} = 1/2\overrightarrow{\varphi(O)\varphi(P)} + 1/2\overrightarrow{\varphi(O)\varphi(Q)}$. En multipliant par 2 et en utilisant que $\vec{\varphi}$ est compatible avec multiplication par un scalaire, on obtient :

$$\vec{\varphi}(\overrightarrow{OP} + \overrightarrow{OQ}) = 2\vec{\varphi}(\overrightarrow{OG}) = \overrightarrow{\varphi(O)\varphi(P)} + \overrightarrow{\varphi(O)\varphi(Q)} = \vec{\varphi}(\overrightarrow{OP}) + \vec{\varphi}(\overrightarrow{OQ}),$$

ce qu'il fallait démontrer. □

1.II.D. Groupe affine. — Soit $\mathcal{E}$ un espace affine de direction E.

1.II.D.1. Groupe linéaire et translations. —

Définition 1.II.19. — Le *groupe affine* $\mathrm{GA}(\mathcal{E})$ est l'ensemble des applications affines inversibles de $\mathcal{E}$ dans $\mathcal{E}$, muni de la loi de composition, avec $\mathrm{id}_{\mathcal{E}}$ comme élément neutre.

Si $\mathcal{E} = \mathbb{K}^n$, on note $\mathrm{GA}(\mathcal{E}) = \mathrm{GA}(n, \mathbb{K})$.

Proposition 1.II.20. — *L'application "partie linéaire" de* $\mathrm{GA}(\mathcal{E})$ *dans* $\mathrm{GL}(E)$ *définie par* $\varphi \mapsto \vec{\varphi}$ *est un morphisme de groupes surjectif, dont le noyau, constitué des translations, est isomorphe à* $(E, +, \vec{0})$.

Démonstration. — L'identité est une transformation affine et la composition de transformations affines l'est aussi, donc $\mathrm{GA}(\mathcal{E})$ est un groupe. Le morphisme qui consiste à prendre la partie linéaire est un morphisme, puisque nous avons vu lors de la remarque 1.II.10 que, si φ et ψ sont transformations affines, $\overrightarrow{\psi \circ \varphi} = \vec{\psi} \circ \vec{\varphi}$ et que $\vec{\mathrm{id}}_{\mathcal{E}} = \mathrm{id}_E$. Le noyau de ce morphisme est constitué des translations, d'après la proposition 1.II.5.

Enfin, le groupe des translation est isomorphe à $(E, +, \vec{0})$ par l'application $\vec{v} \mapsto t_{\vec{v}}$ qui est clairement un isomorphisme de groupes. □

1.II.D.2. Conjugués des translations. —

Remarque 1.II.21. — Soit $\vec{v} \in E$ et $\varphi \in \mathrm{GA}(\mathcal{E})$. Alors

$$\varphi \circ t_{\vec{v}} \circ \varphi^{-1} = t_{\vec{\varphi}(\vec{v})}.$$

Démonstration. — Calculons, pour $P \in \mathcal{E}$:

$$\varphi \circ t_{\vec{v}} \circ \varphi^{-1}(\varphi(P)) = \varphi(P + \vec{v}) = \varphi(P) + \vec{\varphi}(\vec{v}) = t_{\vec{\varphi}(\vec{v})}(\varphi(P)).$$

Ainsi l'égalité cherchée est vraie sur $\varphi(P)$. Comme tout point Q de $\mathcal{E}$ s'écrit $Q = \varphi(P)$, pour $P = \varphi^{-1}(Q)$, l'égalité en question est vraie sur $\mathcal{E}$. □

1.II.D.3. Produit semidirect. — Soit $O \in \mathcal{E}$. Pour $f \in \mathrm{GL}(E)$, nous notons f_O l'application affine de $\mathcal{E}$ dans $\mathcal{E}$ définie par :

$$f_O(P) = O + f(\overrightarrow{OP}).$$

L'application $f \mapsto f_O$ définit un morphisme de groupes $\mathrm{GL}(E) \to \mathrm{GA}(\mathcal{E})$ qui est clairement injectif. On définit aussi le produit semidirect $E \ltimes \mathrm{GL}(E)$ de la façon suivante :

— L'ensemble sous-jacent à $E \ltimes \mathrm{GL}(E)$ est $E \times \mathrm{GL}(E)$.

— L'élément neutre de $E \ltimes \mathrm{GL}(E)$ est $(\vec{0}, \mathrm{id}_E)$.

— Le produit de $(\vec{u}, f)$ et $(\vec{u}, g)$ dans $E \ltimes \mathrm{GL}(E)$ est :

$$(\vec{u}, f) * (\vec{v}, g) = (\vec{u} + f(\vec{v}), f \circ g).$$

— L'inverse de $(\vec{u}, f)$ est $(-f^{-1}(\vec{u}), f^{-1})$.

Le fait que $*$ est une loi associative sera garanti par le théorème suivant.

Théorème 1.II.22. — *Le groupe* $\mathrm{GA}(\mathcal{E})$ *est isomorphe à* $E \ltimes \mathrm{GL}(E)$.

Démonstration. — Commençons par définir une application $\Phi : E \ltimes \mathrm{GL}(E) \to \mathrm{GA}(\mathcal{E})$ par $\Phi(\vec{u}, f) = t_{\vec{u}} \circ f_O$. Nous voulons montrer que Φ est une bijection qui respecte le produit, l'inverse et qui envoie l'identité sur l'identité. On en déduira que le produit $*$ est associatif et que $E \ltimes \mathrm{GL}(E)$ est un groupe, isomorphe à $\mathrm{GA}(\mathcal{E})$.

Soit donc $(\vec{u}, f)$ et $(\vec{u}, g)$ dans $E \ltimes \mathrm{GL}(E)$. On supprime le symbole $\circ$ pour simplifier la notation. On a, d'après la remarque 1.II.21:

$$\begin{aligned}
\Phi(\vec{u}, f)\Phi(\vec{v}, g) &= t_{\vec{u}} f_O t_{\vec{v}} g_O \\
&= t_{\vec{u}} f_O t_{\vec{v}} f_O^{-1} f_O g_O \\
&= t_{\vec{u}} t_{f(\vec{v})} f_O g_O \\
&= t_{\vec{u}+f(\vec{v})} (fg)_O \\
&= \Phi(\vec{u} + f(\vec{v}), fg) = \Phi((\vec{u}, f) * (\vec{v}, g)).
\end{aligned}$$

On voit que $\Phi(\vec{0}, \mathrm{id}_E) = \mathrm{id}_{\mathcal{E}}$ et que Φ respecte les inverses puisque :

$$\Phi(\vec{u}, f)\Phi(-f^{-1}(\vec{u}), f^{-1}) = t_{\vec{u}} f_O t_{-f^{-1}(\vec{u})} f_O^{-1} = t_{\vec{u}} t_{-\vec{u}} = \mathrm{id}_{\mathcal{E}}.$$

L'application Φ est injective. En effet, si $t_{\vec{u}} f_O = t_{\vec{v}} \circ g_O$, alors $t_{\vec{u}} f_O g_O^{-1} = t_{\vec{v}}$ est une translation, ainsi la partie linéaire $f_O g_O^{-1}$ est l'identité, donc $f = g$ et par conséquent $\vec{u} = \vec{v}$.

Enfin, Φ est surjective. En effet, pour $\varphi \in \mathrm{GA}(\mathcal{E})$, on pose $f = \vec{\varphi}$. La partie linéaire de φf_O^{-1} est alors triviale. On a donc $\varphi f_O^{-1} = t_{\vec{u}}$ pour un certain $\vec{u} \in E$, ce qui montre que $\varphi = t_{\vec{u}} f_O$ est dans l'image de Φ. □

Corollaire 1.II.23. — *La partie* G *de* $\mathrm{GA}(\mathcal{E})$ *constituée des compositions d'homothéties et translations est un sous groupe isomorphe à* $E \ltimes \mathbb{K}^*$.

Démonstration. — La partie G contient $\mathrm{id}_{\mathcal{E}}$, est stable par multiplication d'après la remarque 1.II.13 et par inverse puisque, si φ est une homothétie de centre O et rapport $\lambda \in \mathbb{K}^*$, l'inverse de $t_{\vec{u}} \circ \varphi$ est $t_{-1/\lambda \vec{u}} \circ \varphi^{-1}$. C'est donc un sous groupe.

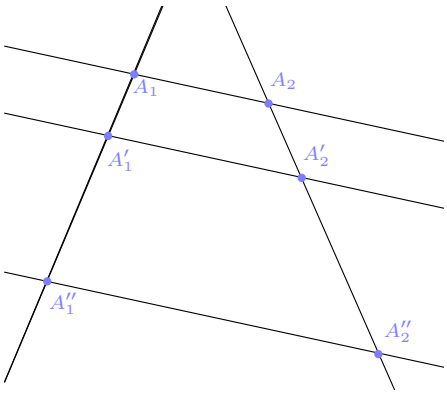
L'isomorphisme Φ se restreint à un isomorphisme entre G et $E \ltimes \mathbb{K}^*$. En effet, puisque $\Phi(t_{\vec{u}}, \varphi) = (\vec{u}, \lambda \mathrm{id}_E)$, l'image $\Phi(G)$ est $E \ltimes \mathbb{K}^* \mathrm{id}_E$ et clairement $\mathbb{K}^* \mathrm{id}_E \simeq \mathbb{K}^*$ en tant groupes multiplicatifs. □

1.II.E. Théorèmes classiques de géométrie affine. — Nous utiliserons la convention suivante. Soit P, Q, R, S points alignés d'un espace affine $\mathcal{E}$. Alors on a $\overrightarrow{PQ} = \lambda \overrightarrow{RS}$ pour un certain $\lambda \in \mathbb{K}$. On écrit alors :

$$\lambda = \frac{PQ}{RS}.$$

On remarque que le scalaire λ, parfois appelé "rapport de mesure algébrique", ne dépend que de la structure affine, autrement dit il n'y a pas besoin de fixer une métrique, ni d'ailleurs que le corps de base soit $\mathbb{R}$, pour parler de ce ratio.

1.II.E.1. Théorème de Thalès. — Considérons un plan affine $\mathcal{E}$. Soit $\mathcal{D}, \mathcal{D}', \mathcal{D}''$ droites parallèles deux à deux distinctes de $\mathcal{E}$ et $\mathcal{L}_1$, $\mathcal{L}_2$, droites distinctes de $\mathcal{E}$ non parallèles à $\mathcal{D}$. Pour $i \in [\![1, 2]\!]$, posons $A_i = \mathcal{D} \cap \mathcal{L}_i$, $A'_i = \mathcal{D}' \cap \mathcal{L}_i$, $A''_i = \mathcal{D}'' \cap \mathcal{L}_i$.



Théorème 1.II.24. — *On a la relation suivante :*

$$\frac{A_1A''_1}{A_1A'_1} = \frac{A_2A''_2}{A_2A'_2}.$$

De plus, étant donné $B \in \mathcal{L}_1$, on a $B = \mathcal{L}_1 \cap \mathcal{D}''$ si:

$$\frac{A_1B''}{A_1A'_1} = \frac{A_2A''_2}{A_2A'_2}.$$

Autrement dit, la relation ci-dessus pour est vérifiée pour $B \in \mathcal{L}_1$ si et seulement si (BA''_2) est parallèle à $\mathcal{D}$.

Démonstration. — Considérons la projection φ de $\mathcal{L}_1$ sur $\mathcal{L}_2$ parallèle à $\mathcal{D}$. La droite affine par A_1 et parallèle à $\mathcal{D}$ étant $\mathcal{D}$, on a $\varphi(A_1) = \mathcal{D} \cap \mathcal{L}_2 = A_2$. De même, $\varphi(A'_1) = A'_2$ et $\varphi(A''_1) = A''_2$. Comme φ est affine, on obtient $\vec{\varphi}(\overrightarrow{A_1A'_1}) = \overrightarrow{A_2A'_2}$ et $\vec{\varphi}(\overrightarrow{A_1A''_1}) = \overrightarrow{A_2A''_2}$.

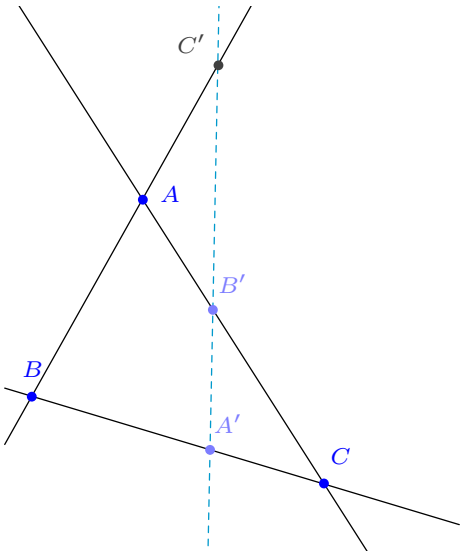
Soit $\lambda \in \mathbb{K}$ tel que $\overrightarrow{A_1A''_1} = \lambda \overrightarrow{A_1A'_1}$. On obtient $\overrightarrow{A_2A''_2} = \vec{\varphi}(\overrightarrow{A_1A''_1}) = \lambda \vec{\varphi}(\overrightarrow{A_1A'_1}) = \lambda \overrightarrow{A_2A'_2}$, ce qu'il fallait démontrer.

Réciproquement, la relation satisfaite par B exprime que $\varphi(B) = A''_2$, donc B se trouve sur la droite par A''_2 et parallèle à $\mathcal{D}$, i.e. sur $\mathcal{D}''$. □

1.II.E.2. Théorème de Ménélaüs. — Soit A, B, C et A', B, C' points deux à deux distincts d'un plan affine $\mathcal{E}$, avec $A' \in (BC)$, $B' \in (AC)$, $C' \in (AB)$.

Théorème 1.II.25. — *Les points A', B', C' sont alignés si et seulement si*

$$\frac{A'B}{A'C}\frac{B'C}{B'A}\frac{C'A}{C'B} = 1.$$



Démonstration. — On considère α, β et γ homothéties de centre A', B' et C', dont les rapports sont définis par les conditions :

$$\alpha(B) = C, \qquad \beta(C) = A, \qquad \gamma(A) = B.$$

On note a, b, c les rapports d'homothétie de α, β, γ :

$$a = \frac{A'B}{A'C}, \qquad b = \frac{B'C}{B'A}, \qquad c = \frac{C'A}{C'B}.$$

L'application affine $\varphi = \beta \circ \alpha \circ \gamma$ est une composition d'homothéties, donc une composition d'une translation et d'une homothétie. Il s'agit en fait d'une homothétie de centre A puisque $\varphi(A) = \beta(\alpha(\gamma(A))) = A$. Ainsi, $\varphi = \mathrm{id}_{\mathcal{E}}$ ssi φ fixe un point de $\mathcal{E}$ autre que A, ou, ce qui est équivalent, une droite de $\mathcal{E}$ ne passant pas par A, par exemple $(A'C')$.

Aussi, le rapport d'homothétie est abc, donc $abc = 1$ ssi $\varphi = \mathrm{id}_{\mathcal{E}}$. L'énoncé est donc réduit à montrer que A', B', C' sont alignés ssi φ fixe $(A'C')$.

Or $(A'C')$ fixée par γ et α, donc elle laissée fixe par φ si et seulement si elle est fixée par β. Or $(A'C')$ est fixée par β si et seulement si A', B', C' sont alignés : si ils sont alignés c'est évident, et réciproquement si la droite est laissée fixe, on doit avoir $\beta(A') \in (A'C')$, et comme $\beta(A') \in (A'B')$, $(A'B') = (A'C')$, i.e. A', B', C' sont aignés. □

1.II.E.3. Théorème de Ceva. —

Théorème 1.II.26. — *Soit A, B, C, A', B', C' comme dans le théorème de Ménélaüs. Alors les droites (AA'), (BB'), (CC') sont concourantes si et seulement si :*

$$\frac{A'B}{A'C}\frac{B'C}{B'A}\frac{C'A}{C'B} = -1.$$

Exercice 1.II.27. — Démontrer le théorème de Ceva.

CHAPITRE 2

GÉOMÉTRIE EUCLIDIENNE

2.I. Espaces euclidiens, rappels

Nous rappelons dans la suite quelques notions de base sur les espaces euclidiens.

2.I.A. Produit scalaire. —

Définition 2.I.1. — Soit E un espace vectoriel réel. Un *produit scalaire* sur E est une forme bilinéaire symétrique définie sur E, dont la forme quadratique associée est définie positive. Si la forme quadratique est seulement positive, on parle d'un *semi-produit* scalaire.

Nous notons souvent $\langle u, v\rangle$ pour le produit scalaire de deux vecteurs $u, v \in E$. On notera $\langle \cdot, \cdot\rangle$ le produit scalaire en tant que application bilinéaire symétrique.

Définition 2.I.2. — Un *espace euclidien* $(E, \langle \cdot, \cdot\rangle)$ est un espace vectoriel E de dimension finie sur $\mathbb{R}$ muni d'un produit scalaire $\langle \cdot, \cdot\rangle$. Si la dimension de E est infinie, on parlera plus en général d'*espace préhilbertiens réel séparé*. La *norme* d'un vecteur u d'un espace préhilbertien réel séparé E, notée $\|u\|$ est $\|u\| = \sqrt{\langle u, u\rangle}$.

Pour un espace vectoriel réel muni d'un semi-produit réel, on parle d'*espace préhilbertiens réel*. On parle dans ce cas de la *semi-norme* de u pour $\sqrt{\langle u, u\rangle}$.

***Exemple 2.I.3* (Produit scalaire canonique)**. — Dans $E = \mathbb{R}^n$, on définit le produit scalaire canonique par:

$$\langle (x_1, \dots, x_n), (y_1, \dots, y_n)\rangle = x_1y_1 + \cdots + x_ny_n.$$

Exemple 2.I.4. — Soit $E = \boldsymbol{M}_n(\mathbb{R})$ et munissons E de la forme bilinéaire symétrique :

$$\langle A, B\rangle = \mathrm{tr}(A^tB),$$

pour toute $A, B \in E$. Alors E est un espace euclidien, de dimension n^2.

Exemple 2.I.5. — Soit E l'espace des fonctions continues, définies sur $[-1, 1]$, à valeurs dans $\mathbb{R}$, et munissons E de la forme bilinéaire symétrique :

$$\langle f_1, f_2\rangle = \int_{-1}^{1} f_1(x)f_2(x)dx$$

pour toute $f, g \in E$. Alors E est un espace préhilbertien réel séparé, de dimension infinie.

Si on considère la même forme bilinéaire symétrique sur l'espace des fonctions intégrables définies sur $[-1, 1]$ à valeurs dans $\mathbb{R}$, on obtient un espace préhilbertien réel qui n'est pas séparé.

2.I.B. Orthogonalité, bases orthonormées. — Soit E un espace préhilbertien réel séparé, muni du produit scalaire $\langle \cdot, \cdot\rangle$.

2.I.B.1. Vecteurs orthogonaux. — Deux vecteurs u, v de E sont *orthogonaux* ssi $\langle u, v\rangle = 0$.

Remarque 2.I.6. — Soit $u \in E$. Si $\langle u, w\rangle = \langle v, w\rangle$ pour tout $w \in E$, alors $u = v$. On a la même conclusion si w varie dans une famille génératrice de E.

Démonstration. — Si $\langle u - v, w\rangle = 0$ pour tout $w \in E$, alors $u - v$ appartient à $E^\perp$. Mais $E^\perp = 0$, car le produit scalaire est non dégénérée. Donc $u = v$. De même, si $\langle u - v, w\rangle = 0$ pour tout w dans une base de E, alors $\langle u - v, w\rangle = 0$ pour tout $w \in E$, ce qui prouve la remarque. □

Remarque 2.I.7. — Soit $(v_1, \ldots, v_\ell)$ des vecteurs orthogonaux non nuls d'un espace euclidien. Alors $(v_1, \ldots, v_\ell)$ sont libres.

Démonstration. — Soit $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ et supposons que la combinaison linéaire $\lambda_1 v_1 + \cdots + \lambda_n v_n$ s'annule. Prenant le produit scalaire entre v_i et cette combinaison linéaire, nous obtenons l'annulation de $\lambda_i \|v_i\|^2$ puisque $v_i \perp v_j$ si $i \neq j$. Comme $v_i \neq 0$ pour tout i, nous en déduisons que $\lambda_i = 0$ pour tout i, autrement dit que la famille en question est libre. □

Le résultat suivant est appelé théorème d'Al-Kashi, ou aussi théorème de Pythagore.

Proposition 2.I.8. — *Soit u, v deux vecteurs de E. Alors on a :*

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2\langle u, v\rangle.$$

En particulier, $\|u + v\|^2 = \|u\|^2 + \|v\|^2$ si et seulement si u et v sont orthogonaux.

Démonstration. — La preuve repose simplement sur la formule $\varphi(u, v) = 1/2(q(u+v) - q(u) - q(v))$, pour la forme bilinéaire φ associée à une forme quadratique q. Ici, nous obtenons:

$$2\langle u, v\rangle = \|u + v\|^2 - \|u\|^2 - \|v\|^2,$$

ce qui implique $\|u+v\|^2 = \|u\|^2 + \|v\|^2 + 2\langle u, v\rangle$. Clairement, $\|u+v\|^2 = \|u\|^2 + \|v\|^2$ ssi $2\langle u, v\rangle = 0$, i. e. ssi $u \perp v$. □

2.I.B.2. Écart angulaire. — Dans un espace muni d'un produit scalaire, nous pouvons définir l'angle entre deux vecteurs. A proprement parler, on peut définir plutôt ce qu'on appelle l'écart angulaire, qui est un angle défini au signe près.

Définition 2.I.9. — Soit u, v deux vecteurs non nuls de E. L'écart angulaire $\widehat{uv} \in [0, \pi]$ est défini par:

$$\widehat{uv} = \arccos\left(\frac{\langle u, v\rangle}{\|u\|\|v\|}\right),$$

donc :

$$\cos(\widehat{uv}) = \frac{\langle u, v\rangle}{\|u\|\|v\|}.$$

En utilisant cette définition, la formule d'Al-Kashi devient:

$$\|u + v\|^2 = \|u\|^2 + \|v\|^2 + 2\cos(\widehat{uv}).$$

Remarque 2.I.10. — Soit $u \perp v$ deux vecteurs de norme 1 de E et $F = \mathrm{vect}(u, v)$. Soit w un vecteur de norme 1 de F. Alors $\cos(\widehat{uw})u$ et $\cos(\widehat{vw})v$ sont les projections orthogonales de w sur les droites $\mathrm{vect}(u)$ et $\mathrm{vect}(v)$.

2.I.B.3. Bases orthogonales et orthonormées. —

Définition 2.I.11. — Une famille $\mathcal{B} = (e_1, e_2, \ldots)$ d'un espace préhilbertien réel séparé est *orthogonale* si $e_i \perp e_j$ pour tout $i \neq j$. Elle est *orthonormée* si de plus $\|e_i\| = 1$ pour tout i.

Proposition 2.I.12. — *Une famille $\mathcal{B} = (e_1, \ldots, e_n)$ d'un espace euclidien E de dimension n est une base orthonormée ssi $\langle e_i, e_j \rangle = \delta_{i,j}$. De plus, tout vecteur $v \in E$ s'écrit:*

$$v = \sum_{i=1,\ldots,n} \langle v, e_i \rangle e_i.$$

Démonstration. — Si $\mathcal{B}$ est une base orthonormée, nous avons $\langle e_i, e_j \rangle = 0$ si $i \neq j$ car dans ce cas $e_i \perp e_j$, et $\langle e_i, e_i \rangle = \|e_i\|^2 = 1$, donc $\langle e_i, e_j \rangle = \delta_{i,j}$.

Réciproquement, si $\langle e_i, e_j \rangle = \delta_{i,j}$, alors $\mathcal{B}$ est une famille libre d'après la Remarque 2.I.7. De plus, nous avons l'orthogonalité entre e_i et e_j pour $i \neq j$, et la normalisation de e_i.

Pour la formule, comparons $\langle v, e_j \rangle$ et le produit scalaire entre $\sum_{i=1,\ldots,n} \langle v, e_i \rangle e_i$ et e_j. Puisque $\langle e_i, e_j \rangle = \delta_{i,j}$, nous obtenons dans les deux cas $\langle v, e_j \rangle$. Donc $v = \sum_{i=1,\ldots,n} \langle v, e_i \rangle e_i$. □

Remarque 2.I.13. — Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base orthonormée et $\mathcal{B}^\vee = (e_1^\vee, \ldots, e_n^\vee)$ sa base duale. Alors pour tout j, $e_j^\vee$ est l'application définie par $v \mapsto \langle v, e_j \rangle$.

Démonstration. — Il suffit de montrer que, pour tout i, j, on a $e_j^\vee(e_i) = \langle e_i, e_j \rangle$. Mais les deux expressions sont égales à $\delta_{i,j}$. □

2.I.B.4. Matrices orthogonales. — Les matrices orthogonales sont celles qui expriment le passage entre deux bases orthonormées.

Définition 2.I.14. — Une matrice M de $\boldsymbol{M}_n(\mathbb{R})$ est *orthogonale* si $M^t M = \mathbb{1}_n$. Ceci est équivalent à ce que M soit inversible, avec $M^{-1} = M^t$, donc équivalent aussi à $MM^t = \mathbb{1}_n$.

Remarque 2.I.15. — Soit $\mathcal{B}$ une base orthonormée d'un espace euclidien E, P un matrice $\boldsymbol{M}_n(\mathbb{R})$ et $\mathcal{C} = \mathcal{B}P$. Alors $\mathcal{C}$ est une base orthonormée si et seulement si P est orthogonale.

Démonstration. — Soit $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{C} = (v_1, \ldots, v_n)$ les deux bases et posons $P = (p_{i,j})_{1 \leq i,j \leq n}$, ainsi:

$$v_j = \sum_{j=1,\ldots,n} p_{i,j} e_i.$$

On calcule alors $\langle v_i, v_k \rangle$ par:

$$\langle v_j, v_k \rangle = \langle \sum_{i=1,\ldots,n} p_{i,j} e_i, \sum_{k=1,\ldots,n} p_{k,h} e_k \rangle = \sum_{i,k=1,\ldots,n} p_{i,j} p_{k,h} \langle e_i, e_k \rangle =$$
$$= \sum_{i,k=1,\ldots,n} p_{i,j} p_{k,h} \delta_{i,k} = \sum_{k=1,\ldots,n} p_{k,j} p_{k,h} = (P^t P)_{j,h}.$$

On en déduit que $P^t P = \mathbb{1}_n$ (i.e., P est orthogonale) si et seulement si $\mathcal{C}$ est une famille orthonormée (i.e., $\mathcal{C}$ est une base orthonormée d'après la proposition 2.I.12). □

2.I.B.5. Algorithme de Gram-Schmidt. —

***Théorème 2.I.16* (Algorithme de Gram-Schmidt)**. — *Soit $\mathcal{B} = (e_1, \ldots, e_n)$ une famille libre dans E. Alors il existe une famille orthonormée $\mathcal{C} = (u_1, \ldots, u_n)$ de E telle que, pour tout $k \leq n$, on ait* $\mathrm{vect}(e_1, \ldots, e_k) = \mathrm{vect}(u_1, \ldots, u_k)$.

Démonstration. — Pour commencer, posons:

$$u_1 = \frac{1}{\|e_1\|} e_1.$$

Nous construisons u_k par récurrence, ayant supposé construits $(u_1, \dots, u_{k-1})$ avec les propriétés souhaitées. De manière similaire à ce que nous faisions lors de la preuve du critère de Sylvester, nous posons:

$$\tilde{u}_k = e_k - \sum_{j=1,\dots,k-1} \langle e_k, u_j \rangle u_j. \tag{3}$$

On calcule alors $\langle u_i, \tilde{u}_k \rangle = 0$ pour $1 \leq i \leq k-1$. En effet, $\langle u_i, u_j \rangle = 0$ si $i \neq j$, donc $\langle u_i, \tilde{u}_k \rangle = \langle e_k, u_i \rangle - \langle e_k, u_i \rangle \|u_i\|^2 = 0$ puisque les u_i sont normalisés à 1 pour $i = 1, \dots, k-1$.

Donc $\tilde{u}_k$ est orthogonale à $u_1, \dots, u_{k-1}$, et nous posons $u_k = 1/\|u_k\| u_k$. Remarquons que cela est bien posé car $\tilde{u_k} \neq 0$, puisque $u_j \in \mathrm{vect}(e_1, \dots, e_{k-1})$ si $j \leq k-1$ donc e_k est indépendant de $u_1, \dots, u_{k-1}$, donc l'expression de $\tilde{u_k}$ garantit $\tilde{u_k} \neq 0$.

Nous avons construit la famille $(u_1, \dots, u_k)$ orthonormée. Comme cette procédure est valide pour tout $k \leq n$, nous avons la famille cherchée $\mathcal{C}$. La famille $\mathcal{C}$ est libre, car la matrice qui exprime $(u_1, \dots, u_n)$ comme combinaison linéaire de $(e_1, \dots, e_n)$ est triangulaire supérieure, avec des 1 sur la diagonale, ce qui est clair d'après l'expression (3), puisque $u_j \in L_{k-1} = \mathrm{vect}(e_1, \dots, e_{k-1})$ pour $j \leq k-1$.

De plus, nous avons $\mathrm{vect}(u_1, \dots, u_k) = \mathrm{vect}(e_1, \dots, e_{k-1}, u_k)$ par hypothèse de récurrence, et cet espace est égale à $\mathrm{vect}(e_1, \dots, e_{k-1}, e_k) = L_k$, puisque u_k s'écrit comme combinaison linéaire de e_k et de $u_1, \dots, u_{k-1}$, i. e. de $e_1, \dots, e_{k-1}$. □

2.I.C. Sous espaces, projections et symétries. — Nous revenons sur les projections dans le cadre des espaces vectoriels quelconques, ensuite nous traitons le cas des projections et des symétries orthogonales. Nous noterons V un espace vectoriel sur un corps $\mathbb{K}$. La lettre E sera réservée à un espace euclidien.

2.I.C.1. Endomorphismes diagonalisables à deux valeurs propres. — Soit V un espace vectoriel sur un corps $\mathbb{K}$ et soit f un endomorphisme de V.

Théorème 2.I.17. — *Soit $\lambda \neq \mu \in \mathbb{K}$. Les conditions suivantes sont équivalentes:*

i) on a $(f - \lambda \mathrm{id}_V) \circ (f - \mu \mathrm{id}_V) = 0$;

ii) on a une décomposition $V = U \oplus W$, avec $f_{|U} = \lambda \mathrm{id}_U$ et $f_{|W} = \mu \mathrm{id}_W$.

On peut dire que f est diagonalisables, ses espaces propres étant U et W, donc ses valeurs propres sont λ et/ou μ, car un des deux espaces U, W pourrait être réduit à 0, auquel cas f est un multiple de l'identité (une homothétie).

Démonstration. — Supposons que $(f - \lambda \mathrm{id}_V) \circ (f - \mu \mathrm{id}_V) = 0$, et posons:

$$U = \ker(f - \lambda \mathrm{id}_V), \qquad W = \ker(f - \mu \mathrm{id}_V).$$

Évidemment, U et W sont des sous espaces vectoriels de V, et nous avons $f_{|U} = \lambda \mathrm{id}_U$ et $f_{|W} = \mu \mathrm{id}_W$.

Montrons que $V = U \oplus W$. D'abord, vérifions $U \cap W = 0$. Soit donc $v \in U \cap W$, i. e. soit v tel que $f(v) = \lambda v$ et $f(v) = \mu v$. On a $(\lambda - \mu)v = 0$, donc $v = 0$ puisque $\lambda \neq \mu$.

Montrons donc que tout vecteur v de V s'écrit comme $u + w$, avec $u \in U$ et $w \in W$. Puisque $\lambda \neq \mu$ nous pouvons poser:

$$u = \frac{1}{\lambda - \mu}(f(v) - \mu v), \qquad w = \frac{1}{\mu - \lambda}(f(v) - \lambda v).$$

On calcule facilement $v = u + w$. Il suffit donc de montrer que $u \in U$ et $w \in W$. Remarquons que $u \in \mathrm{Im}(f - \mu \mathrm{id}_V)$ et que $w \in \mathrm{Im}(f - \lambda \mathrm{id}_V)$. Or l'hypothèse $(f - \lambda \mathrm{id}_V) \circ (f - \mu \mathrm{id}_V) = 0$ fait que $\mathrm{Im}(f - \mu \mathrm{id}_V) \subset \ker(f - \lambda \mathrm{id}_V) = U$, donc $u \in U$. De plus, on a $(f - \mu \mathrm{id}_V) \circ (f - \lambda \mathrm{id}_V) = 0$, car cette composition est $f^2 - (\mu + \lambda) f + \lambda \mu \mathrm{id}_V = (f - \lambda \mathrm{id}_V) \circ (f - \mu \mathrm{id}_V) = 0$ (autrement dit, $(f - \lambda \mathrm{id}_V)$ et $(f - \mu \mathrm{id}_V)$ commutent). Donc $\mathrm{Im}(f - \lambda \mathrm{id}_V) \subset \ker(f - \mu \mathrm{id}_V) = W$, et $w \in W$.

Réciproquement, supposons $V = U \oplus W$ avec $f_{|U} = \lambda \mathrm{id}_U$ et $f_{|W} = \mu \mathrm{id}_W$. Soit v un vecteur de V et montrons $(f-\lambda \mathrm{id}_V)\circ(f-\mu \mathrm{id}_V)(v) = 0$. Nous pouvons écrire $v = u+w$, pour un unique couple de vecteurs $u \in U$ et $w \in W$. On a $(f-\mu \mathrm{id}_V)(v) = (f-\mu \mathrm{id}_V)(u+w) = (f-\mu \mathrm{id}_V)(u)$ car $f_{|W} = \mu \mathrm{id}_W$ donc $f(w) - \mu w = 0$. De nouveau, $(f-\lambda \mathrm{id}_V)$ et $(f-\mu \mathrm{id}_V)$ commutent, donc:

$$(f-\lambda \mathrm{id}_V)\circ(f-\mu \mathrm{id}_V)(v) = (f-\lambda \mathrm{id}_V)\circ(f-\mu \mathrm{id}_V)(u) = (f-\mu \mathrm{id}_V)\circ(f-\lambda \mathrm{id}_V)(u) = 0,$$

car $f_{|U} = \lambda \mathrm{id}_U$ donc $f(u) - \lambda u = 0$. Ceci termine la démonstration. □

2.I.C.2. Projection sur un sous espace parallèle à un supplémentaire. — Soit V un espace vectoriel sur un corps $\mathbb{K}$.

***Définition 2.I.18* (Projection sur U parallèle à W).** — Soit U un sous espace de V et soit W un supplémentaire de U, i. e. $V = U \oplus W$. Un vecteur v de V s'écrit de manière unique comme $u + w$, avec $u \in U$ et $w \in W$. Alors la *projection* π sur U, parallèle à W est définie par :

$$\pi(v) = u.$$

Proposition 2.I.19. — *La projection π est un endomorphisme de V.*

Démonstration. — Clairement π est une application de V dans V, et nous devons montrer qu'elle est linéaire. Soit $v = \lambda_1 v_1 + \lambda_2 v_2$, avec $v_i \in V$ et $\lambda_i \in \mathbb{R}$. Pour $i = 1, 2$, il existe des vecteurs u_i et w_i tels que $u_i \in U$, $w_i \in W$, uniquement déterminés, satisfaisant :

$$v_1 = u_1 + w_1, \qquad v_2 = u_2 + w_2.$$

Alors $v = u + w$ avec $u = \lambda_1 u_1 + \lambda_2 u_2$ et $w = \lambda_1 w_1 + \lambda_2 w_2$ et $u \in U$ et $w \in W$. Donc :

$$\pi(\lambda_1 v_1 + \lambda_2 v_2) = \pi(v) = u = \lambda_1 u_1 + \lambda_2 u_2 = \lambda_1 \pi(v_1) + \lambda_2 \pi(v_2),$$

ce qui prouve que π est linéaire. □

***Proposition 2.I.20* (Caractérisation des projections).** — *Soit f un endomorphisme de V. Les affirmations suivantes sont équivalentes:*

i) f est une projection;

ii) l'endomorphisme f est idempotent, i. e. $f^2 = f$;

iii) on a $V = U \oplus W$ avec $f_{|U} = \mathrm{id}_U$ et $f_{|W} = 0$.

Si ces conditions sont vérifiées, f est la projection sur $U = \mathrm{Im}(f)$ parallèle à $W = \ker(f)$.

Démonstration. — Grâce au Théorème 2.I.17, nous avons l'équivalence entre (ii)) et (iii)). En effet, la condition (ii)) s'écrit $f(f - \mathrm{id}_V) = 0$.

Montrons que (i)) implique (iii)). Soit donc f est une projection, disons une projection sur U parallèle à W, ainsi $V = U \oplus W$. Alors, pour $v \in V$, on écrit de manière unique $v = u+w$, avec $u \in U$ et $w \in W$, et $f(v) = u$. Or $v \in V$ implique $w = 0$ donc $f(v) = f(u) = u$, et $f_{|U} = \mathrm{id}_U$. Par contre, $v \in W$ implique $u = 0$ donc $f(v) = f(w) = 0$, et $f_{|W} = 0$. Nous avons montré (iii)).

Réciproquement, supposant valide (iii)), nous avons $V = U \oplus W$, avec $f_{|U} = \mathrm{id}_U$ et $f_{|W} = 0$, et pour $v \in V$, on écrit de manière unique $v = u + w$, avec $u \in U$ et $w \in W$. On calcule $f(v) = f(u+w) = u$ puisque $f(w) = 0$ et $f(u) = u$. Il en résulte que f est la projection sur U parallèle à W, et nous avons (i)).

Si ces conditions sont vérifiées, nous avons $V = U \oplus W$, avec $f_{|U} = \mathrm{id}_U$ et $f_{|W} = 0$. Nous avons vu que f est la projection sur U parallèle à W, donc il suffit de montrer que $U = \mathrm{Im}(f)$ et $W = \ker(f)$. Clairement $W \subset \ker(f)$ car $f_{|W} = 0$. Mais, pour tout $v \in V$, en écrivant $v = u + w$ avec $u \in U$ et $w \in W$, on a $f(v) = u$. Alors $f(u) = 0$ implique $u = 0$, donc $\ker(f) \subset W$, et nous obtenons $\ker(f) = W$. De même, $U \subset \mathrm{Im}(f)$ car $f_{|U} = \mathrm{id}_U$, et $f(v) = u$ implique $\mathrm{Im}(f) \subset U$ donc $U = \mathrm{Im}(f)$. □

2.I.C.3. Sous espaces euclidiens et projections orthogonales. — Soit E un espace préhilbertien réel séparé, muni du produit scalaire $\langle\cdot,\cdot\rangle$.

Proposition 2.I.21. — *Soit F un sous espace vectoriel de E. Alors F est un espace préhilbertien séparé, muni du produit scalaire induit par restriction.*

Démonstration. — La restriction du produit scalaire à F est bien sûr une forme bilinéaire symétrique, positive car $\langle v,v\rangle \geq 0$ pour tout $v \in E$ (en particulier pour tout $v \in F$) et en fait définie positive, puisque $\langle v,v\rangle = 0$ implique $v = 0$ dans E, et en particulier dans F. Donc, F est un espace préhilbertien séparé réel. □

Lorsque F est de dimension finie, d'après la proposition suivante on a toujours $E = F \oplus F^\perp$, et nous pouvons écrire la formule de la projection orthogonale π_F.

Définition 2.I.22. — Soit F un sous espace de E, tel que $E = F \oplus F^\perp$. La *projection orthogonale* π_F est définie comme la projection sur F, parallèle à $F^\perp$.

Théorème 2.I.23. — *Soit F un sous espace de dimension finie d'un espace préhilbertien séparé. Alors nous avons $E = F \oplus F^\perp$. De plus, si $(e_1,\dots,e_n)$ est une base orthonormée de F, alors π_F s'écrit :*

$$\pi_F(v) = \sum_{i=1,\dots,n} \langle v, e_i\rangle e_i.$$

Démonstration. — Si F est de dimension finie, disons $\dim(F) = n$, nous pouvons choisir une base orthonormée $(e_1,\dots,e_n)$ de F (une telle base existe d'après le chapitre 2.I.

L'application suivante est un endomorphisme de E :

$$\xi : E \to E, \qquad v \mapsto \sum_{i=1,\dots,n} \langle v, e_i\rangle e_i,$$

ce que l'on vérifie immédiatement grâce à la linéarité du produit scalaire en la première variable, une fois fixée la deuxième.

Montrons que ξ est la projection orthogonale de E sur F, parallèle à $F^\perp$. Cela implique, bien entendu, que $E = F \oplus F^\perp$. Pour montrer que ξ est une projection, on peut vérifier que $\xi^2 = \xi$, ce qui vient de la formule:

$$\begin{aligned}
\xi^2(v) = \xi(\xi(v)) &= \sum_{i=1,\dots,n} \langle \xi(v), e_i\rangle e_i = \\
&= \sum_{i=1,\dots,n} \langle \sum_{j=1,\dots,n} \langle v, e_j\rangle e_j, e_i\rangle e_i = \\
&= \sum_{i,j=1,\dots,n} \langle v, e_j\rangle \langle e_j, e_i\rangle e_i = \\
&= \sum_{i,j=1,\dots,n} \langle v, e_j\rangle \delta_{i,j} e_i = \sum_{i=1,\dots,n} \langle v, e_i\rangle e_i = \xi(v).
\end{aligned}$$

Si v est un vecteur de E, évidemment $\xi(v)$ appartient à F donc $\mathrm{Im}(\xi) \subset F$. De plus, $\xi(e_i) = e_i$ donc $\xi_{|F} = \mathrm{id}_F$, donc $\mathrm{Im}(f) = F$. De plus, si $v \in F^\perp$ alors $\xi(v) = 0$ car $v \perp e_i$ pour tout i. Finalement, si $v \in \ker(\xi)$ on a $\sum_{i=1,\dots,n}\langle v, e_i\rangle e_i = 0$ donc $\langle v, e_i\rangle = 0$ pour tout i puisque les e_i sont libres, donc $v \in F^\perp$ puisque les e_i engendrent F. On en obtient que $\ker(\xi) = F^\perp$, donc ξ est bien la projection sur F, parallèle à $F^\perp$. □

2.I.D. Projection orthogonale sur une droite. — Soit E un espace préhilbertien réel séparé, et soit $0 \neq u$ un vecteur de E. La droite $L = \mathrm{vect}(u)$ est formée par le vecteurs de la forme λu, où λ varie dans $\mathbb{R}$.

La projection orthogonale π_L prend la forme:

$$\pi_L(v) = \frac{\langle v, u\rangle}{\|u\|^2} u.$$

En coordonnées, si $\mathcal{B} = (e_1, \dots, e_n)$ est une base orthonormée d'un espace euclidien E et L est une droite engendrée par le vecteur $u = y_1 e_1 + \cdots + y_n e_n$, alors π_L prend la forme:

$$\pi_L(x_1 e_1 + \cdots + x_n e_n) = \frac{\sum_{j=1}^n x_j y_j}{\sum_{j=1}^n y_j^2} \sum_{i=1}^n y_i e_i.$$

2.I.E. Projection orthogonale sur un hyperplan. — Soit E un espace euclidien, et H un hyperplan de E, autrement dit un sous espace vectoriel de codimension 1 dans E. Alors H est défini par une équation donnée par une forme linéaire $f \in E^\vee$:

$$H = \{v \in E \,|\, f(v) = 0\}.$$

Supposons avoir fixé une base orthonormée $\mathcal{B}$ de E et sa base duale $\mathcal{B}^\vee$. Soit $f = a_1 e_1^\vee + \cdots + a_n e_n^\vee$. L'orthogonal de H est alors la droite engendrée par le vecteur $n_H = (a_1 e_1 + \cdots + a_n e_n)$, que nous pouvons penser comme un vecteur normal de H.

$$H^\perp = \mathrm{vect}(n_H).$$

En effet, il suffit de montrer que:

$$n_H^\perp = H,$$

ce qui est clair puisque, si $v = x_1 e_1 + \cdots + x_n e_n$, on a:

$$\langle n_H, v \rangle = a_1 x_1 + \cdots + a_n x_n = f(v),$$

donc $v \in H$ ssi $f(v) = 0$ ssi $v \perp n_H$.

La projection orthogonale π_H prend la forme:

$$\pi_H(x_1 e_1 + \cdots + x_n e_n) = \sum_{i=1,\dots,n} \left(1 - \frac{a_i}{\sum_{j=1}^n a_j^2}\right) x_i e_i.$$

2.I.E.1. Symétrie relative à un sous espace, parallèle à un supplémentaire. — Soit V un espace vectoriel sur un corps $\mathbb{K}$.

***Définition 2.I.24* (Symétrie relative à U parallèle à W).** — Soit U un sous espace de V et soit W un supplémentaire de U, i. e. $V = U \oplus W$. Un vecteur v de V s'écrit de manière unique comme $u + w$, avec $u \in U$ et $w \in W$. La *symétrie σ par rapport à U et parallèle à W* est définie par par :

$$\sigma(v) = u - w.$$

On dira aussi que *U est l'axe* de σ.

Nous avons que les symétries sont des applications involutives, ce qui par définition veut dire que, appliquées deux fois, donnent l'identité.

Proposition 2.I.25. — *La symétrie σ par rapport à un sous espace est un endomorphisme involutif de V.*

Démonstration. — Bien entendu, σ est une application de V dans V. Le même argument utilisé pour montrer la Proposition 2.I.19 peut être utilisé pour prouver que σ est linéaire. De plus, on montre directement de la formule $\sigma(u) = u' - u''$ que $\sigma(\sigma(u)) = u' + u'' = u$, donc:

$$\sigma^2 = \mathrm{id}_V, \qquad \text{donc } \sigma = \sigma^{-1},$$

ce qui dit que σ est involutive. □

***Proposition 2.I.26* (Caractérisation des symétries).** — *Soit f un endomorphisme de V. Le affirmations suivantes sont équivalentes:*

i) f est une symétrie;

ii) f est une involution, i. e. $f^2 = \mathrm{id}_V$;

iii) on a $V = U \oplus W$ avec $f_{|U} = \mathrm{id}_U$ et $f_{|W} = -\mathrm{id}_W$.

Si ces conditions sont vérifiées, alors f est la symétrie d'axe $\ker(f-\mathrm{id}_V)$*, parallèle à* $\ker(f+\mathrm{id}_V)$.

Démonstration. — L'équivalente entre (ii)) et (iii)) est claire d'après le Théorème 2.I.17, puisque la condition (ii)) s'écrit $f^2-\mathrm{id}_V=0$, ce qui équivaut à $(f+\mathrm{id}_V)\circ(f-\mathrm{id}_V)=0$.

La proposition précédente montre que (i)) implique (ii)). De plus, si (iii)) est valide, alors $V=U\oplus W$, ainsi un vecteur u de V s'écrit uniquement comme $v=u+w$ avec $u\in U$ et $w\in W$. Nous avons alors $f(v)=f(u)+f(w)=u-w$ puisque $f_{|U}=\mathrm{id}_U$ et $f_{|W}=-\mathrm{id}_W$, donc f est la symétrie par rapport à U, parallèle à W, et nous avons (i)).

Pour montrer le dernier énoncé, remarquons que si $u\in U$ alors $f(u)=u$ donc $U\subset\ker(f-\mathrm{id}_V)$. Pour l'autre inclusion, pour tout $v\in V$, nous écrivons uniquement v comme $u+w$ avec $u\in U$ et $w\in W$, et $f(v)=u-w$. Donc $v\in\ker(f-\mathrm{id}_V)$ implique $f(v)=v$, ce qui entraîne $u+w=u-w$ donc $w=0$. Ainsi $v\in U$ et $\ker(f-\mathrm{id}_V)\subset U$.

De même, si $w\in W$ alors $f(w)=-w$ donc $W\subset\ker(f+\mathrm{id}_V)$. Pour l'autre inclusion, soit $v\in V$ sous la forme $u+w$ avec $u\in U$ et $w\in W$, ainsi $f(v)=u-w$, et supposons $v\in\ker(f+\mathrm{id}_V)$. Alors $f(v)=-v$, ce qui implique $u-w=-u-w$ donc $u=0$. Ainsi $v\in W$ et $\ker(f+\mathrm{id}_V)\subset W$. □

2.I.E.2. Symétries orthogonales. — Soit maintenant E un espace euclidien, muni du produit scalaire $\langle\cdot,\cdot\rangle$. Étant donné un sous espace F de E, nous avons $E=F\oplus F^\perp$.

Définition 2.I.27. — La *symétrie orthogonale* σ_F est définie comme la symétrie par rapport à F, parallèle à $F^\perp$.

Proposition 2.I.28. — *Soit F un sous espace de dimension k de E, et soit $(e_1,\dots,e_n)$ une base orthonormée de E avec $e_i\in F$ ssi $i\leq k$. Alors la symétrie orthogonale σ_F s'écrit:*

$$\sigma_F(v)=\sum_{i=1,\dots,k}\langle v,e_i\rangle e_i-\sum_{i=k+1,\dots,n}\langle v,e_i\rangle e_i.$$

Démonstration. — Montrons que:

$$\sigma_F=\pi_F-\pi_{F^\perp}.$$

En effet, si $u\in F$, on a $\sigma_F(u)=u=\pi_F(u)=\pi_F-\pi_{F^\perp}(u)$. Si $w\in F^\perp$, on a $\sigma_F(w)=-w=-\pi_{F^\perp}(w)=\pi_F-\pi_{F^\perp}(w)$. Puisque $F=U\oplus V$, et σ_F coïncide avec $\pi_F-\pi_{F^\perp}$ sur U et sur W, on a $\sigma_F=\pi_F-\pi_{F^\perp}$.

D'après le Théorème 2.I.23 nous avons $\pi_F(v)=\sum_{i=1,\dots,k}\langle v,e_i\rangle e_i$. De manière analogue, on obtient $\pi_{F^\perp}(v)=\sum_{i=k+1,\dots,n}\langle v,e_i\rangle e_i$. Donc:

$$\sigma_F(v)=\pi_F(v)-\pi_{F^\perp}(v)=\sum_{i=1,\dots,k}\langle v,e_i\rangle e_i-\sum_{i=k+1,\dots,n}\langle v,e_i\rangle e_i.$$

□

Définition 2.I.29. — On parle de *réflexion orthogonale* si F est un hyperplan. On parle de *renversement* si F a codimension 2.

2.II. Automorphismes orthogonaux

Fixons E un espace euclidien.

2.II.A. Isométries vectorielles. —

2.II.A.1. Isométries vectorielles linéaires. —

Définition 2.II.1. — Soit F un espace euclidien. Une *isométrie vectorielle* est une application $f : E \to F$ avec $f(0) = 0$ et telle que, pour tout $u, v \in E$, on ait $\|u-v\|_E = \|f(u)-f(v)\|_F$.

Proposition 2.II.2. — *. Une isométrie vectorielle est un isomorphisme linéaire sur son image et respecte le produit scalaire.*

Démonstration. — Pour commencer, on a f est injective, car si $u, v \in E$ satisfont $f(u) = f(v)$ alors $\|f(u) - f(v)\| = \|u - v\| = 0$ donc $u = v$. Aussi, f respecte la norme car, pour tout $u \in E$, on a $\|f(u)\| = \|f(u) - f(0)\| = \|u\|$.

Montrons que f respecte le produit scalaire. On a, pour tout $u, v \in E$:

$$\langle f(u), f(v)\rangle = \frac{1}{2}(\|f(u)\|^2 + \|f(v)\|^2 - \|f(u) - f(v)\|^2) = \frac{1}{2}(\|u\|^2 + \|v\|^2 - \|u - v\|^2) = \langle u, v\rangle.$$

Fixons $\mathcal{B} = (e_1, \ldots, e_n)$ base orthonormée de E et posons $u_i = f(e_i)$. Comme f respecte le produit scalaire, la famille $(u_1, \ldots, u_n)$ est aussi orthonormée, donc libre, donc une base de l'espace vectoriel engendré par l'image de F. Ainsi, si on montre que f est linéaire, la proposition sera démontrée.

Pour montrer que f est linéaire, il suffit de voir que, pour tout $i, j \in [\![1, n]\!]$ avec $i \neq j$, si $\lambda \in \mathbb{R}$, alors $f(\lambda e_i) = \lambda u_i$ et que $f(e_i + e_j) = u_i + u_j$. On a $f(\lambda e_i) \perp u_j$ pour tout $j \neq i$, donc $f(\lambda e_i) = \mu u_i$ pour un certain $\mu \in \mathbb{R}$. Mais $\lambda = \langle \lambda e_i, e_i\rangle = \langle \mu u_i, u_i\rangle = \mu$ dit $\lambda = \mu$. Enfin $f(e_i + e_j)$ appartient à $\mathrm{vect}(u_i, u_j)$ donc on écrit $f(e_i + e_j) = \lambda u_i + \mu u_j$ pour certains $\lambda, \mu \in \mathbb{R}$. Ensuite, on trouve :

$$\lambda = \langle \lambda u_i + \mu u_j, u_i\rangle = \langle f(e_i + e_j), u_i\rangle = \langle f(e_i + e_j), f(e_i)\rangle = \langle e_i + e_j, e_i\rangle = 1,$$

donc $\lambda = 1$. De même, $\mu = 1$, donc f est linéaire. □

2.II.A.2. Automorphismes orthogonaux. —

Définition 2.II.3. — Un endomorphisme de E qui est une isométrie vectorielle est appelé un *automorphisme orthogonal*.

Remarque 2.II.4. — Les valeurs propres d'un automorphisme orthogonal ont module 1.

Démonstration. — Fixons une base orthonormée $\mathcal{B}$ de E. Soit $\lambda \in \mathbb{C}$ une valeur propre de f automorphisme orthogonal et soit $Z \in \mathbb{C}^n \setminus \{0\}$ tel que $MZ = \lambda Z$, où $M = \mathrm{Mat}_{\mathcal{B}}(f)$. On a :

$$\|Z\|^2 = \langle Z, Z\rangle = \langle MZ, MZ, =\rangle\langle \lambda Z, \lambda Z\rangle = |\lambda|^2\|Z\|^2.$$

Donc $|\lambda| = 1$. □

2.II.B. Automorphismes orthogonaux et matrices orthogonales. —

Théorème 2.II.5. — *Soit f un endomorphisme de E. Alors les conditions suivantes sont équivalentes:*

i) f est orthogonal;

ii) pour toute base orthonormée $\mathcal{B}$ de E, on a que $f(\mathcal{B})$ est une base orthonormée;

iii) il existe une base orthonormée $\mathcal{B}$ de E telle que $f(\mathcal{B})$ est une base orthonormée;

iv) f est isométrique.

Démonstration. — Montrons que (i)) implique (ii)), donc soit f est orthogonal et soit $\mathcal{B} = (e_1, \ldots, e_n)$ une base orthonormée de E. Nous avons, pour tout $u, v \in E$, $\langle f(u), f(v)\rangle = \langle u, v\rangle$, en particulier $\langle f(e_i), f(e_j)\rangle = \langle e_i, e_j\rangle$ donc $f(\mathcal{B})$ est une famille orthonormée de n vecteurs, donc une base orthonormée.

Il est évident que (ii)) implique (iii)), car nous avons prouvé que E admet une base orthogonale.

Pour voir que (iii)) implique (iv)), nous considérons une base orthonormée $\mathcal{B} = (e_1, \dots, e_n)$ telle que $f(\mathcal{B})$ est orthonormée, et nous calculons $\|f(v)\|$ en coordonnées. Nous avons $v = x_1e_1 + \cdots + x_ne_n$, pour un certain vecteur colonne $X = (x_1, \dots, x_n)^t$. Comme $\mathcal{B}$ est orthonormée, on a $\|v\|^2 = x_1^2 + \cdots + x_n^2$. De plus, $f(v) = x_1f(e_1) + \cdots + x_nf(e_n)$ donc $\|f(v)\|^2 = x_1^2 + \cdots + x_n^2$ puisque $f(\mathcal{B}) = (f(e_1), \dots, f(e_n))$ est une base orthonormée. Donc f est une isométrie.

Enfin, montrons que (iv)) implique (i)), i. e. qu'un endomorphisme isométrique est orthogonal. Étant donnés $u, v \in E$, on sait:

$$\langle u, v\rangle = \frac{1}{2}\left(\|u+v\|^2 - \|u\|^2 - \|v\|^2\right),$$

et de même $\langle f(u), f(v)\rangle = 1/2(\|f(u+v)\|^2 - \|f(u)\|^2 - \|f(v)\|^2)$. Donc si $\|f(w)\| = \|w\|$ pour tout $w \in E$, les trois termes de $\|u+v\|^2 - \|u\|^2 - \|v\|^2$ coïncident un par un avec les trois termes de $\|f(u+v)\|^2 - \|f(u)\|^2 - \|f(v)\|^2$, donc $\langle u, v\rangle = \langle f(u), f(v)\rangle$. □

2.II.C. Sphères. —

Remarque 2.II.6. — Les orbites de $\mathrm{SO}(E)$ sont les sphères constituées des vecteurs de norme r, pour $r \in [0, +\infty[$.

Démonstration. — Soit $u \in E$. Comme f préserve la norme, si $\|u\| = r$ alors $\|f(u)\| = r$ donc l'orbite de u est contenue dans la sphère de centre 0 et rayon r. Aussi, si v appartient à cette sphère, on peut compléter u puis v à deux bases orthonormées de E, $(u, u_2, \dots, u_n)$ et $(v, v_2, \dots, v_n)$, puis envoyer u sur v et u_i sur v_i pour se rendre compte que v est dans l'orbite de u. □

Remarque 2.II.7. — Soit $k \leq n$. Le groupe $\mathrm{SO}(E)$ opère transitivement sur l'ensemble des sous espaces de E de dimension k.

Démonstration. — Soit F et F' deux sous espaces de dimension k de E. On choisit des bases orthonormées $(e_1, \dots, e_n)$ et $(e'_1, \dots, e'_n)$ de E de sorte que $e_1, \dots, e_k \in F$ et $e'_1, \dots, e'_k \in F'$ puis on définit f par $f(e_i) = e'_i$. On a $f \in \mathrm{O}(E)$, et quitte à remplacer e'_1 par e'_1, on peut obtenir $f \in \mathrm{SO}(E)$. En tout cas, $f(F) = F'$. □

Lemme 2.II.8. — *Soit E un $\mathbb{K}$-espace vectoriel, $f, g \in \mathrm{GL}(E)$ et $F = \mathrm{Fix}(g)$. Alors* $\mathrm{Fix}(fgf^{-1}) = f(F)$.

Démonstration. — Soit $u \in E$ et $v = f^{-1}(u)$ de sorte que $u = f(v)$. On a $u \in f(F)$ ssi $v \in F$. Dans ce cas on trouve $fgf^{-1}(f(v)) = f(g(v)) = f(v)$ i.e. $u \in \mathrm{Fix}(fgf^{-1})$. Et réciproquement si $fgf^{-1}(f(v)) = f(v)$ alors $g(v) = v$ donc $v \in \mathrm{Fix}(g)$ et $u \in f(F)$. □

Corollaire 2.II.9. — *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. Si $f \in \mathrm{GL}(E)$ laisse fixe toute droite, f est une homothétie.*

Démonstration. — Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E. Si f laisse fixe toute droite, pour tout $i \in [\![1, n]\!]$ on a $f(e_i) = \lambda e_i$, pour certains scalairs $\lambda_1, \dots, \lambda_n \in \mathbb{K}^*$. Mais il existe $\lambda \in \mathbb{K}^*$ tel que $f(e_1 + \cdots + e_n) = \lambda(e_1 + \cdots + e_n)$. Donc $\lambda(e_1 + \cdots + e_n) = \lambda_1e_1 + \cdots + \lambda_ne_n$, ainsi $\lambda_i = \lambda$ pour tout $i \in [\![1, n]\!]$. Ainsi f est une homothétie. □

Interlude : orientation. — Soit E un $\mathbb{R}$-espace vectoriel de dimension $0 < n < \infty$. Etant donnée deux bases $\mathcal{B}$ et $\mathcal{B}'$ de E, leur matrice de transition P a déterminant $\det(P)$ qui est positif ou négatif, strictement.

Définition 2.II.10. — On dit que $\mathcal{B}$ et $\mathcal{B}'$ ont *même orientation* si $\det(P) > 0$, ou *orientations opposées* si $\det(P) < 0$.

Le fait d'avoir même orientation est une relation d'équivalence sur l'ensemble des bases de E. Une *orientation* sur E est une classe d'équivalence cette relation d'équivalence. On dit que E est orienté si on fixe une orientation sur E. Une base de E orienté est *positive* si elle est dans la classe d'équivalence fixée par l'orientation, autrement elle est *négative*.

Définition 2.II.11. — Soit $\mathcal{B}$ une base de E. On dit que $f \in \mathrm{GL}(E)$ est *direct* si $\det(\mathrm{Mat}_{\mathcal{B}}(f)) > 0$, *indirect* sinon.

Si $\mathcal{B} = (e_1, \ldots, e_n)$ et $\mathcal{B}' = (e'_1, \ldots, e'_n)$ est une autre base de E, l'automorphisme f défini par $f(e_i) = e'_i$ est direct si et seulement si $\mathcal{B}'$ et $\mathcal{B}$ ont même orientation.

2.II.D. Automorphismes orthogonaux du plan. — Dans cette section, E est un espace euclidien de dimension 2.

2.II.D.1. Matrices orthogonales de taille 2. — Étudions les matrices orthogonales de taille 2, donc les automorphismes orthogonaux de E.

Proposition 2.II.12. — *Soit f un automorphisme orthogonal de E, soit $\mathcal{B} = (e_1, e_2)$ une base orthonormée de E, et posons $M = \mathrm{Mat}_{\mathcal{B}}(f)$. Alors M est de l'une des deux formes $M = R_\vartheta$ ou $M = \check{R}_\vartheta$:*

$$R_\vartheta = \begin{pmatrix} \cos(\vartheta) & -\sin(\vartheta) \\ \sin(\vartheta) & \cos(\vartheta) \end{pmatrix}, \qquad \text{et} \qquad \check{R}_\vartheta = \begin{pmatrix} \cos(\vartheta) & \sin(\vartheta) \\ \sin(\vartheta) & -\cos(\vartheta) \end{pmatrix}.$$

pour un certain $\vartheta \in [0, 2\pi[$. La forme R_ϑ se produit ssi $\det(M) = 1$, et la forme $\check{R}_\vartheta$ ssi $\det(M) = -1$.

Démonstration. — Soit $M = \mathrm{Mat}_{\mathcal{B}}(f)$ la matrice:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

De la relation $M^t M = \mathbb{1}_2$, nous obtenons:

$$a^2 + c^2 = b^2 + d^2 = 1, \qquad ab + cd = 0,$$

donc il existent deux nombres réels ϑ, φ tels que:

$$a = \cos(\vartheta), \quad b = \sin(\vartheta), \quad c = \cos(\varphi), \quad d = \sin(\varphi).$$

Il s'en suit que:

$$ab + cd = \cos(\vartheta - \varphi) = 0,$$

donc $\vartheta - \varphi = \pi/2 + k\pi$, avec $k \in \mathbb{Z}$.

$$k \text{ pair} \Longrightarrow \begin{cases} c = \cos(\varphi) = \sin(\vartheta) = b \\ d = \sin(\varphi) = -\cos(\vartheta) = -a \end{cases}$$

$$k \text{ impair} \Longrightarrow \begin{cases} c = \cos(\varphi) = -\sin(\vartheta) = -b \\ d = \sin(\varphi) = \cos(\vartheta) = a \end{cases}$$

Nous avons donc obtenu les deux formes possibles R_ϑ et $\check{R}_\vartheta$. Il est clair qu'elles sont caractérisées par le signe de $\det(M)$. □

2.II.D.2. Rotations du plan orienté. — Supposons que, dans la base orthonormée $\mathcal{B} = (e_1, e_2)$, on ait $\mathrm{Mat}_{\mathcal{B}}(f) = R_\vartheta$ avec $\vartheta \in]0, \pi[\cup]\pi, 2\pi[$. Alors $\vartheta' = 2\pi - \vartheta$ appartient encore à $]0, \pi[\cup]\pi, 2\pi[$, et nous pouvons définir la base $\mathcal{B}' = (e_1, -e_2)$. On a $\mathrm{Mat}_{\mathcal{B}'}(f) = R_{-\vartheta} = R_{\vartheta'}$. C'est la seule ambiguïté dans la définition de ϑ, qui disparaît si nous considérons E orienté.

Soit donc E orienté.

Remarque 2.II.13. — Soit f un automorphisme orthogonal direct de E. Alors il existe un unique $\vartheta \in [0, 2\pi[$ tel que, pour toute base orthonormée positive $\mathcal{B}$ de E, on ait $M_{\mathcal{B}}(f) = R_\vartheta$.

Démonstration. — Soit $\mathcal{B}$ une base orthonormée positive de E et $M = \mathrm{Mat}_{\mathcal{B}}(f)$. Puisque f est direct, on a $\det(M) = 1$, et il existe $\vartheta \in [0, 2\pi[$ tel que $M = R_\vartheta$.

Pour l'unicité. Les valeurs propres λ, μ de M, vue comme matrice complexe, satisfont :

$$\lambda\mu = 1, \qquad \lambda + \mu = 2\cos(\vartheta).$$

Donc on a :

$$\lambda = \cos(\vartheta) + i\sin(\vartheta), \qquad \mu = \cos(\vartheta) - i\sin(\vartheta).$$

Pour toute base orthonormée $\mathcal{B}'$ de E il existe $\vartheta' \in [0, 2\pi[$ tel que $\mathrm{Mat}_{\mathcal{B}'}(f) = R_{\vartheta'}$, et nous avons $\cos(\vartheta) = \cos(\vartheta')$ par égalité des traces de R_ϑ et $R_{\vartheta'}$, donc $\vartheta' = \vartheta$ ou $\vartheta' = 2\pi - \vartheta$.

Nous voulons montrer que, si $\mathcal{B}'$ est positive, $\vartheta' = \vartheta$. Nous pouvons supposer $\vartheta \neq 0, \pi$, et nous voulons montrer que $\vartheta' = 2\pi - \vartheta$ implique que $\mathcal{B}'$ est négative. Soit P la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. On écrit:

$$P = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad PR_{2\pi-\vartheta} = R_\vartheta P.$$

Nous obtenons, en développant : $b = c$ et $a = -d$. Donc P devient:

$$P = \begin{pmatrix} a & b \\ b & -a \end{pmatrix} \quad \Rightarrow \quad \det(P) = -a^2 - b^2 < 0,$$

ainsi $\mathcal{B}'$ est négative. □

Définition 2.II.14. — Si f est un automorphisme orthogonal d'un plan euclidien orienté, on dit que f est une *rotation d'angle* ϑ si, lorsque $\mathcal{B}$ est une base orthonormée positive de E, on a:

$$M_{\mathcal{B}}(f) = R_\vartheta = \begin{pmatrix} \cos(\vartheta) & -\sin(\vartheta) \\ \sin(\vartheta) & \cos(\vartheta) \end{pmatrix}.$$

La remarque précédente dit que la définition de rotation est bien posée.

Proposition 2.II.15. — *Soit E orienté, f un automorphisme orthogonal de E, $\mathcal{B} = (e_1, e_2)$ une base orthonormée positive de E et $M = \mathrm{Mat}_{\mathcal{B}}(f)$. Alors:*

i) l'automorphisme f est une rotation d'angle $\pm\vartheta$ ssi:

$$\det(M) = 1, \qquad \mathrm{tr}(M) = 2\cos(\vartheta);$$

ii) l'automorphisme f est une réflexion orthogonale ssi :

$$\det(M) = -1;$$

iii) l'automorphisme f est diagonalisables ssi f est indirect ou si f est une rotation d'angle 0 ou π.

Démonstration. — Nous savons que f est direct ssi $\det(M) = 1$ ssi f est une rotation d'angle ϑ, pour un certain $\vartheta \in [0, 2\pi[$. Ensuite, si f est une rotation d'angle ϑ, on calcule $\mathrm{tr}(R_\vartheta) = 2\cos(\vartheta)$ donc une implication de (i)) est prouvée. Réciproquement, si $\det(M) = 1$ alors $M = R_\varphi$ pour un certain $\varphi \in [0, 2\pi[$, et $\mathrm{tr}(M) = 2\cos(\vartheta) = 2\cos(\varphi)$ implique $\vartheta = \pm\varphi$.

Montrons (ii)). Clairement, si f une réflexion orthogonale, alors f est indirect donc $\det(f) = -1$. Ce que nous devons montrer, c'est l'autre implication, donc soit f indirect, ainsi $M = \check{R}_\vartheta$ pour un certain $\vartheta \in [0, 2\pi[$. Posons $u = (\sin(\vartheta), 1 - \cos(\vartheta))$ et $w = (-\sin(\vartheta), 1 + \cos(\vartheta))$. Nous allons montrer que $w \perp u$, et que f est la réflexion orthogonale par rapport à la droite $\mathrm{vect}(u)$.

On calcule $\langle u, w\rangle = 0$ donc $u \perp w$:

$$\langle u, w\rangle = -\sin^2(\vartheta) + 1 - \cos^2(\vartheta) = 0.$$

Ensuite, $Mu = u$ et $Mw = -w$ car:

$$\begin{aligned} Mu &= \begin{pmatrix} \cos(\vartheta) & \sin(\vartheta) \\ \sin(\vartheta) & -\cos(\vartheta) \end{pmatrix} \begin{pmatrix} \sin(\vartheta) \\ 1 - \cos(\vartheta) \end{pmatrix} = \\ &= \begin{pmatrix} \sin(\vartheta)\cos(\vartheta) - \sin(\vartheta)\cos(\vartheta) + \sin(\vartheta) \\ \sin^2(\vartheta) + \cos^2(\vartheta) - \cos(\vartheta) \end{pmatrix} = u, \\ Mw &= \begin{pmatrix} \cos(\vartheta) & \sin(\vartheta) \\ \sin(\vartheta) & -\cos(\vartheta) \end{pmatrix} \begin{pmatrix} -\sin(\vartheta) \\ 1 + \cos(\vartheta) \end{pmatrix} = \\ &= \begin{pmatrix} -\sin(\vartheta)\cos(\vartheta) + \sin(\vartheta)\cos(\vartheta) + \sin(\vartheta) \\ -\sin^2(\vartheta) - \cos^2(\vartheta) - \cos(\vartheta) \end{pmatrix} = -w. \end{aligned}$$

Donc M est la matrice de la symétrie orthogonale d'axe $\mathrm{vect}(u)$, et parallèle à $\mathrm{vect}(w) = u^\perp$, i. e. de la réflexion orthogonale d'axe $\mathrm{vect}(u)$.

Montrons le dernier énoncé. Si f est indirect alors f est diagonalisable, car f est alors une réflexion orthogonale. Puis, si f est une rotation d'angle 0 ou π alors $M = \mathbb{1}_2$ ou $M = -\mathbb{1}_2$, donc f est diagonalisable.

En revanche, si f est une rotation d'angle $\vartheta \neq 0, \pi$, nous avons vu que les valeurs propres de M sont $\cos(\vartheta) + i\sin(\vartheta)$ et $\cos(\vartheta) - i\sin(\vartheta)$, et comme $\vartheta \neq 0, \pi$ on a $\sin(\vartheta) \neq 0$, donc les deux valeurs propres ne sont pas réelles et f n'est pas diagonalisable. □

On que f est une rotation d'angle ϑ ssi, lorsque $\mathcal{B}$ est positive, $\det(M) = 1$ $\mathrm{tr}(M) = 2\cos(\vartheta)$ et si $m_{2,1}$ et $\sin(\vartheta)$ on le même signe.

Proposition 2.II.16. — *Soit u, v vecteurs de norme 1 d'un plan euclidien orienté E. Alors il existe une unique rotation f telle que $f(u) = v$. Si f est d'angle ϑ, on dit que ϑ est l'angle orienté $\widehat{uv}$ entre u et v.*

Démonstration. — Puisque u est de norme 1, nous pouvons considérer une base orthonormée (u, u') de E, donc u' appartient à la droite vectorielle $u^\perp$ (c'est une droite car $\dim(\mathrm{vect}(u)) + \dim(u^\perp) = 2$). Quitte à remplacer u' par $-u'$, nous pouvons supposer que (u, u') est positive, en effet $(u, -u')$ est aussi orthonormée, et le déterminant de la matrice de passage entre (u, u') et $(u, -u')$ vaut -1, donc au moins une de ces deux bases est positive. De même, on peut compléter v à une base orthonormée positive (v, v').

L'endomorphisme f défini par $f(u) = v$ et $f(u') = v'$ est orthogonal car il envoie une base orthonormée sur une base orthonormée, et il est direct car les deux bases sont positives. C'est donc une rotation, et l'existence est prouvée.

Montrons l'unicité. Soit g est une autre rotation telle que $g(u) = v$. Puisque $u \perp u'$ et g est orthogonale, on a $v \perp g(u')$, donc $g(u')$ est proportionnel à v', au fait $g(u') = \pm v'$ car g étant orthogonale, elle envoie u' sur un vecteur de norme 1. Or (u, u') et (v, v') sont positives, tandis que $(v, -v')$ est négative, donc l'hypothèse que g est positive implique $g(u') = v'$. En conclusion, f et g coïncident sur la base (u, u') donc $f = g$. □

2.II.E. Forme normale des automorphismes orthogonaux. —

Théorème 2.II.17. — *Soit f un automorphisme orthogonal de E. Alors il existe une base orthonormée $\mathcal{B}$ de E, des entiers r, s, et des uniques réels $\vartheta_1, \dots, \vartheta_t \in]0, \pi[$, avec $n = r+s+2t$, tels que $M = \mathrm{Mat}_{\mathcal{B}}(f)$ soit de la forme:*

$$M = \left(\begin{array}{c|c|ccc} \mathbb{1}_r & 0 & \multicolumn{3}{c}{0} \\ \hline 0 & -\mathbb{1}_s & \multicolumn{3}{c}{0} \\ \hline & & R_{\vartheta_1} & 0 & 0 \\ \cline{3-5} 0 & 0 & 0 & \ddots & 0 \\ \cline{3-5} & & 0 & 0 & R_{\vartheta_t} \end{array}\right).$$

En particulier, f est direct si et seulement si s est pair.

Nous avons besoin de deux lemmes.

Lemme 2.II.18. — *Soit $\dim(E) \geq 3$ et f un automorphisme orthogonal. Alors E admet un sous espace stable par f de dimension 1 ou 2.*

Démonstration. — Considérons une base orthonormée $\mathcal{B}$ de E et notons $M = \mathrm{Mat}_{\mathcal{B}}(f)$. Le polynôme caractéristique de M ayant des racines sur $\mathbb{C}$, nous pouvons choisir $\lambda \in \mathbb{C}$ et Z un vecteur colonne non nul dans $\mathbb{C}^n$ tels que:

$$MZ = \lambda Z.$$

Puisque M est réelle, nous avons :

$$M\overline{Z} = \overline{M}\,\overline{Z} = \overline{MZ} = \overline{\lambda Z} = \overline{\lambda}\,\overline{Z}.$$

Écrivons $Z = X + iY$, avec X, Y vecteurs colonne dans $\mathbb{R}^n$ et aussi $\lambda = \alpha + i\beta$, avec $\alpha, \beta \in \mathbb{R}$. Remarquons que :

$$Z + \overline{Z} = 2X, \qquad i(Z - \overline{Z}) = -2Y.$$

Soit F l'espace engendré par $u = \mathcal{B}X$ et $v = \mathcal{B}Y$, donc $F = \mathrm{vect}_{\mathbb{R}}(u, v)$. Nous avons alors:

$$\begin{aligned} 2MX &= M(Z + \overline{Z}) = \lambda Z + \overline{\lambda}\,\overline{Z} = \\ &= \alpha Z + i\beta Z + \alpha\overline{Z} - i\beta\overline{Z} = \\ &= 2\alpha X - 2\beta Y \in F, \\ 2MY &= -iM(Z - \overline{Z}) = -i\lambda Z + i\overline{\lambda}\,\overline{Z} = \\ &= -i\alpha Z + \beta Z + i\alpha\overline{Z} + \beta\overline{Z} = \\ &= 2\beta X + 2\alpha Y \in F. \end{aligned}$$

Donc le sous espace F est stable par f, et sa dimension est au plus 2. Clairement, la dimension de cet espace est au moins 1, car autrement $u = v = 0$, ce qui est absurde car $Z \neq 0$. Nous avons donc trouvé notre espace stable de dimension 1 ou 2. □

Lemme 2.II.19. — *Soit f un automorphisme orthogonal de E et soit F un sous espace de E stable par f. Alors $F^\perp$ est stable par f.*

Démonstration. — Soit F stable par f, et remarquons que $f_{|F} : F \to F$ est un automorphisme de F : il suffit de voir que $f_{|F}$ est injectif, or ceci est évident car f est injectif. Donc, pour tout vecteur $u \in F$, on a $f^{-1}(u) \in F$.

Soit donc $w \in F^\perp$ et montrons $f(w) \in F^\perp$. On doit prouver que, pour tout $u \in F$, on a $\langle u, f(w)\rangle = 0$. Mais:

$$\langle u, f(w)\rangle = \langle f^*(u), w\rangle = \langle f^{-1}(u), w\rangle = 0,$$

car u appartenant à F, on a $f^{-1}(u) \in F$. □

Démontration du théorème spectral orthogonal. — Nous démontrons le théorème par récurrence sur $n = \dim(E)$. Si $n \leq 2$, le théorème est valide. En effet, pour $n = 1$, la matrice d'un morphisme orthogonal vaut (± 1), ce qui est précisément notre énoncé pour $n = 1$.

Pour $n = 2$, dans la section 2.II.D nous avons prouvé qu'un endomorphisme f sur un espace euclidien de dimension 2 est soit une rotation d'angle ϑ qui est alors unique, soit une réflexion orthogonale d'axe une droite $\mathrm{vect}(u)$, parallèle à $\mathrm{vect}(w)$. Dans le premier cas, la matrice de f dans une base orthonormée est réduite au bloc R_ϑ si $\pi \neq \vartheta \in]0, 2\pi[$ et $\mathbb{1}_2$ si $\vartheta = 0$, $-\mathbb{1}_2$ si $\vartheta = \pi$). Dans le second cas, la matrice de f en la base (u, w) est $\mathrm{diag}(1, -1)$. Ce sont précisément toutes les formes possibles de notre énoncé.

Montrons l'étape de récurrence, donc soit $n \geq 3$. Par le Lemme 2.II.18, il existe un sous espace F de E stable par f avec $\dim(F) \in \{1, 2\}$. Soit $G = F^\perp$, et notons que G est aussi stable par f grâce au Lemme 2.II.19.

Supposons d'abord $\dim(F) = 1$, donc $F = \mathrm{vect}(u)$ avec $\|u\| = 1$. Dans ce cas, comme $f_{|F}$ est encore orthogonale, nous avons $f_{|F} = \pm \mathrm{id}_F$ donc $\mathrm{Mat}_{(u)}(f_{|F}) = (\pm 1)$. De plus, $\dim(G) = n - 1 < n$, donc G admet une base orthonormée $C = (e_1, \ldots, e_{n-1})$ telle que $\mathrm{Mat}_C(f_{|G})$ ait la forme du théorème. On prend $\mathcal{B} = (u, C)$. C'est une base orthonormée de E, car $\|u\| = 1$, $u \perp e_i$ pour tout $i = 1, \ldots, n-1$ et C est orthonormée. Nous avons alors:

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} \pm 1 & 0 \\ 0 & \mathrm{Mat}_C(f_{|G}) \end{pmatrix}.$$

La matrice $\mathrm{Mat}_{\mathcal{B}}(f)$ est encore de la forme voulue, quitte éventuellement à réordonner les vecteurs de $\mathcal{B}$, si $f(u) = -1$.

Supposons maintenant $\dim(F) = 2$, et on peut supposer aussi que F ne contienne aucun sous espace stable par f de dimension 1, autrement on est dans le cas précédent. Alors $f_{|F}$ est une rotation d'angle $\pi \neq \vartheta \in]0, 2\pi[$ donc $\mathrm{Mat}_D(f) = R_\vartheta$ dans une base orthonormée D de F. De nouveau $\dim(G) = n - 2 < n$, donc G admet une base orthonormée $C = (e_1, \ldots, e_{n-2})$ telle que $\mathrm{Mat}_C(f_{|G})$ ait la forme du théorème. On prend $\mathcal{B} = (C, D)$. C'est une base orthonormée de E, car $D \subset F \perp G \supset C$ et C, D sont orthonormées. Nous avons alors:

$$\mathrm{Mat}_{\mathcal{B}}(f) = \begin{pmatrix} \mathrm{Mat}_C(f_{|G}) & 0 \\ 0 & R_\vartheta \end{pmatrix}.$$

La matrice $\mathrm{Mat}_{\mathcal{B}}(f)$ est encore de la forme voulue.

Pour montrer l'unicité des ϑ_i, on liste les valeurs propres de f:

$$\begin{cases} 1 & \text{avec multiplicité } r, \\ -1 & \text{avec multiplicité } s, \\ \cos(\vartheta_i) \pm \sin(\vartheta_i) & \text{pour tout bloc } R_{\vartheta_i}. \end{cases}$$

Donc r, s et t sont déterminés, et les ϑ_i sont déterminés dans $[0, 2\pi[$, quitte à les permuter et à remplacer ϑ_i avec $2\pi - \vartheta_i$, car ces deux valeurs sont les antécédents de $\cos(\vartheta_i)$ dans $[0, 2\pi[$. On peut donc assumer $\vartheta_i \in]0, \pi[$ et les ϑ_i sont alors uniquement déterminés. □

2.II.F. Automorphismes orthogonaux en dimension 3. — Soit maintenant E un espace euclidien de dimension 3.

Proposition 2.II.20. — *Soit f un endomorphisme orthogonal de E. Alors l'un des cas se produit:*

i) f est une symétrie orthogonale;

ii) il existe un plan vectoriel F dans E tel que f est la rotation dans F d'angle $\vartheta \in]0, \pi[\cup]\pi, 2\pi[$, et f est alors direct;

iii) il existe un plan vectoriel F dans E tel que f est la rotation dans F d'angle $\vartheta \in]0, \pi[\cup]\pi, 2\pi[$, suivie par la réflexion orthogonale d'axe F, ainsi f est indirect.

Les rotations sont détermines à la transformation $\vartheta \mapsto 2\pi - \vartheta$ près.

Démonstration. — Il s'agit d'une application du théorème de la forme normale des endomorphismes orthogonaux. Soit donc $\mathcal{B} = (e_1, e_2, e_3)$ une base orthonormée $\mathcal{B}$ de E, telle que $M = \mathrm{Mat}_{\mathcal{B}}(f)$ ait la forme du théorème 2.II.17. Si aucun bloc M_{ϑ_i} n'apparaît, alors f est une symétrie orthogonale, d'axe un sous espace F de E de dimension m où m est le nombre d'indices i tels que $f(e_i) = -1$. C'est le cas (i)).

Si ce n'est pas le cas, alors f n'est pas une symétrie orthogonale, et puisque $\dim(E) = 3$, un seul bloc R_ϑ apparaît dans M, avec $\vartheta \in]0, \pi[\cup]\pi, 2\pi[$, ainsi $F = \mathrm{vect}(e_2, e_3)$ est un plan vectoriel de E et $f_{|F}$ est bien une rotation d'angle ϑ. De plus nous avons $f(e_1) = \pm e_1$. Si c'est $f(e_1) = e_1$, on est dans le cas (ii)) et f est direct, si $f(e_1) = -e_1$, on est dans le cas (iii)) et f est indirect. □

Corollaire 2.II.21. — *Un élément $f \in \mathrm{SO}(E)$ est une rotation d'angle $\vartheta \in [0, 2\pi[$ d'axe $\mathrm{vect}(u)$ et, si $\mathcal{B}$ est une base orthonormée de E, on a $\mathrm{tr}(\mathrm{Mat}_{\mathcal{B}}(f)) = 1 + 2\cos(\vartheta)$.*

2.III. Groupe orthogonal euclidien

Soit E un espace vectoriel euclidien de dimension $n < \infty$.

Remarque 2.III.1. — Le centre de $\mathrm{O}(E)$ est $\{\pm \mathrm{id}_E\}$.

Démonstration. — Il est évident que $\{\pm \mathrm{id}_E\}$ est contenu dans le centre. Réciproquement, soit f dans le centre de $\mathrm{O}(E)$. □

2.III.A. Générateurs du groupe orthogonal. —

Théorème 2.III.2. — *Soit $\dim(E) = n$, et soit $f \in \mathrm{O}(E)$. Alors f peut être décomposé comme produit de k réflexions orthogonales, avec $k \leq n - \dim(\mathrm{Fix}(f))$.*

Démonstration. — On considère l'espace des points fixes de f, i. e. l'espace propre de la valeur propre 1 de f:

$$F = \mathrm{Fix}(f) = \{v \in E \mid f(v) = v\}.$$

Nous allons montrer que f s'écrit comme produit de k réflexions orthogonales, avec $k \leq n - \dim(F)$.

Soit donc $m = n - \dim(F) = \dim(F^\perp)$, et raisonnons par récurrence sur m. Si $m = 0$, nous avons $\dim(F) = \dim(E)$ donc $F = E$, ce qui veut dire que f est l'identité. Dans ce cas, nous n'avons besoin d'aucune réflexion, i. e. $k = 0$, et l'énoncé est valide.

Montrons l'étape de récurrence, donc soit $m > 1$. Rappelons que $F^\perp$ est stable par f grâce au Lemme 2.II.19. Soit $0 \neq u \in F \perp$ et posons $w = f(u)$, donc $u \neq w$ car u n'appartient pas à F. On note aussi:

$$\xi = \frac{u + w}{2}, \qquad \eta = \frac{u - w}{2}.$$

On remarque alors $\xi \perp \eta$. En effet:

$$\langle \xi, \eta \rangle = \frac{1}{4}(\|u\|^2 - \|w\|^2 + \langle u, v \rangle - \langle u, v \rangle) = 0,$$

car $\|u\| = \|w\|$, f étant orthogonale. Posons:

$$G = \mathrm{vect}(\eta), \qquad H = G^\perp, \qquad g = \sigma_H,$$

donc $\eta \in G$, $\xi \in H$, et g est une réflexion orthogonale.

Maintenant, on observe que, si $v \in F$, alors $v \perp u$, $v \perp w$ donc $v \perp \eta$, ainsi $v \in H$, et $g(v) = v$. De plus, $w = \xi - \eta$, donc $g(w) = \xi + \eta = u$. Alors $g \circ f$ contient tous les points fixes de f et de plus u. Il s'en suit que $\dim(\mathrm{Fix}(g \circ f) \geq \dim(F) + 1$, donc $n - \dim(\mathrm{Fix}(g \circ f) \leq n - \dim(F) - 1 \leq m - 1$. Alors $g \circ f$ est le produit de k réflexions orthogonales $r_1 \circ \cdots \circ r_k$ avec, par hypothèse de

récurrence, $k \leq m-1$. Ainsi $f = g \circ r_1 \circ \cdots \circ r_k$ est le produit de $k+1$ réflexions, avec $k+1 \leq m$. □

Proposition 2.III.3. — *Si $n \geq 3$, alors tout $f \in \mathrm{SO}(n, \mathbb{R})$ peut s'écrire comme produit de k renversements, avec $k \leq \mathrm{codim}(\mathrm{Fix}(f))$.*

Démonstration. — Soit $f \in \mathrm{SO}(n, \mathbb{R})$. Alors f est produit de k réflexions, où k est un nombre pair et $k \leq \mathrm{codim}(\mathrm{Fix}(f))$.

Si $n = 3$, alors f est soit l'identité soit le produit de 2 réflexions, car f est direct. Regardons ce deuxième cas. Si σ est une réflexion, alors $-\sigma$ est un renversement. En effet, si H est un hyperplan $-\sigma_H = \sigma_{H^\perp}$ et $H^\perp$ a dimension 1, i.e., codimension 2. Donc f est le produit de l'opposé de deux réflexsions, i.e. de deux renversements.

Soit $n \geq 4$ et considérons σ_{H_1} et σ_{H_2} deux réflexions orthogonales $H_1 = u_1^\perp$ et $H_2 = u_2^\perp$, que l'on peut supposer distincts. On a alors $\mathrm{codim}(H_1 \cap H_2) = 2$.

Soit $F = \mathrm{vect}(u_1, u_2)$. On a $F = (H_1 \cap H_2)^\perp$ et $\dim(F) = 2$. On choisit L, un sous espace E de dimension 3 qui contient F. Les restrictions de $-\sigma_{H_1}$ et $-\sigma_{H_2}$ à L sont des renversements de L, notés $\bar{\tau}_1$ et $\bar{\tau}_2$. On prolonge $\bar{\tau}_1$ et $\bar{\tau}_2$ à des automorphismes orthogonaux τ_1 et τ_2 de E en déclarant que ceux-ci se restreignent à l'identité sur $F^\perp$. On a $\sigma_1\sigma_2 = \tau_1\tau_2$ car cette égalité est évidente sur F, tandis que sur $F^\perp$ autant les σ_i que les τ_i sont l'identité.

Tout couple de réflexions orthogonales σ_1, σ_2 dans la décomposition de f donnant lieu à un couple de renversements orthogonaux τ_1, τ_2 tels que $\sigma_1\sigma_2 = \tau_1\tau_2$ et ces réflexions étant en nombre $k \leq \mathrm{codim}(\mathrm{Fix}(f))$ pair, nous avons l'énoncé souhaité. □

2.III.B. Compacité et connexité du groupe orthogonal. — Le groupe $\mathrm{SO}(E)$ s'identifie à $\mathrm{SO}(n, \mathbb{R})$ une fois fixée une base orthonormée de E. Le groupe $\mathrm{SO}(n, \mathbb{R})$ est une partie de l'espace vectoriel des matrices $\boldsymbol{M}_n(\mathbb{R})$, que l'on peut considérer comme un espace vectoriel normé par la norme du maximum des normes des vecteurs colonne d'une matrice. De même on peut considérer la norme d'opérateur de $f \in \mathrm{O}(E)$, définie comme le maximim des normes de $f(u)$ lorsque u parcourt la sphère des vecteurs de norme 1 dans E.

Théorème 2.III.4. — *Le groupe $\mathrm{SO}(E)$ est compact et connexe par arcs.*

Démonstration. — Fixons une base orthonormée $\mathcal{B}$ de E et donc un isomorphisme entre $\mathrm{SO}(E)$ et $\mathrm{SO}(n, \mathbb{R})$, montrons ensuite que $\mathrm{SO}(n, \mathbb{R})$ est fermé et borné dans $\boldsymbol{M}_n(\mathbb{R})$.

Pour voir que $\mathrm{SO}(n, \mathbb{R})$ est fermé, on regarde $\mathrm{SO}(n, \mathbb{R})$ comme la partie de $\boldsymbol{M}_n(\mathbb{R})$ définie par les conditions $MM^t = \mathbb{1}_n$ et $\det(M) = 1$, M étant une matrice de $\boldsymbol{M}_n(\mathbb{R})$. Ces équation étant polynomiales en les coefficients $a_{i,j}$ de M (et donc continues), on a $\mathrm{SO}(n, \mathbb{R})$ fermé.

Pour la compacité de $\mathrm{SO}(n, \mathbb{R})$, on écrit la i-ième colonne de M comme un vecteur $v_i = (a_{1,i}, \ldots, a_{n,i})^t \in \mathbb{R}^n$. La condition $MM^t = \mathbb{1}_n$ exprime alors $\|v_i\| = 1$ pour chaque $i \in [\![1, n]\!]$ et $v_i \perp v_j$ pour $i \neq j$ dans $[\![1, n]\!]$. La condition $\|v_i\| = 1$ implique déjà que $\mathrm{SO}(n, \mathbb{R})$ est borné.

Montrons enfin que $\mathrm{SO}(n, \mathbb{R})$ est connexe par arcs. Pour le faire, nous utilisons la forme normale des automorphismes normaux. Celle-ci nous donne, pour tout $M \in \mathrm{SO}(n, \mathbb{R})$, une matrice P orthogonale et des réels $\vartheta_1, \ldots, \vartheta_t \in]0, \pi[$, avec $n = r + s + 2t$, tels que $M = PNP^t$ où N est de la forme:

$$N = \left(\begin{array}{c|c|ccc} \mathbb{1}_r & 0 & \multicolumn{3}{c}{0} \\ \hline 0 & -\mathbb{1}_s & \multicolumn{3}{c}{0} \\ \hline & & R_{\vartheta_1} & 0 & 0 \\ \cline{3-5} 0 & 0 & 0 & \ddots & 0 \\ \cline{3-5} & & 0 & 0 & R_{\vartheta_t} \end{array}\right).$$

On définit alors un chemin $[0,1] \to \mathrm{SO}(n,\mathbb{R})$ par $\lambda \mapsto N_\lambda$ où :

$$N_\lambda = \left(\begin{array}{c|c|ccc} \mathbb{1}_r & 0 & \multicolumn{3}{c}{0} \\ \hline 0 & -\mathbb{1}_s & \multicolumn{3}{c}{0} \\ \hline & & R_{\lambda\vartheta_1} & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 \\ & & 0 & 0 & R_{\lambda\vartheta_t} \end{array}\right).$$

On trouve $N_0 = \mathbb{1}_n$ et $N_1 = N$. Ainsi, $M_\lambda = PN_\lambda P^t$ satisfait $M_0 = \mathbb{1}_n$ et $M_1 = N$. Le chemin $\lambda \mapsto M_\lambda$ est clairement continu, et relie M à $\mathbb{1}_n$. Tout point de $\mathrm{SO}(n,\mathbb{R})$ étant lié à $\mathbb{1}_n$, on a donc $\mathrm{SO}(n,\mathbb{R})$ connexe par arcs. □

2.III.C. Simplicité du groupe orthogonal. —

2.III.C.1. Simplicité du groupe orthogonal en dimension 3. —

Théorème 2.III.5. — *Le groupe* $\mathrm{SO}(3,\mathbb{R})$ *est simple.*

Démonstration. — Soit H un sous groupe distingué de $\mathrm{SO}(3,\mathbb{R})$, pas réduit à l'élément neutre. Nous voulons montrer que H contient un renversement. En effet, tous les renversements étant conjugués et H étant distingué, H va contenir tous les renversements. Puisque les renversements engendrent $\mathrm{SO}(3,\mathbb{R})$, on aura alors $H = \mathrm{SO}(3,\mathbb{R})$.

Soit donc $g \neq \mathbb{1}_3$ un élément de H. On a l'application $\varphi : \mathrm{SO}(3,\mathbb{R}) \to \mathbb{R}$ définie par:

$$\varphi(f) = \mathrm{tr}(fgf^{-1}g^{-1}).$$

Cette application est clairement continue. Du moment que $fgf^{-1}g^{-1}$ est une rotation, d'angle disons ϑ, sa trace est $1 + 2\cos(\vartheta) \in [1,3]$, i.e. $\mathrm{Im}(\varphi) \subset [1,3]$.

Plus précisément, l'image de $\mathrm{Im}(\varphi)$ étant compacte et connexe, est un intervalle $[a,b] \subset [1,3]$, et $\varphi(\mathbb{1}_3) = 3$, donc $b = 3$. Aussi, $a < 3$. En effet, si $\varphi(f) = 3$, alors $\vartheta = 0$ donc $fg = gf$. Si g est une rotation dont l'axe est une droite L, alors fgf^{-1} est une rotation d'axe $f(L)$. Si $fg = gf$ alors $L = f(L)$, et ceci ne peut pas arriver pour tout $f \in \mathrm{SO}(3,\mathbb{R})$.

Comme $1 + 2\cos(\vartheta)$ tend vers 3 lorsque ϑ tend vers 0, il existe $n_0 \in \mathbb{N}$ tel que, pour tout $n \geq n_0$, on ait $1 + 2\cos(\pi/n) > a$, donc $1 + 2\cos(\pi/n) \in \mathrm{Im}(\varphi)$. Fixons $n \geq n_0$.

Soit alors $f_n \in \mathrm{SO}(3,\mathbb{R})$ tel que $\varphi(f_n) = 1+2\cos(\pi/n)$, de sorte que $h_n := f_n g f_n^{-1} g^{-1}$ est une rotation d'angle π/n. On a $h_n \in H$ car $f_n g f_n^{-1} \in H$, H étant normal dans $\mathrm{SO}(3,\mathbb{R})$ et $g^{-1} \in H$. Enfin, h_n^n appartient aussi à H et est une rotation d'angle π, i.e. un renversement. □

2.III.C.2. Simplicité du groupe orthogonal en dimension supérieure. —

Lemme 2.III.6. — *Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $1 \leq k \leq n-1$. Un automorphisme qui fixe tout sous espace de dimension k est une homothétie.*

Démonstration. — Soit D une droite vectorielle de E. On peut écrire D comme intersection de sous espaces de dimension k. En effet, si L est définie par $n-1$ équations indépendantes $\{f_1,\dots,f_{n-1}\}$, donc comme intersection de $n-1$ hyperplans, on définit des sous espaces de dimension k en choisissant k équations parmi $\{f_1,\dots,f_{n-1}\}$. L'intersection de ces sous espaces est D.

Il en résulte que, comme f fixe chacun de ces sous espaces, f fixe D. Donc f est une homothétie. □

Théorème 2.III.7. — *Si $n \geq 5$, le groupe* $\mathrm{PSO}(n,\mathbb{R})$ *est simple.*

Démonstration. — Nous fixons un espace euclidien (E,q) de dimension n, où E est un espace vectoriel réel et q est une forme quadratique définie positive, et un isomorphisme $\mathrm{PSO}(E,q) \simeq \mathrm{PSO}(n,\mathbb{R})$. Soit H_0 un sous groupe distingué de $\mathrm{PSO}(E,q)$, non réduit à l'identité. Alors nous avons H sous groupe distingué de $\mathrm{SO}(E,q)$, qui ne consiste pas uniquement de $\pm\mathrm{id}_E$.

Soit $h \in H$, $h \neq \pm \mathrm{id}_E$. Les homothéties orthogonales sont id_E et $-\mathrm{id}_E$, donc h n'en est pas une. Il existe alors un plan P de E tel que $P \neq h(P)$, d'après le lemme 2.III.6.

Posons $L = P^\perp$ soit τ_L le renversement de plan P. On a:

$$g = [h, \tau_L] = h\tau_L h^{-1}\tau_L = \tau_{hL}\tau_L.$$

Comme H est distingué, $\tau_L h^{-1}\tau_L \in H$ donc $g \in H$. De plus, $\mathrm{Fix}(g)$ contient l'intersection $L \cap h(L)$, un sous espace intersection de deux sous espaces de codimension 2, donc de dimension au moins $n-4$. Comme $n \geq 5$, il existe $u \in \mathrm{Fix}(g) \setminus \{0\}$.

On a $g \neq -\mathrm{id}_E$ car g possède le vecteur fixe u. On a aussi $g \neq \mathrm{id}_E$, puisque $P \neq h(P)$.

Nous avons trouvé un élément $g \in H$ qui n'est pas une homothétie et qui possède le vecteur fixe u. Soit $H = u^\perp$ et considérons τ_H. Bien sûr on a $gH = H$ donc $\tau_{gH}\tau_H = \mathrm{id}_E$. Comme g n'est pas une homothétie, il existe $u' \in E \setminus \{0\}$ tel que $H' = (u')^\perp$ n'est pas fixé par g. On pose $\sigma = \tau_{H'}\tau_H$, on considère le commutateur :

$$f = [\sigma, g] = \sigma g \sigma^{-1} g^{-1} = \tau_{H'}\tau_H g \tau_H \tau_{H'} g^{-1} = \tau_{H'}\tau_H g \tau_H \tau_{H'} g^{-1} =$$

$$= \tau_{H'}\tau_H g \tau_H g^{-1} g \tau_{H'} g^{-1} = \tau_{H'}\tau_H \tau_{gH}\tau_{gH'} = \tau_{H'}\tau_{gH'}.$$

L'élément f appartient à H, toujours puisque H est distingué. Aussi, $f = \tau_{H'}\tau_{gH'}$ possède un lieu fixe de dimension au moins $n-2$, car $\mathrm{Fix}(f) \supset H' \cap gH'$. De plus, $f \neq -\mathrm{id}_E$ car f possède des vecteurs fixes non nuls. Aussi, $f \neq \mathrm{id}_E$ puisque $H \neq gH'$.

Considérons alors un sous espace de dimension $n-3$ dans $\mathrm{Fix}(f)$ et un son orthogonal $M \subset E$. Le sous espace M a dimension 3 et f se restreint à $f_0 \in H_0 = H \cap \mathrm{SO}(M, q|_M)$, avec $f_0 \neq \pm \mathrm{id}_M$. Ainsi, H_0 est un sous groupe distingué de $\mathrm{SO}(M, q|_M)$ qui n'est pas réduit à l'élément neutre, donc $H_0 = \mathrm{SO}(M, q|_M)$ par simplicité de $\mathrm{SO}(3, \mathbb{R})$. Donc H_0 contient un renversement, par conséquent il en est de même pour H, et comme ceux-ci sont tous conjugués ils sont tous dans H. Du moment que les renversements engendrent $\mathrm{SO}(E, q)$, on a donc $H = \mathrm{SO}(E, q)$. □

2.IV. Espaces affines euclidiens

2.IV.A. Structure euclidienne sur un espace affine. —

Définition 2.IV.1. — Soit $\mathcal{E}$ un espace affine réel de direction E. Une *structure d'espace affine euclidien* sur $\mathcal{E}$ est un produit scalaire sur E. On définit la *distace* $d(P, Q)$ entre deux points $P, Q \in \mathcal{E}$ comme $\|\overrightarrow{PQ}\|$.

Remarque 2.IV.2. — L'application $d : \mathcal{E} \times \mathcal{E} \to \mathbb{R}$ est une distance, i.e. :

i) pour tout $P, Q \in \mathcal{E}$, $d(P, Q) \geq 0$;

ii) pour tout $P, Q \in \mathcal{E}$, $d(P, Q) = d(Q, P)$;

iii) pour tout $P, Q, R \in \mathcal{E}$, $d(P, R) \leq d(P, Q) + d(Q, R)$;

iv) pour tout $P, Q \in \mathcal{E}$, $d(P, Q) = 0$ si et seulement si $P = Q$.

Démonstration. — Toutes les propriétés sont claires du moment que E est un espace vectoriel euclidien. □

Remarque 2.IV.3. — Si on muni E de sa structure canonique d'espace affine, la distance dans E est $d(u, v) = \|u - v\|$.

Si $O \in \mathcal{E}$, la bijection $\Theta_O : \mathcal{E} \to E$ est isométrique dans le sens que, pour tout $P, Q \in \mathcal{E}$, on a $d(P, Q) = \|\overrightarrow{PQ}\| = \|\overrightarrow{OQ} - \overrightarrow{OP}\| = d(\Theta_O(P), \Theta_O(Q))$.

2.IV.B. Orthogonalité. —

Définition 2.IV.4. — Deux sous espaces affines $\mathcal{F}$ et $\mathcal{G}$ de $\mathcal{E}$ sont *orthogonaux* si $\vec{\mathcal{F}} \perp \vec{\mathcal{G}}$.

2.IV.B.1. Hyperplan médiateur. —

Définition 2.IV.5. — Soit $P \neq Q \in \mathcal{E}$, I le milieu du segment $[P,Q]$. L'*hyperplan médiateur* de $[P,Q]$ est $I + \overrightarrow{PQ}^{\perp}$.

Proposition 2.IV.6. — *L'hyperplan médiateur $\mathcal{H}$ de $[P,Q]$ satisfait :*

$$\mathcal{H} = \{M \in \mathcal{E} \mid d(M,P) = d(M,Q)\} = \{M \in \mathcal{E} \mid \overrightarrow{IM} \perp \overrightarrow{PQ}\}.$$

Démonstration. — Le sous espace $\overrightarrow{PQ}^{\perp}$ est constitué des vecteurs $\vec{v} \in E$ tels que $\vec{v} \perp \overrightarrow{PQ}$. Si on vectorialise en I, on trouve les vecteurs de la forme $\overrightarrow{IM}$ tels que $\overrightarrow{IM} \perp \overrightarrow{PQ}$. Ainsi, $\mathcal{H}$ est l'ensemble des points M de $\mathcal{E}$ tels que $\overrightarrow{IM} \perp \overrightarrow{PQ}$.

Ensuite, écrivons :

$$\begin{aligned} d(M,P) = d(M,Q) &\Leftrightarrow \|\overrightarrow{MP}\| = \|\overrightarrow{MQ}\| \Leftrightarrow \|\overrightarrow{MP}\|^2 - \|\overrightarrow{MQ}\|^2 = 0 \\ &\Leftrightarrow \langle \overrightarrow{MP} + \overrightarrow{MQ}, \overrightarrow{MP} - \overrightarrow{MQ} \rangle = 0 \\ &\Leftrightarrow \langle 2\overrightarrow{MI}, \overrightarrow{QP} \rangle = 0 \Leftrightarrow \overrightarrow{IM} \perp \overrightarrow{PQ}. \end{aligned}$$

□

2.IV.B.2. Projections orthogonales. —

Définition 2.IV.7. — Soit $\mathcal{F}$ un sous espace affine de $\mathcal{E}$ et $P \in \mathcal{E}$. La *distance* de P à $\mathcal{F}$ est $d(P,\mathcal{F}) = \inf_{Q \in \mathcal{F}} d(P,Q)$.

Remarque 2.IV.8. — Si $\pi_{\mathcal{F}}$ est la projection orthogonale de $\mathcal{E}$ sur $\mathcal{F}$, alors

$$d(P,\mathcal{F}) = d(P, \pi_{\mathcal{F}}(P)).$$

Démonstration. — Soit $Q = \pi_{\mathcal{F}}(P)$ et $M \in \mathcal{F}$. On a :

$$d(P,M) = \|\overrightarrow{PM}\| = \|\overrightarrow{PQ} + \overrightarrow{QM}\| \geq \|\overrightarrow{PQ}\| = d(P,Q).$$

L'égalité se produit si et seulement si $\overrightarrow{QM} = \vec{0}$, i.e. lorsque $M = Q$. □

2.V. Isométries affines

Fixons $\mathcal{E}$ espace affine euclidien de direction E. On notera $d_{\mathcal{E}}(P,Q)$ la distance entre deux points P,Q de $\mathcal{E}$, ou simplement $d(P,Q)$ lorsque aucune ambiguïté n'est possible.

2.V.A. Isométries et automorphismes orthogonaux. — Soit $\mathcal{F}$ un espace affine euclidien de direction F muni de la distance $d_{\mathcal{F}}$.

2.V.A.1. Linéarité des isométries. —

Définition 2.V.1. — Une *isométrie* est une application $\varphi : \mathcal{E} \to \mathcal{F}$ telle que, pour tout $P,Q \in \mathcal{E}$ on ait $d_{\mathcal{E}}(P,Q) = d_{\mathcal{F}}(\varphi(P), \varphi(Q))$.

Proposition 2.V.2. — *Toute isométrie φ est affine et $\vec{\varphi}$ est orthogonale.*

Démonstration. — Considérons une application $\varphi : \mathcal{E} \to \mathcal{F}$, choisissons $O \in \mathcal{E}$ et écrivons, pour $P \in \mathcal{E}$, $\varphi(P) = R + f(\overrightarrow{OP})$, où $R = \varphi(R)$. Il s'agit de montrer que $f : E \to F$ est linéaire. Étant donnés $P,Q \in \mathcal{E}$, on trouve :

$$\|\overrightarrow{OP} - \overrightarrow{OQ}\|_E = d(P,Q)_{\mathcal{E}} = d(\varphi(P),\varphi(Q))_{\mathcal{F}} = \|\overrightarrow{R\varphi(P)} - \overrightarrow{R\varphi(Q)}\|_F = \|f(\overrightarrow{OP}) - f(\overrightarrow{OQ})\|_F.$$

Aussi, $f(\vec{0}) = \vec{0}$. La f proposition 2.II.2 montre alors que f est linéaire.

Il est clair que $f = \vec{\varphi}$ est alors une isométrie vectorielle, i.e. f est orthogonale. En effet, pour tout $P \in \mathcal{E}$, on a $\|f(\overrightarrow{OP})\|_E = d(R,\varphi(P))_{\mathcal{F}} = d(O,P)_{\mathcal{E}} = \|\overrightarrow{OP}\|_E$. □

Remarque 2.V.3. — Une isométrie est un isomorphisme affine sur son image. La composition de deux isométries l'est aussi. L'inverse d'une isométrie l'est aussi.

2.V.A.2. Translations. —

Remarque 2.V.4. — Une translation est une isométrie.

Démonstration. — C'est immédiat d'après la règle du parallélogramme. □

2.V.B. Décomposition des isométries. — Soit $\mathcal{E}$ un espace affine euclidien de dimension n. Nous avons deux façons principales de décomposer une isométrie affine de $\mathcal{E}$: soit en produit de réflexions, soit (et de manière canonique) en produit d'une translation et d'une isométrie ψ à point fixe, qui commutent, la direction de translation étant fixée par ψ.

2.V.B.1. Produit de réflexions. —

Proposition 2.V.5. — *Une isométrie φ de $\mathcal{E}$ peut s'écrire comme produit de k réflexions orthogonales, avec $k \leq n+1$*

Démonstration. — Soit φ une isométrie de $\mathcal{E}$. Si φ possède un point fixe O, on vectorialise $\mathcal{E}$ en O et on applique le résultat connu pour E.

Sinon, soit $O \in \mathcal{E}$ et $Q = \varphi(O)$. L'hyperplan médiateur $\mathcal{H}$ de $[OQ]$ définit une réflexion orthogonale σ d'axe $\mathcal{H}$, avec $\sigma(Q) = O$. Donc $\sigma \circ \varphi$ s'écrit comme produit de k réflexions orthogonales avec $k \leq n$, d'où le résultat. □

2.V.B.2. Structure des isométries. —

Proposition 2.V.6. — *Soit φ une isométrie de $\mathcal{E}$. Alors il existe un et un seul couple $(\psi, \vec{u})$, avec ψ isométrie,* $\mathrm{Fix}(\psi) \neq \varnothing$, $\vec{u} \in \ker(\vec{\psi} - \mathrm{id}_E)$ *et* $\varphi = t_{\vec{u}} \circ \psi = \psi \circ t_{\vec{u}}$.

Démonstration. — Nous voulons montrer que $E = \ker(\vec{\varphi} - \mathrm{id}_E) \oplus \mathrm{Im}(\vec{\varphi} - \mathrm{id}_E)$. Nous allons voir que pour tout $\vec{u} \in \ker(\vec{\varphi} - \mathrm{id}_E)$ et $\vec{v} \in E$, on a $\langle \vec{u}, \vec{\varphi}(\vec{v}) - \vec{v} \rangle = \vec{0}$. En effet :

$$\langle \vec{u}, \vec{\varphi}(\vec{v}) - \vec{v} \rangle = \langle \vec{u}, \vec{\varphi}(\vec{v}) \rangle - \langle \vec{u}, \vec{v} \rangle = \langle \vec{\varphi}(\vec{u}), \vec{\varphi}(\vec{v}) \rangle - \langle \vec{u}, \vec{v} \rangle = \langle \vec{u}, \vec{v} \rangle - \langle \vec{u}, \vec{v} \rangle = \vec{0}.$$

On a donc $\ker(\vec{\varphi} - \mathrm{id}_E) \perp \mathrm{Im}(\vec{\varphi} - \mathrm{id}_E)$, donc $E = \ker(\vec{\varphi} - \mathrm{id}_E) \oplus \mathrm{Im}(\vec{\varphi} - \mathrm{id}_E)$ car la somme des espaces $\ker(\vec{\varphi} - \mathrm{id}_E)$ et $\mathrm{Im}(\vec{\varphi} - \mathrm{id}_E)$ est $n = \dim(E)$. L'existence et unicité de ψ affine et $\vec{u}$ découle du théorème 1.II.15, aussi bien que le fait $\vec{u} \in \ker(\vec{\psi} - \mathrm{id}_E)$. Enfin ψ est une isométrie comme composition d'isométries. □

CHAPITRE 3

GÉOMÉTRIE PROJECTIVE

3.I. Espaces projectifs

Ici, $\mathbb{K}$ est un corps. Tous les corps, sauf mention contraire, seront commutatifs.

3.I.A. Droites vectorielles. —

Définition 3.I.1. — Soit E un $\mathbb{K}$-espace vectoriel de dimension finie. L'*espace projectif* $\mathbb{P}(E)$ associé à E est l'ensemble des droites vectorielles de E, c'est-à-dire l'ensemble des sous espaces vectoriels de dimension 1 de E.

Si $v \in E \setminus \{0\}$, on note $[v]$ le point de $\mathbb{P}(E)$ correspondant à la droite $\mathrm{vect}(v) \subset E$. Si $\dim(E) = n+1$, on dit que $\mathbb{P}(E)$ est un espace projectif *de dimension* n.

Exemple 3.I.2. — Si $E = \mathbb{K}^{n+1}$, on note $\mathbb{P}(E) = \mathbb{P}^n(\mathbb{K})$. Si $(x_0, \dots, x_n) \in \mathbb{K}^{n+1} \setminus \{0\}$, la notation usuelle pour le point de $\mathbb{P}^n(\mathbb{K})$ associé à $(x_0, \dots, x_n)$ est :

$$[x_0, \dots, x_n] = (x_0 : \dots : x_n).$$

Les valeurs des x_i sont définies à multiplication par un scalaire près :

$$(x_0 : \dots : x_n) = (x'_0 : \dots : x'_n) \Leftrightarrow \exists \lambda \in \mathbb{K}^* \mid x'_i = \lambda x_i, \forall i \in [\![0, n]\!].$$

3.I.B. Ouverts affines. —

Définition 3.I.3. — Soit α une forme linéaire non nulle sur E. On pose :

$$U_\alpha = \{[v] \in \mathbb{P}(E) \mid \alpha(v) \neq 0\}.$$

On nomme U_α l'*ouvert affine* associé à α. La définition est bien posée car, si $[v] = [v']$, il existe $\lambda \in \mathbb{K}^*$ tel que $v' = \lambda v$ donc $\alpha(v') = \lambda\alpha(v) \neq 0$.

Remarque 3.I.4. — L'ouvert affine U_α s'identifie à l'espace affine de dimension n :

$$\mathcal{K}_\alpha = \{v \in E \mid \alpha(v) = 1\},$$

grâce à l'application $\psi : U_\alpha \to \mathcal{K}_\alpha$ définie par

$$[v] \mapsto \psi(v) = \frac{1}{\alpha(v)} v.$$

En effet, d'abord on se rend compte facilement que cette application est bien définie. Pour le voir, d'abord on a clairement $1/\alpha(v)$ bien défini puisque $\alpha(v) \neq 0$. Ensuite, si $[v] = [v']$, alors il existe $\lambda \in \mathbb{K}^*$ tel que $v' = \lambda v$ donc :

$$\frac{1}{\alpha(v')} v' = \frac{1}{\lambda\alpha(v)} \lambda v = \frac{1}{\alpha(v)} v.$$

L'application inverse $\iota : \mathcal{K}_\alpha \to U_\alpha$ est définie par $v \mapsto [v]$.

Ces applications sont bien l'inverse l'une de l'autre, i. e. l'on a :

$$\iota \circ \psi = \mathrm{id}_{U_\alpha}, \qquad \text{et} \qquad \psi \circ \iota = \mathrm{id}_{\mathcal{K}_\alpha}.$$

En effet, si $v \in \mathcal{K}_\alpha$, alors :

$$\psi(\iota(v)) = \psi([v]) = \frac{1}{\alpha(v)} v = v.$$

Aussi, si $[v] \in U_\alpha$, on a :

$$\iota(\psi([v]) = \iota\left(\frac{1}{\alpha(v)} v\right) = \left[\frac{1}{\alpha(v)} v\right] = [v].$$

3.I.C. Repères projectifs. — En cours de rédaction

3.I.D. Dualité. —

3.I.D.1. Dualité vectorielle. — Soit E un $\mathbb{K}$-espace vectoriel de dimension finie $n+1 < \infty$. On définit le dual $E^\vee$ de E comme l'ensemble des applications linéaires $\alpha : E \to \mathbb{K}$ de E vers $\mathbb{K}$, muni de sa structure évidente de $\mathbb{K}$-espace vectoriel.

Cette définition est "contravariante", dans le sens que, si E et F sont deux espaces vectoriels et $f : F \to E$ est une application linéaire, alors il existe une application linéaire naturelle $f^\vee : E^\vee \to F^\vee$, qui consiste à composer $\beta \in F^\vee$ avec f, i.e.:

$$f^\vee(\beta) = \beta \circ f.$$

Rappelons que E étant de dimension finie, E est réflexif, c'est-à-dire E s'identifie avec $E^{\vee\vee}$ par l'application d'évaluation $e : E \to E^{\vee\vee}$ définie, pour tout $u \in E$ par :

$$u \mapsto e_u, \qquad \text{où } e_u(\alpha) = \alpha(u), \forall \alpha \in E^\vee.$$

Définition 3.I.5. — Étant donné un sous espace vectoriel F de E, notons j_F l'inclusion $j_F : F \to E$. *L'orthogonal* de F dans $E^\vee$ est :

$$F^\perp = \mathrm{Ker}(j_F^\vee).$$

Remarquons que $j_F^\vee$ est l'application de restriction des formes à F. Ainsi :

$$F^\perp = \{\alpha \in E^\vee \mid \alpha|_F = 0\}.$$

Proposition 3.I.6. — *Soit F, G sous espace vectoriels de E. Alors :*

i) à travers l'identification $E \cong E^{\vee\vee}$, on a $F^{\perp\perp} = F$;

ii) $F \subset G$ si et seulement si $G^\perp \subset F^\perp$;

iii) $(F+G)^\perp = F^\perp \cap G^\perp$;

iv) $(F \cap G)^\perp = F^\perp + G^\perp$.

Démonstration. — Montrons i). Soit $f : F^\perp \to E^\vee$ l'inclusion et considérons:

$$g : E \xrightarrow{e} E^{\vee\vee} \xrightarrow{f^\vee} (F^\perp)^\vee.$$

On veut montrer que $\mathrm{Ker}(g) = F$. On a:

$$\begin{aligned}
\mathrm{Ker}(g) &= \{u \in E \mid f^\vee(e_u) = 0\} = \\
&= \{u \in E \mid e_u|_{F^\perp} = 0\} = \\
&= \{u \in E \mid e_u(\alpha) = 0, \forall \alpha \in F^\perp\} = \\
&= \{u \in E \mid \alpha(u) = 0, \forall \alpha \in F^\perp\} = \\
&= \{u \in E \mid \alpha(u) = 0, \forall \alpha \text{ tels que } \alpha(v) = 0 \text{ pour tout vecteur } v \in F\}.
\end{aligned}$$

Donc, si $v \in F$ alors clairement $v \in \mathrm{Ker}(g)$ puisque $\alpha(v) = 0$ quelque soit $\alpha \in F^\perp$.

Réciproquement, si nous écrivons une base $(e_1, \dots, e_k)$ de F et nous la complétons à une base $\mathcal{B} = (e_1, \dots, e_n)$ de E, nous pouvons construire la base duale $\mathcal{B}^\vee = (e_1^\vee, \dots, e_n^\vee)$ de $E^\vee$, définie par la condition satisfaisant $e_i^\vee(e_j) = \delta_{i,j}$ pour tout $i, j \in [\![1, n]\!]$. Alors un vecteur $v \in E \setminus F$ s'écrit $v = \sum_{i=1}^n a_i e_i$ avec $a_i \neq 0$ pour au moins un indice $i \in [\![k+1, n]\!]$. Ainsi $\alpha = e_i^\vee$ s'annule sur F mais pas en v. Donc v n'appartient pas à $\mathrm{Ker}(g)$.

Montrons ii). On a, si $F \subset G$ et $\alpha \in E^\vee$ n'annule sur G, alors $\alpha|_F = 0$. Donc $G^\perp \subset F^\perp$. Ensuite, si $G^\perp \subset F^\perp$ en utilisant i) on obtient $F \subset G$.

Pour iii), il est clair que $\alpha \in E^\vee$ s'annule en $F + G$ si et seulement si $\alpha|_G = 0$ et $\alpha|_F = 0$. Pour terminer la preuve, en appliquant iii) à $F_0 = F^\perp$ et $G_0 = G^\perp$ nous obtenons par i):

$$(F^\perp + G^\perp)^\perp = (F_0 + G_0)^\perp = F_0^\perp \cap G_0^\perp = F \cap G,$$

donc en utilisant de nouveau i):

$$F^\perp + G^\perp = (F \cap G)^\perp.$$

□

3.I.D.2. Dualité projective. — En cours de rédaction

3.I.E. Théorèmes classiques. — Nous allons traiter deux théorème classiques de la géométrie du plan projectif. Fixons donc un $\mathbb{K}$-espace vectoriel E de dimension 3 et le plan projectif $\mathbb{P}(E)$.

3.I.E.1. Théorème de Pappus. —

Théorème 3.I.7. — *Soit D et D' deux droites projectives distinctes d'un plan projectif. Soit $A, B, C \in D$ et $A', B', C' \in D'$ points deux à deux distincts. Alors les trois points $c = (AB') \cap (A'B)$, $a = (BC') \cap (B'C)$ et $b = (CA') \cap (C'A)$ sont alignés.*

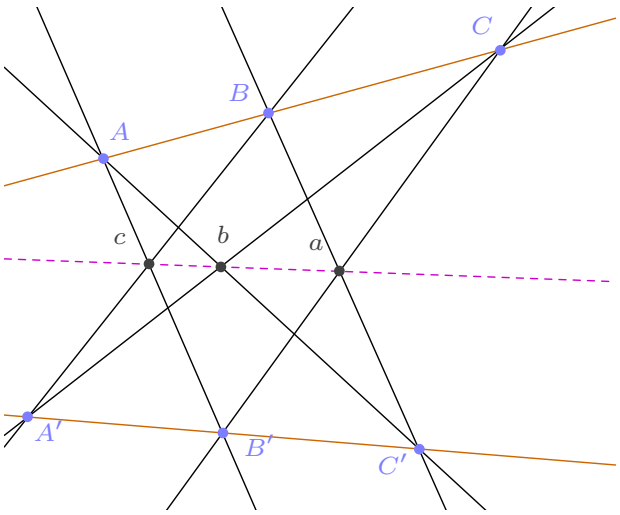


FIGURE 1. Théorème de Pappus

Démonstration. — Soit $O = D \cap D'$. Choisissons la (ab) comme droite à l'infini, donc considérons le plan affine $\mathbb{A}^2$ comme ouvert affine U_α de $\mathbb{P}^2$, où α est une forme linéaire qui définit la droite (ab). Il s'agit de montrer que c appartient à cette droite. Bien sûr, les traces des droites (AC') et $(C'B)$ sont parallèles dans $\mathbb{A}^2$, aussi bien que les droites (BC') et $(B'C)$. Comme il s'agit de montrer que $c = (AB') \cap (A'B)$ appartient à la droite à l'infini (ab), nous devons montrer que (AB') et $(A'B)$ sont parallèles. Nous examinons deux cas.

Si $O \notin (ab)$: Dans ce cas nous considérons l'homothétie φ de centre O qui envoie A sur B puis l'homothétie ψ de centre O qui envoie B sur C. On a $\psi(\varphi(A)) = C$. Puisque (AB') est parallèle à (BA'), le théorème de Thalès dit que $\varphi(B') = A'$. De même on a $\psi(C') = B'$. Or φ et ψ commutent, étant homothéties de même centre, donc $\psi(\varphi(C')) = \varphi(\psi(C')) = A'$. Ainsi (AC') et $(A'C)$ sont parallèles d'après la réciproque de Thalès.

En termes de rapports de similitude, nous pouvons écrire cela de la façon suivante. Comme (AB') est parallèle à (BA'), Thalès dit que, si $\lambda \in \mathbb{K}$ est tel que $\overrightarrow{OB} = \lambda\overrightarrow{OA}$, alors $\overrightarrow{OA'} = \lambda\overrightarrow{OB'}$. De même, si $\mu \in \mathbb{K}$ est tel que $\overrightarrow{OC} = \mu\overrightarrow{OB}$ alors $\overrightarrow{OB'} = \mu\overrightarrow{OC'}$. Ainsi, $\overrightarrow{OC} = \lambda\mu\overrightarrow{OA}$ et $\overrightarrow{OA'} = \lambda\mu\overrightarrow{OC'}$, ce qui veut dire que (AC') et $(A'C)$ sont parallèles.

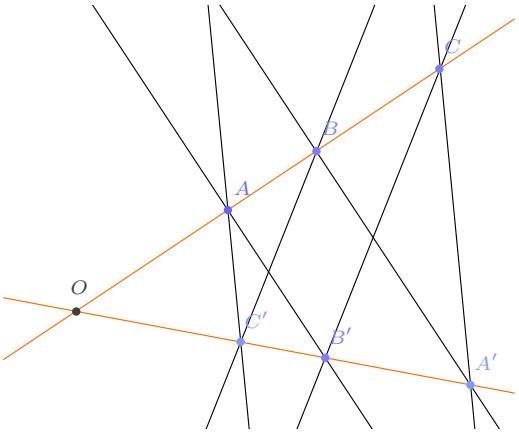


FIGURE 2. Pappus si $O \notin (ab)$

Si $O \in (ab)$: Dans ce cas on considère la translation φ d'axe $\vec{D}$ qui envoie A sur B puis la translation toujours d'axe $\vec{D}$ qui envoie B sur C. On a $\psi(\varphi(A)) = C$. Du parallélisme entre (AB') et $(A'B)$ on déduit $\varphi(B') = A'$, puis de même $\psi(C') = B'$. De nouveau les translations φ et ψ commutent donc $\psi(\varphi(C')) = A'$, ainsi (AC') et $(A'C)$ sont parallèles.

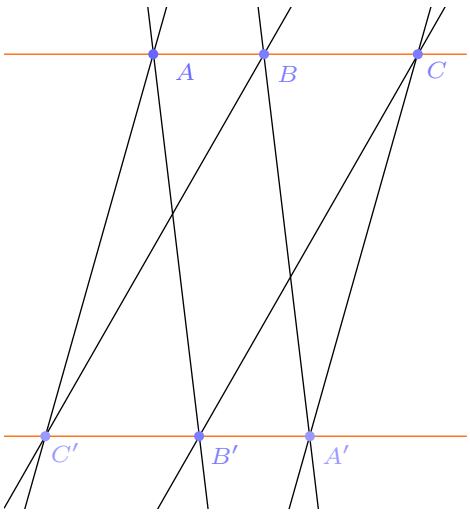


FIGURE 3. Pappus si $O \in (ab)$

□

3.I.E.2. Théorème Désargues. —

Théorème 3.I.8. — *Soit (A, B, C) et (A', B', C') deux triplets de points deux à deux distincts de $\mathbb{P}(E)$. Posons:*

$$\alpha = (BC) \cap (B'C'), \qquad \beta = (AC) \cap (A'C'), \qquad \gamma = (AB) \cap (A'B').$$

Alors les droites (AA'), (BB') et (CC') sont concourantes si et seulement si α, β et γ sont alignés.

Démonstration. — Démontrons une première implication : supposons que α, β et γ soient alignés et montrons que alors les droites (AA'), (BB') et (CC') sont concourantes.

Choisissons la droite H contenant α, β et γ comme droite à l'infini et considérons le plan affine $\mathcal{F} = \mathbb{P}(E) \setminus H$. Nous avons trois couples de droites parallèles de $\mathcal{F}$:

$$((BC), (B'C')), \qquad ((AC), (A'C')), \qquad \text{et } ((AB), (A'B')).$$

Montrons que (AA'), (BB') et (CC') sont parallèles ou concourantes. Ceci terminera la preuve de la première implication, car si (AA'), (BB') et (CC') sont parallèles, cela veut dire que ces trois droites ont un point d'intersection commun qui se trouve sur H. Pour conclure il suffit de montrer que, si deux parmi les trois droites (AA'), (BB') et (CC') sont incidentes – disons (AA') et (BB') – alors (AA'), (BB') et (CC') sont concourantes.

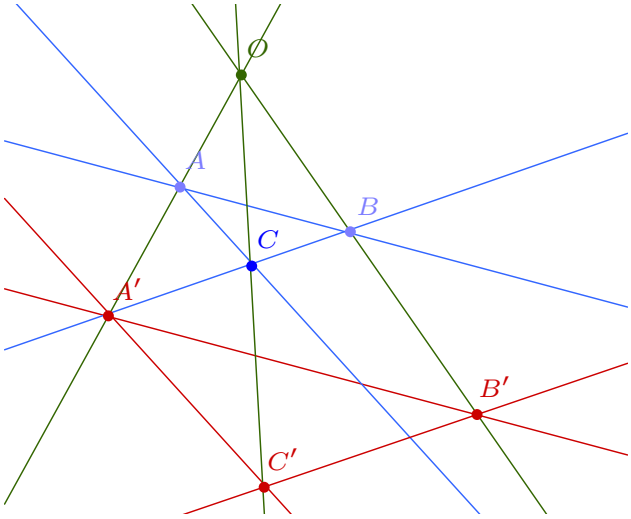


FIGURE 4. Théorème de Désargues

Soit donc $O = (AA') \cap (BB')$. Considérons la dilatation φ qui envoie A sur A'. Par le théorème de Thalès, comme (AB) et $(A'B')$ sont parallèles, le rapport de dilatation de φ est:

$$\frac{OA'}{OA} = \frac{OB'}{OB},$$

donc $\varphi(B) = B'$. On applique de nouveau Thalès pour calculer $\varphi(C)$: on découvre que $\varphi(C)$ se trouve sur la droite par A' parallèle à (AC), i. e., sur $(A'C')$, et bien sûr sur (OC) donc :

$$\varphi(C) = (A'C') \cap (OC).$$

De même en partant de B, on trouve $\varphi(C) = (B'C') \cap (OC)$. Ainsi, $\varphi(C) = (B'C') \cap (A'C') = C'$ se trouve sur (OC). Autrement dit, les droites (AA'), (BB') et (CC') sont incidentes en O.

Montrons maintenant l'implication réciproque, en faisant appel à la dualité. Posons:

$$X = (BC)^\perp, \qquad Y = (AC)^\perp, \qquad Z = (AB)^\perp,$$
$$X' = (B'C')^\perp, \qquad Y' = (A'C')^\perp, \qquad Z' = (A'B')^\perp.$$

On trouve donc deux triangles de $\mathbb{P}(E)^\vee$. Ils sont non dégénérés car les triangles de départ ne l'étaient pas. On a $A = (AB) \cap (AC)$ donc :

$$A^\perp = \mathrm{proj}((AB)^\perp, (AC)^\perp) = (YZ), \qquad B^\perp = (XZ), \qquad C^\perp = (AX).$$

Posons aussi:

$$\xi = (YZ) \cap (Y'Z'), \qquad \eta = (XZ) \cap (X'Z'), \qquad \zeta = (XY) \cap (X'Y').$$

Regardons l'effet de la dualité sur α. On a :

$$\alpha^\perp = ((BC) \cap (B'C'))^\perp = \mathrm{proj}((BC)^\perp, (B'C')^\perp) = (XX').$$

On obtient également :

$$\alpha^\perp = (XX'), \qquad \beta^\perp = (YY'), \qquad \gamma^\perp = (ZZ').$$

Étudions aussi la dualité sur (AA'). On a :

$$(AA')^\perp = \mathrm{proj}(A, A')^\perp = A^\perp \cap (A')^\perp = (YZ) \cap (Y'Z') = \xi.$$

De même :

$$(AA')^\perp = \xi, \qquad (BB')^\perp = \eta, \qquad (CC')^\perp = \zeta.$$

La deuxième implication est maintenant une conséquence de la première, appliquée aux triangles dans $\mathbb{P}(E)^\vee$. En effet, rappelons que trois droites du plan projectif sont concourantes si et seulement si les trois points correspondant dans le plan dual sont alignés. Alors, si (AA'), (BB') et (CC') sont concourantes, les trois points ξ, η et ζ sont alignés. Donc (XX'), (Y, Y') et (Z, Z') sont concourantes. Ainsi, α, β et γ sont alignés. □

3.II. Applications projectives

3.II.A. Applications projectives et linéaires. — Soit E et F espaces vectoriels sur $\mathbb{K}$. Soit $f : E \to F$. Alors f envoie une droite de E sur une droite de F si et seulement si la celle-ci n'est pas contenue dans le noyau de f.

Définition 3.II.1. — L'*application projective* φ associée à f est l'application :

$$\mathbb{P}(E) \setminus \mathbb{P}(\mathrm{Ker}(f)) \to \mathbb{P}(F),$$

qui, à une droite $[v]$ engendrée par $v \in E \setminus \mathrm{Ker}(f)$ associe $[f(v)]$.

On note $\mathbb{P}(E) \dashrightarrow \mathbb{P}(F)$ une application définie sur *une partie* de $\mathbb{P}(E)$.

On voit que, si on choisit $v' = \lambda v$ comme représentant de $[v]$, λ étant dans $\mathbb{K}^*$, on a $[f(v')] = [f(\lambda v)] = [\lambda(f(v))] = [f(v)]$, donc φ est bien définie.

Remarque 3.II.2. — Soit f et f' applications linéaires de E vers F. Alors f et f' définissent la même application projective si et seulement si $f = \lambda f'$ pour un $\lambda \in \mathbb{K}^*$.

Démonstration. — S'il existe $\lambda \in \mathbb{K}^*$ tel que $f = \lambda f'$, alors clairement $\mathrm{Ker}(f) = \mathrm{Ker}(f')$ et, pour tout $v \in E \setminus \mathrm{Ker}(f)$, on a $\varphi([v]) = [f(v)] = [\lambda f(v)]) = [f'(v)]$ donc f et f' induisent la même application projective.

Réciproquement, si f et f' définissent la même application projective, alors d'abord $\mathbb{P}(\mathrm{Ker}(f)) = \mathbb{P}(\mathrm{Ker}(f'))$ car les deux applications projectives doivent avoir le même domaine de définition. Ainsi $\mathrm{Ker}(f) = \mathrm{Ker}(f')$. Soit donc $B = (e_0, \dots, e_n)$ une base de E telle que $(e_0, \dots, e_k)$ est une base de $\mathrm{Ker}(f)$, posons $A_i = [e_i] \in \mathbb{P}(E)$ pour tout $i \in [\![k+1, n]\!]$ et $A_{n+1} = [e_0 + \cdots + e_n]$.

On a $A_i \in \mathbb{P}(E) \setminus \mathbb{P}(\mathrm{Ker}(f))$ pour $i \geq k+1$ donc $\varphi(A_i) = [f(e_i)] = [f'(e_i)]$, ainsi pour tout $i \in [\![k+1, n+1]\!]$ il existe $\lambda_i \in \mathbb{K}^*$ tel que $f(e_i) = \lambda_i f'(e_i)$. De plus, une base de $\bar{E} = E/\mathrm{Ker}(f)$ est constituée de $(\bar{e}_{k+1}, \dots, \bar{e}_{n+1})$ et l'application $\bar{f} : \bar{E} \to F$ définie par $\bar{f}(\bar{v}) = f(v)$ est injective. Ainsi, $(f(e_{k+1}), \dots, f(e_{n+1}))$ est une base de $\mathrm{Im}(f) \subset F$. Donc, de la relation:

$$\lambda_{n+1} f(e_{n+1}) = \lambda_{n+1}(f(e_k) + \cdots + f(e_n)) = \lambda_{k+1} f(e_k) + \cdots + \lambda_n f(e_n)$$

on déduit $\lambda_{n+1} = \lambda_i$ pour tout $i \in [\![k+1, n]\!]$. Nous avons montré $f' = \lambda_{n+1} f$. □

Exemple 3.II.3. — Soit F et G sous espaces de E tels que $E = F \oplus G$. Alors la *projection sur* $\mathbb{P}(F)$ *parallèle à* $\mathbb{P}(G)$ est l'application projective:

$$\pi : \mathbb{P}(E) \setminus \mathbb{P}(G) \to \mathbb{P}(F)$$

associée à la projection linéaire p de E sur F parallèle à G.

De façon géométrique, l'image d'un point $P \in \mathbb{P}(E)$ par π est le point d'intersection de l'espace G_P, que l'on définit comme $\mathrm{proj}(\mathbb{P}(G), P)$ avec $\mathbb{P}(F)$:

$$\pi(P) = G_P \cap \mathbb{P}(F).$$

Posons $c = \dim(G)$ et remarquons que $\dim(F) = n + 1 - c$ i. e. $\mathrm{codim}(\mathbb{P}(F)) = c$. Aussi, si $P \notin \mathbb{P}(G)$ et $P = [v]$, pour un certain $v \in E$, on a bien $\dim(G \oplus \mathbb{K}v) = c + 1$ et bien sûr $F + G + \mathbb{K}v = E$. Donc:

$$\dim(F \cap (G + \mathbb{K}v)) = (n + 1 - c) + (c + 1) - (n + 1) = 1.$$

De ce fait, on voit que l'intersection $G_P \cap \mathbb{P}(F)$ est bien un point, qui appartient à $\mathbb{P}(F)$. Si l'on écrit $v = u + w$, avec $u \in F$ et $w \in G$ alors $p(v) = u$ et $\pi([v]) = [u]$ et $u = -w + v \in G + \mathbb{K}v$, donc le point $G_P \cap \mathbb{P}(F)$ est bien $\pi([v])$.

Soit $\mathcal{R} = (A_0, \dots, A_{n+1})$ et $\mathcal{S} = (B_0, \dots, B_{m+1})$ sont des repères projectifs de $\mathbb{P}(E)$ et $\mathbb{P}(F)$, nous pouvons choisir $(u_0, \dots, u_{n+1})$ et $(v_0, \dots, v_{m+1})$ vecteurs de E et F tels que $A_i = [u_i]$ et $B_j = [v_j]$ pour tout i et j. Nous avons des bases $B = (u_0, \dots, u_n)$ de E et $C = (v_0, \dots, v_m)$ de F.

Nous considérons alors la matrice $\mathrm{Mat}_{C,B}(f)$. Cette matrice est déterminée à un scalaire non nul près, nous notons $\mathrm{Mat}_{\mathcal{S},\mathcal{R}}(\varphi)$ une quelconque des matrices, avec un certain abus de notation.

3.II.B. Applications projectives et affines. —

3.II.B.1. Complétion projective des applications affines. — Soit $\mathcal{E}$ et $\mathcal{F}$ espaces affines et $\varphi : \mathcal{E} \to \mathcal{F}$ une application affine. Soit $O \in \mathcal{E}$ et $Q \in \mathcal{F}$. Considérons $\mathcal{E}$ et $\mathcal{F}$ comme parties affines des espaces projectifs $\hat{\mathcal{E}}$ et $\hat{\mathcal{F}}$. Posons $\vec{w} = \overrightarrow{Q\varphi(O)}$.

Définition 3.II.4. — L'application projective $\hat{\varphi} : \hat{\mathcal{E}} \dashrightarrow \hat{\mathcal{F}}$ définie par:

$$\hat{\varphi}(\lambda : \overrightarrow{OP}) = (\lambda : \lambda\vec{w} + \vec{\varphi}(\overrightarrow{OP}))$$

est le *complété projectif* de φ. C'est une application définie en $\hat{\mathcal{E}} \setminus \mathbb{P}(\mathrm{Ker}(\vec{\varphi}))$.

Remarque 3.II.5. — La restriction de $\hat{\varphi}$ à $\mathcal{E}$ est φ.

Démonstration. — L'espace affine $\mathcal{E}$ est plongé dans $\hat{\mathcal{E}}$ comme l'ensemble des points des la forme $(1 : \overrightarrow{OP})$, quelque soit P dans $\mathcal{E}$. Sur ces points, $\hat{\varphi}$ prend valeur

$$(1 : \vec{w} + \vec{\varphi}(\overrightarrow{OP}) = \left(1 : \overrightarrow{Q\varphi(O)} + \overrightarrow{\varphi(O), \varphi(P)}\right) = (1 : \overrightarrow{Q\varphi(P)}),$$

ce qui représente le point $\varphi(P)$ dans $\mathcal{F} \subset \hat{\mathcal{F}}$. □

Décrivons $\hat{\varphi}$ en coordonnées. Notons E la direction de $\mathcal{E}$ et F celle de $\mathcal{F}$. Soit $\mathcal{R} = (O, \vec{u}_1, \dots, \vec{u}_n)$ un repère cartésien de $\mathcal{E}$ et $\mathcal{S} = (Q, \vec{v}_1 \dots, \vec{v}_m)$ un repère cartésien de $\mathcal{F}$. On a donc $B = (\vec{u}_1, \dots, \vec{u}_n)$ base de E et $C = (\vec{v}_1, \dots, \vec{v}_m)$ base de F. Fixons donc $\hat{u}_0 = (1 : \vec{0}) \in \mathbb{K} \oplus E$ et, pour $i \in [\![1, n]\!]$, $\hat{u}_i = (0 : u_i) \in \mathbb{K} \oplus E$, ainsi $\hat{B} = (\hat{u}_0, \dots, \hat{u}_n)$ est une base de $\mathbb{K} \oplus E$. Avec des notations analogues, $\hat{C} = (\hat{v}_0, \dots, \hat{v}_m)$ est une base de $\mathbb{K} \oplus F$. Nous posons $\hat{u}_{n+1} = \hat{u}_0 + \cdots + \hat{u}_n$ et $\hat{v}_{m+1} = \hat{v}_0 + \cdots + \hat{v}_m$ et considérons les repères projectifs $\hat{\mathcal{R}}$ et $\hat{\mathcal{S}}$ en prenant les droites associées aux $(n+2)$ et $(m+2)$ vecteurs que l'on vient de définir.

Soit maintenant $a_i \in \mathbb{K}$ tels que le point $\varphi(O)$ ait coordonnées $\mathrm{Mat}_{\mathcal{S}}(\varphi(O)) = (1, a_{1,0}, \dots, a_{m,0})$ en le repère $\mathcal{S}$ et considérons la matrice $\mathrm{Mat}_{C,B}(\vec{\varphi}) = (m_{i,j})$ de $\vec{\varphi}$ en les bases C et B, donc:

$$\vec{\varphi}(x_1 \vec{u}_1 + \cdots + x_n \vec{u}_n) = \sum_{i=1}^{m} a_{i,j} \vec{v}_i.$$

Soit $f : \mathbb{K} \oplus E \to \mathbb{K} \oplus F$ l'application linéaire définie par

$$f(\lambda, \vec{u}) = (\lambda, \lambda \vec{w} + \vec{\varphi}(\vec{v}))$$

L'application $\hat{\varphi}$ est induite par f. La matrice de f en les bases $\hat{C}$, $\hat{B}$ est

$$\mathrm{Mat}_{\hat{\mathcal{S}},\hat{\mathcal{R}}}(\hat{\varphi}) = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_{1,0} & a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \ddots & \\ a_{m,0} & a_{m,1} & \cdots & a_{m,n} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ a^t & M \end{pmatrix},$$

où $a = (a_{1,0}, \dots, a_{m,0})$. Il s'agit précisément de la matrice $\mathrm{Mat}_{\mathcal{R},\mathcal{S}}(\varphi)$.

3.II.B.2. Application affine induite par une application projective. — Soit $\varphi : \mathbb{P}(E) \dashrightarrow \mathbb{P}(F)$ une application projective, H et K des hyperplans de $\mathbb{P}(E)$ et $\mathbb{P}(F)$, posons $\mathcal{E} = \mathbb{P}(E) \setminus H$ et $\mathcal{F} = \mathbb{P}(F) \setminus K$. On se demande quand φ est le complété d'une application affine $\mathcal{E} \to \mathcal{F}$.

Soit $f : E \to F$ linéaire induisant φ, $\alpha \in E^\vee$ et $\beta \in F^\vee$ tels que $H = \mathbb{P}(\mathrm{Ker}(\alpha))$ et $K = \mathbb{P}(\mathrm{Ker}(\beta))$. On considère aussi $f^\vee : F^\vee \to E^\vee$.

Proposition 3.II.6. — *L'application φ se restreint à une application affine $\varphi_0 : \mathcal{E} \to \mathcal{F}$ induisant φ si et seulement si $\varphi(H) \subset K$. Ceci arrive si et seulement s'il existe $\lambda \in \mathbb{K}^*$ tel que $f^\vee(\beta) = \lambda\alpha$.*

Démonstration. — Pour que φ soit définie sur $\mathcal{E}$ il faut et il suffit que, pour tout $v \in E \setminus \mathrm{Ker}(\alpha)$, on ait $f(v) \in F \setminus \mathrm{Ker}(\beta)$. Autrement dit, il faut que $f(v) \in \mathrm{Ker}(\beta) = \mathrm{Ker}(f^\vee(\beta))$ implique $v \in \mathrm{Ker}(\alpha)$, i. e. :

$$\mathrm{Ker}(f^\vee(\beta)) \subset \mathrm{Ker}(\alpha).$$

Ceci arrive si et seulement si $f^\vee(\beta)$ est un multiple non nul de α. □

3.II.C. Homographies et repères. —

Définition 3.II.7. — Une *homographie* est une application projective bijective, i. e., une application projective induite par un isomorphisme linéaire.

Proposition 3.II.8. — *Soit $(A_0, \dots, A_{n+1})$ et $(B_0, \dots, B_{n+1})$ repères projectifs de deux espaces projectifs $\mathbb{P}(E)$ et $\mathbb{P}(F)$ de dimension n. . Alors il existe une et une seule homographie $\varphi : \mathbb{P}(E) \to \mathbb{P}(F)$ telle que $\varphi(A_i) = B_i$ pour tout $i \in [\![0, n+1]\!]$.*

Démonstration. — Soit $(u_0, \dots, u_n)$ et $(v_0, \dots, v_n)$ bases de E et de F telles que:

$$\begin{aligned} A_i &= [u_i], && \forall i \in [\![0, n+1]\!], \\ A_{n+1} &= [u_0 + \cdots + u_n], \\ B_i &= [v_i], && \forall i \in [\![0, n+1]\!], \\ B_{n+1} &= [v_0 + \cdots + v_n]. \end{aligned}$$

Alors nous définissons l'isomorphisme $f : E \to F$ par $f(u_n i) = v_i$, $\forall i \in [\![0, n+1]\!]$ et nous en déduisons $f(u_0 + \cdots + u_n) = v_0 + \cdots + v_n$, donc l'application projective φ associée à f est l'homographie cherchée.

Si $g : E \to F$ est une deuxième application linéaire dont l'application projective associée ψ est une homographie telle que $\psi(A_i) = B_i$ pour tout $i \in [\![0, n+1]\!]$, alors pour tout $i \in [\![0, n+1]\!]$ il existe $\lambda_i \in \mathbb{K}^*$ tel que $g(u_i) = \lambda_i v_i$ et $g(u_0 + \cdots + u_n) = \lambda_{n+1}(v_0 + \cdots + v_n)$. Donc $\lambda_{n+1}(v_0 + \cdots + v_n) = \lambda_0 v_0 + \cdots + \lambda_n v_n$. Comme $(v_0, \ldots, v_n)$ est une base de F, on en déduit $\lambda_i = \lambda_{n+1}$ pour tout $i \in [\![0, n+1]\!]$. Ainsi $g = \lambda_{n+1} f$ donc $\varphi = \psi$. □

3.II.D. Groupe des homographies. —

Définition 3.II.9. — Le *groupe des homographies* $\mathrm{PGL}(E)$ est le groupe des applications projectives bijectives de l'espace projectif $\mathbb{P}(E)$, muni de la loi de composition, avec élément neutre $\mathrm{id}_{\mathbb{P}(E)}$. On écrit $\mathrm{PGL}_{n+1}(\mathbb{K}) = \mathrm{PGL}(\mathbb{K}^{n+1})$.

Proposition 3.II.10. — *On a* $\mathrm{PGL}(E) = \mathrm{GL}(E)/\mathbb{K}^*\mathrm{id}_E$*, où le groupe des homothéties* $\mathbb{K}^*\mathrm{id}_E$ *est le centre de* $\mathrm{GL}(E)$*.*

Démonstration. — Une homographie est déterminée par un automorphisme de E, et cela à un scalaire multiplicatif non nul près, donc $\mathrm{PGL}(E)$ s'identifie à $\mathrm{GL}(E)/\mathbb{K}^*\mathrm{id}_E$, et cela en respectant la structure de groupe.

Les homothéties sont dans le centre de $\mathrm{GL}(E)$. Réciproquement, si $g \in \mathrm{GL}(E)$ est dans le centre de $\mathrm{GL}(E)$, déjà g commute avec toute transvection. Mais si f est une transvection de droite D, alors gfg^{-1} est une transvection de droite $g(D)$, donc on aurait $g(D) = D$. En prenant des droites $D_i = \mathrm{vect}(u_i)$, où $(u_1, \ldots, u_n)$ est une base de E, on obtient pour tout $i \in [\![1, n]\!]$, $g(u_i) \in \mathrm{vect}(u_i)$ donc il existe $\lambda_i \in \mathbb{K}^*$ tel que $g(u_i) = \lambda_i u_i$. Mais il existe aussi $\lambda \in \mathbb{K}^*$ tel que $g(u_1 + \cdots + u_n) = \lambda(u_1 + \cdots + u_n)$. On obtient, comme $(u_1, \ldots, u_n)$ est une base, que $\lambda = \lambda_i$ quelque soit $i \in [\![1, n]\!]$. Ceci montre que g est une homothétie, de rapport λ. □

3.II.E. Birapport. — Fixons dans la droite $\mathbb{P}^1 = \mathbb{P}(\mathbb{K}^2)$ formée des points $(x_0 : x_1)$ la partie affine $U_1 = \{(x_0 : x_1) \mid x_1 \neq 0\}$ et le point à l'infini $\infty = (1 : 0)$. Ainsi un élément $x \in \mathbb{K}$ se voit en tant que élément de U_1 comme $(x : 1)$ et avec ces identifications nous écrivons $\mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$.

Définition 3.II.11. — Soit $\mathbb{L} = \mathbb{P}(E)$ une droite projective et A, B, C trois points deux à deux distincts de $\mathbb{P}(E)$. Soit $\varphi : \mathbb{P}(E) \to \mathbb{P}^1$ l'unique homographie qui envoie A sur ∞, B sur 0 et C sur 1. Alors, pour $D \in \mathbb{P}(A)$ le birapport $[A, B, C, D]$ est :

$$[A, B, C, D] = \varphi(D) \in \mathbb{K} \cup \{\infty\}.$$

Remarque 3.II.12. — Par définition nous avons:

$$\begin{aligned} [A, B, C, D] = \infty \quad &\Longleftrightarrow \quad D = A, \\ [A, B, C, D] = 0 \quad &\Longleftrightarrow \quad D = B, \\ [A, B, C, D] = 1 \quad &\Longleftrightarrow \quad D = C. \end{aligned}$$

Proposition 3.II.13. — *Soit* $\mathbb{P}(E)$ *et* $\mathbb{P}(E')$ *droites projectives et* A, B, C, D *points de* $\mathbb{P}(E)$*,* A', B', C', D' *points de* $\mathbb{P}(E')$*, dont* A, B, C *et* A', B', C' *deux à deux distincts. Alors* $[A, B, C, D] = [A', B', C', D']$ *si et seulement s'il existe une homographie* $\mathbb{P}(E) \to \mathbb{P}(E')$ *qui envoie* A *sur* A'*,* B *sur* B'*,* C *sur* C'*,* D *sur* D'*.*

Démonstration. — Il existe deux homographies, chacune étant uniquement déterminée, $\varphi : \mathbb{P}(E) \to \mathbb{P}^1$ et $\varphi' : \mathbb{P}(E') \to \mathbb{P}^1$ telles que :

$$\varphi(A) = \varphi'(A') = \infty, \qquad \varphi(B) = \varphi'(B') = 0, \qquad \varphi(C) = \varphi'(C') = 1.$$

Par définition de birapport, $\varphi(D) = \varphi'(D')$ si et seulement si on a égalité de birapports $[A,B,C,D] = [A',B',C',D']$. Dans ce cas, l'homographie $(\varphi')^{-1} \circ \varphi$ envoie A sur A', B sur B', C sur C', D sur D'.

Réciproquement, si une homographie $\psi : \mathbb{P}(E) \to \mathbb{P}(E')$ existe qui envoie A sur A', B sur B', C sur C', D sur D', alors $\varphi' \circ \psi$ coïncide avec φ sur sur A, B et C, donc partout. Ainsi :

$$[A,B,C,D] = \varphi(D) = \varphi'(\psi(D)) = \varphi'(D') = [A',B',C',D'].$$

□

Remarque 3.II.14. — Soit φ une homographie de $\mathbb{P}^1 = \mathbb{K} \cup \{\infty\}$. Alors il existe $a,b,c,d \in \mathbb{K}$ avec $ad - ba \neq 0$ tels que φ s'écrit :

$$\varphi(z) = \frac{az+b}{cz+d}.$$

En effet, si $z \neq \infty$ alors on identifie z à $(z:1)$ et φ s'écrit en coordonnées :

$$\varphi(z) = \varphi(z:1) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \frac{az+b}{cz+d}.$$

Cette expression a un sens même si $z = \infty$, que l'on identifie à $(1:0)$. Bien sûr $ad-ba$ est le déterminant de la matrice ci-dessus, qui est la matrice en la base canonique de l'application linéaire à laquelle est associée l'homographie : il est donc non nul.

Proposition 3.II.15. — *Soit $A,B,C \in \mathbb{K} \cup \{\infty\}$ deux à deux distincts. Alors, pour tout $D \in \mathbb{K} \cup \{\infty\}$, on a le birapport :*

$$[A,B,C,D] = \frac{D-B}{D-A} \Big/ \frac{C-B}{C-A}.$$

Dans la proposition ci-dessus, on utilise implicitement les règles :

$$\frac{A}{0} = \infty, \qquad \frac{A}{\infty} = 0, \qquad A + \infty = \infty, \qquad A\infty = \infty.$$

Démonstration. — On considère l'homographie $\varphi : \mathbb{K} \cup \{\infty\} \to \mathbb{K} \cup \{\infty\}$ définie par:

$$\varphi(z) = \frac{z-B}{z-A} \Big/ \frac{C-B}{C-A}.$$

En effet, d'après la remarque précédente, cette expression est celle d'une homographie.

Alors $\varphi(A) = \infty$, $\varphi(B) = 0$ et $\varphi(C) = 1$. Donc $\varphi(D) = [A,B,C,D]$, ce qui achève la démonstration. □

Proposition 3.II.16. — *Soit A,B,C points deux à deux distincts d'une droite projective $\mathbb{L}$ et $D \in \mathbb{L}$. Posons $\lambda = [A,B,C,D] \in \mathbb{K} \cup \{\infty\}$. Alors:*

$$[B,A,C,D] = [A,B,D,C] = \lambda^{-1}; \qquad [A,C,B,D] = 1 - \lambda.$$

En particulier, les valeurs du birapport sur les 24 permutations de (A,B,C,D) sont:

$$\lambda, \quad \frac{1}{\lambda}, \quad 1-\lambda, \quad 1-\frac{1}{\lambda}, \quad \frac{1}{1-\lambda}, \quad \frac{\lambda}{\lambda-1}.$$

Démonstration. — Soit $\mathbb{L} = \mathbb{P}(E)$ et (u_0,u_1) base de E telle que $A = [u_0]$, $B = [u_1]$, $C = [u_0+u_1]$. Alors il existe un couple $(x_0,x_1) \in \mathbb{K}^2$ tel que $D = [x_0u_0 + x_1u_1]$, et ce couple est unique à un scalaire non nul multiplicatif près. On a alors $[A,B,C,D] = (x_0 : x_1) \in \mathbb{P}^1$, i. e. $[A,B,C,D] = x_0/x_1 \in \mathbb{K} \cup \{\infty\}$. En effet, l'homographie associée au morphisme qui envoie u_0 sur $(1,0)$ et u_1 sur $(0,1)$ – et par conséquent u_0+u_1 sur $(1,1)$ – envoie D sur $(x_0:x_1)$.

On considère alors la base $(u_0',u_1') = (-u_0, u_0+u_1)$. On a $[u_0'] = A$, $[u_1'] = C$, $[u_0'+u_1'] = B$, donc :

$$x_0u_0 + x_1u_1 = (x_1 - x_0)u_0' + x_1u_1'.$$

Donc $[A,C,B,D] = (x_1 - x_0 : x_1)$, i. e.:

$$[A,C,B,D] = \frac{x_1 - x_0}{x_1} = 1 - \lambda.$$

Pour les autres égalités, on a une base $(u_0', u_1') = (u_1, u_0)$ donc $u_0 + u_1 = u_0' + u_1'$ et $[x_1 u_0' + x_0 u_1'] = D$ donc $[B,A,C,D] = (x_1 : x_0) = \lambda^{-1}$. Pour l'égalité qui reste à montrer, elle a un sens à priori seulement si $B \neq D \neq A$. Dans ce cas, $x_0 \neq 0 \neq x_1$. Nous prenons alors $u_0' = x_0 u_0$ et $u_1' = x_1 u_1$ de sorte que $D = [u_0' + u_1']$. Alors:

$$(A,B,D,C) = \left(\frac{1}{x_0} : \frac{1}{x_1}\right) = \frac{x_1}{x_0} = \frac{1}{\lambda}.$$

On voit par les mêmes arguments que :

$$[A,B,C,D] = [B,A,D,B] = [D,C,B,A] = [C,D,A,B].$$

Considérons alors l'opération $\mathfrak{S}_4$ par permutation de $\{A,B,C,D\}$ et l'action induite sur $\mathbb{P}^1$, ensemble des birapports. Soit $\mathcal{O}(\lambda)$ l'orbite de $\lambda = [A,B,C,D]$ pour cette action. Le sous groupe de Klein K de $\mathfrak{S}_4$ constitué de

$$K = \{\mathrm{id}, (12)(34), (14)(23), (13)(24)\}$$

est donc dans le stabilisateur de λ, $\mathcal{O}(\lambda)$ est un diviseur de $6 = 24/4 = |\mathfrak{S}_4|/|K|$. D'ailleurs, si on fait opérer $\mathfrak{S}_4$ sur l'ensemble, de cardinal 3, des produits de deux permutations disjointes sur 4 éléments, on voit que K est le stabilisateur d'un tel produit et que $\mathfrak{S}_4/K \simeq \mathfrak{S}_3$.

Par ailleurs, $\mathfrak{S}_3$ opère sur $\mathcal{O}(\lambda) \subset \mathbb{P}^1$ par homographies, par une représentation:

$$\rho : \mathfrak{S}_3 \to \mathrm{PGL}_2(\mathbb{Z}).$$

En effet, (12) envoie λ sur $1/\lambda$, (24) sur $1-\lambda$, $(132) = (23)(12)$ sur $1 - 1/\lambda$, $(123) = (12)(23)$ sur $1/(1-\lambda)$, Nous avons:

$$\rho(\overline{12}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \rho(\overline{24}) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \qquad \rho(\overline{132}) = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Les autres cas sont laissés par exercice. □

CHAPITRE 4

GROUPE LINÉAIRE

Ce chapitre est très inspiré par [**Per96**]. Nous fixons un espace vectoriel E sur un corps $\mathbb{K}$. Nous notons en général n la dimension de E.

4.I. Propriétés de base

Définition 4.I.1. — Le *groupe linéaire* $\mathrm{GL}(E)$ est le groupe des automorphismes de E avec la loi de composition, dont l'élément neutre est l'identité. Le groupe *spécial linéaire* $\mathrm{SL}(E)$ est le groupe des automorphismes de déterminant 1.

Une fois fixée une base de E, le groupe $\mathrm{GL}(E)$ devient isomorphe au groupe $\mathrm{GL}_n(\mathbb{K})$ des matrices inversibles de taille n, tandis que $\mathrm{SL}(E)$ devient isomorphe au groupe $\mathrm{SL}_n(\mathbb{K})$ des matrices de taille n et de déterminant 1.

4.I.A. Générateurs. —

4.I.A.1. Dilatations. — Soit H un hyperplan de E et D une droite de E, avec

$$D \not\subset H.$$

Définition 4.I.2. — Une *dilatation* d'hyperplan H, de rapport $1 \neq \lambda \in \mathbb{K}^*$ et de droite D est un endomorphisme f de E tel que $H = \mathrm{Ker}(f - \mathrm{id}_E)$ et $D = \mathrm{Ker}(f - \lambda \mathrm{id}_E)$.

Parfois, id_E est considérée aussi une dilatation.

Proposition 4.I.3. — *Soit H un hyperplan de E, $f \in \mathrm{GL}(E)$ telle que $f|_H = \mathrm{id}_H$ et $\lambda \in \mathbb{K}^* \setminus \{1\}$. Les propriétés suivantes sont équivalentes :*

i) le morphisme f est une dilatation d'hyperplan H et de rapport λ ;

ii) le morphisme f est diagonalisable, semblable à $\mathrm{diag}(1, \dots, 1, \lambda)$;

iii) on a $\det(f) = \lambda$;

iv) on a $\mathrm{Im}(f - \mathrm{id}_E) \not\subset H$.

Si ces conditions sont vérifiées, alors f est une dilatation de droite $D = \mathrm{Im}(f - \mathrm{id}_E)$.

Démonstration. — Voyons que i)⇒ii). Si f une dilatation de rapport λ, alors f est diagonalisable, car l'on peut choisir une base de E formée de $n-1$ vecteurs libres de H et d'un vecteur non nul de $D = \mathrm{Ker}(f - \lambda \mathrm{id}_E)$.

Clairement, ii)⇒iii). Aussi, ii)⇒i) car nous avons déjà H comme espace propre de la valeur propre 1, donc $D = \mathrm{Ker}(f - \lambda \mathrm{id}_E)$ est un supplémentaire de H.

Montrons iii)⇒iv). Remarquons que, par le théorème du rang, on a $\dim(\mathrm{Im}(f - \mathrm{id}_E)) = 1$. Soit u vecteur propre de la valeur propre λ, donc $u \notin H$. On a $f(u) = \lambda u$ donc $f - \mathrm{id}_E(u) = (\lambda - 1)u \notin H$, car $u \notin H$ et $\lambda \neq 1$. Ainsi $\mathrm{Im}(f - \mathrm{id}_E) = \mathrm{vect}(u) \not\subset H$, donc nous avons iv).

Montrons iv)⇒ii). Prenons une base B de E formée de $n-1$ vecteurs libres de H et d'un vecteur non nul u, générateur de $D = \mathrm{Im}(f - \mathrm{id}_E)$. Le vecteur $f(u) - u$ appartient à D donc $f(u) - u = \mu u$ pour un certain $\mu \in \mathbb{K}$. Au fait $\mu \neq 0$ car sinon $f(u) = u$, i. e. $u \in H$ ce qui est exclu. Donc $f(u) = (1+\mu)u$, d'où $\mathrm{Mat}_B(f) = \mathrm{diag}(1, \ldots, 1, \lambda)$, où $\lambda = 1 + \mu \in \mathbb{K} \setminus \{1\}$.

Les quatre conditions sont donc équivalentes. La droite de dilatation est donc $D = \mathrm{Ker}(f - \lambda \mathrm{id}_E)$. Dans la démonstration de iii)⇒iv) nous avons vu qu'un vecteur propre u de la valeur propre λ – i. e., un générateur de D – est envoyé par $f - \mathrm{id}_E$ sur un multiple de u qui est un générateur de $\mathrm{Im}(f - \mathrm{id}_E)$, donc $D = \mathrm{Im}(f - \mathrm{id}_E)$. □

4.I.A.2. Transvections. — Soit H un hyperplan de E et D une droite de E, avec :

$$D \subset H.$$

Définition 4.I.4. — Une *transvection* d'hyperplan H et de droite D est un endomorphisme inversible f de E tel que $H = \mathrm{Ker}(f - \mathrm{id}_E)$ et $D = \mathrm{Im}(f - \mathrm{id}_E)$.

Proposition 4.I.5. — *Soit $H = \ker(\alpha)$ un hyperplan de E, $f \in \mathrm{GL}(E) \setminus \{\mathrm{id}_E\}$ telle que $f|_H = \mathrm{id}_H$. Les propriétés suivantes sont équivalentes :*

i) le morphisme f est une transvection ;

ii) le morphisme f n'est pas diagonalisable ;

iii) on a $\det(f) = 1$;

iv) on a $\mathrm{Im}(f - \mathrm{id}_E) \subset H$;

v) l'homomorphisme $\bar{f} : E/H \to E/H$ induit par f est l'identité ;

vi) il existe $w \in H$ tel que, pour tout $v \in E$ on ait :

$$f(v) = v + \alpha(v)w;$$

vii) il existe un base B de E telle que :

$$\mathrm{Mat}_B(f) = \begin{pmatrix} 1 & 0 & & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ 0 & \ddots & \ddots & 0 & 0 \\ 0 & & 0 & 1 & 1 \\ 0 & & \cdots & 0 & 1 \end{pmatrix}$$

Si ces conditions sont vérifiées, alors f est une dilatation de droite $D = \mathrm{Im}(f - \mathrm{id}_E)$.

Démonstration. — Le schéma est i) ⇒ iv) ⇒ vii) ⇒ iii) ⇒ ii) ⇒ vii) ⇒ i). Ensuite on montre v) ⇔ vii) et iv) ⇔ vi).

i) ⇒ iv). C'est par définition.

iv) ⇒ vii). On choisit une base appropriée $(u_1, \ldots, u_n)$ de E en commençant par $u_n \notin H$. L'espace $D = \mathrm{Im}(f - \mathrm{id}_E)$ est une droite d'après le théorème du rang, car $f \neq \mathrm{id}_E$ et $H \subset \ker(f - \mathrm{id}_E)$, donc $H = \ker(f - \mathrm{id}_E)$ et $\dim \ker(f - \mathrm{id}_E) = n - 1$.

De $u_n \notin H$ on déduit $f(u_n) - u_n \neq 0$. On pose alors $u_{n-1} = f(u_n) - u_n$ et on trouve $f(u_n) = u_{n-1} + u_n$. De plus $u_{n-1} \in H$ par hypothèse. On complète u_{n-1} à une base $(u_1, \ldots, u_{n-1})$ de H. Soit $B = (u_1, \ldots, u_n)$. La matrice $\mathrm{Mat}_B(f)$ a la forme voulue.

vii) ⇒ iii). Évident.

iii) ⇒ ii). Si f était diagonalisable, on aurait $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ valeurs propres de f avec $1 = \det(f) = \prod_{i=1}^n \lambda_i$. Mais $H = \ker(f - \mathrm{id}_E)$ est un hyperplan donc $\lambda_1 = \cdots = \lambda_{n-1} = 1$. Donc $\lambda_n = 1$, ainsi la matrice de f dans une base quelconque est semblable à $\mathbb{1}_n$. Mais alors $f = \mathrm{id}_E$, ce qui n'est pas.

ii) ⇒ vii). La matrice de la forme requise pour vii) est une matrice de Jordan ayant $n-2$ blocs de taille 1 et 1 bloc de taille 2, tous associés à la valeur propre 1. Nous avons déjà $n-1$ vecteurs propres libres associés à la valeur propre 1 : il suffit de choisir une base de H,

ainsi il ne peut y avoir de blocs de Jordan de taille supérieure à 2. Pour conclure, il suffit donc de montrer que f est trigonalisable mais pas diagonalisable (donc qu'il existe un bloc de Jordan de taille supérieure à 1), et que toutes les valeurs propres sont 1.

Or, nous avons 1, valeur propre de multiplicité géométrique $n-1$, donc de multiplicité algébrique au moins n, ainsi f est trigonalisable car le polynôme caractéristique est scindé sur $\mathbb{K}$: il vaut $(x-1)^{n-1}(x-\lambda)$, pour un certain $\lambda \in \mathbb{K}^*$. Mais si $\lambda \neq 1$, f serait diagonalisable, donc au fait $\lambda = 1$, et nous avons un bloc de Jordan de taille 2, ce qui achève la démonstration.

vii) $\Rightarrow$ i). Soit $B = (u_1, \dots, u_n)$. On a $H = \ker(f - \mathrm{id}_E) = \mathrm{vect}(e_1, \dots, e_{n-1})$ et $\mathrm{Im}(f - \mathrm{id}_E) = \mathrm{vect}(e_{n-1}) \subset H$, donc f est une transvection.

vii) $\Rightarrow$ v). Soit $B = (u_1, \dots, u_n)$. On a $H = \ker(f - \mathrm{id}_E) = \mathrm{vect}(e_1, \dots, e_{n-1})$. Notons $\bar{v}$ la classe de $v \in E$ dans E/H. On a $E/H = \mathrm{vect}(\bar{u}_n)$ et $f(u_n) = u_n + u_{n-1}$ donc $\bar{f}(\bar{u}_n) = \bar{u}_n$, ce qui montre v).

vii) $\Leftarrow$ v). On sait $H = \ker(f - \mathrm{id}_E)$, car $H \subset \ker(f - \mathrm{id}_E)$ et $f \neq \mathrm{id}_E$. Soit u_n un vecteur de $E \setminus H$. On a $\bar{f}(\bar{u}_n) = \bar{u}_n$ donc $f(u_n) = u_n + u$, pour un certain $u \in H$. On a $u \neq 0$, car sinon $u_n \in \ker(f - \mathrm{id}_E) = H$. On pose alors $u_{n-1} = u$ et on complète u_{n-1} à une base de H, ce qui donne la matrice souhaitée pour montrer vii).

iv) $\Rightarrow$ vi). On sait $H = \ker(f - \mathrm{id}_E)$. Soit $u \notin H$ et posons $w_0 = f(u) - u$. On a $w_0 \neq 0$ car autrement $w_0 \in \ker(f - \mathrm{id}_E) = H$. Donc $\mathrm{Im}(f - \mathrm{id}_E) = \mathrm{vect}(w_0)$. Soit $a = \alpha(u)$: nous avons $a \neq 0$ car $H = \ker(\alpha)$. Soit alors $w = (1/a)w_0$. Nous avons alors, pour tout $x \in E$:

$$f(x) = x + \alpha(x)w,$$

car ceci est vrai pour u, par construction, et pour une base de H, parce que $f|_H = \mathrm{id}_H$: c'est donc vrai sur une base de E et par conséquent sur E.

iv) $\Leftarrow$ vi). Si f prend la forme décrite dans vi), alors $\mathrm{Im}(f - \mathrm{id}_E) = \mathrm{vect}(w) \subset H$. □

Remarque 4.I.6. — L'inverse d'une transvection f d'hyperplan $H = \ker(\alpha)$ et droite $D = \mathrm{vect}(w)$ définie par $f(v) = v + \alpha(v)w$ est encore une transvection d'hyperplan H et droite D. Elle est définie, pour tout $v \in E$, par :

$$f^{-1}(v) = v - \alpha(v)w.$$

En effet, comme $w \in H = \ker(\alpha)$ on a $\alpha(w) = 0$ donc :

$$f(v - \alpha(v)w) = v - \alpha(v)w + \alpha(v - \alpha(v)w)w = v - \alpha(v)w + \alpha(v)w = v.$$

Le produit de deux transvections f et f' d'hyperplan $H = \ker(\alpha)$ est l'identité ou une transvection d'hyperplan H. Si f et f' sont définies par $f(v) = v + \alpha(v)w$ et $f'(v) = v + \alpha(v)w'$ pour certains $w, w' \in E$, alors ff' est définie par :

$$f^{-1}(v) = v + \alpha(v)(w + w').$$

En effet, comme $w' \in H = \ker(\alpha)$ on a $\alpha(w') = 0$ donc :

$$ff'(v) = f(v + \alpha(v)w') = v + \alpha(v)w' + \alpha(v + \alpha(v)w')w = v + \alpha(v)w' + \alpha(v)w.$$

Lemme 4.I.7. — *Soit f une transvection de droite D et hyperplan H et soit $g \in \mathrm{GL}(E)$. Alors gfg^{-1} est une transvection de droite $g(D)$ et d'hyperplan $g(H)$.*

Démonstration. — Soit $v \in E$ et $u = g^{-1}(v)$, donc $v = g(u)$. On a:

$$\begin{aligned} v \in \ker(gfg^{-1} - \mathrm{id}_E) &\Leftrightarrow gfg^{-1}(v) = v \\ &\Leftrightarrow gfg^{-1}(g(u)) = g(u) \\ &\Leftrightarrow gf(u) = g(u) \\ &\Leftrightarrow f(u) = (u) \\ &\Leftrightarrow u \in \ker(f - \mathrm{id}_E) = H \\ &\Leftrightarrow v \in g(H). \end{aligned}$$

Donc $\ker(gfg^{-1} - \mathrm{id}_E) = g(H)$. De même :

$$\begin{aligned} v \in \mathrm{Im}(gfg^{-1} - \mathrm{id}_E) &\Leftrightarrow g(u) \in \mathrm{Im}(gfg^{-1} - \mathrm{id}_E) \\ &\Leftrightarrow \exists w \in E \mid g(u) = gfg^{-1}(w) - w \\ &\Leftrightarrow \exists w \in E \mid u = fg^{-1}(w) - g^{-1}(w) \qquad \text{en posant } z = g^{-1}(w), \\ &\Leftrightarrow \exists z \in E \mid u = f(z) - z \\ &\Leftrightarrow u \in \mathrm{Im}(f - \mathrm{id}_E) = D \\ &\Leftrightarrow v \in g(D). \end{aligned}$$

Et bien sûr $D \subset H$ implique $f(D) \subset f(H)$, ce qui conclut la preuve. □

4.I.A.3. Générateurs de $\mathrm{GL}(E)$ *et* $\mathrm{SL}(E)$. —

Théorème 4.I.8. — *Les transvections engendrent* $\mathrm{SL}(E)$. *Les transvections et les dilatations engendrent* $\mathrm{GL}(E)$.

Démonstration. — Fixons une base de E et un isomorphisme $\mathrm{SL}(E) \simeq \mathrm{SL}_n(\mathbb{K})$. Nous allons considérer des transvections d'un type particulier, étant donné $i, j \in [\![1, n]\!]$ et $\lambda \in \mathbb{K}^*$, on fixe $t_{i,j}(\lambda)$ transvection de droite $D_i = \mathrm{vect}(e_i)$ et d'hyperplan $\ker(e_j^\vee)$, comme l'endomorphisme dont la matrice est:

$$T_{i,j}(\lambda) = \mathbb{1}_n + \lambda E_{i,j},$$

où $E_{i,j}$ est la matrice dont le coefficient au poste (h, k) est $\delta_{i,h}\delta_{j,k}$, où $\delta_{j,k}$ est le symbole de Kronecker. Autrement dit, $t_{i,j}(\lambda)$ envoie x sur $x + \lambda e_j^\vee(x)e_i$. Le coefficient (h, k) de $T_{i,j}(\lambda)$ est

$$\delta_{h,k} + \lambda\delta_{i,h}\delta_{j,k}.$$

On affirme que, si $A \in \mathrm{SL}_n(\mathbb{K})$, alors si on pose $A' = T_{i,j}(\lambda)A$ et $A'' = AT_{i,j}(\lambda)$, en désignant $L_i(M)$ le i-ième vecteur ligne d'une matrice M et $C_i(M)$ le i-ième vecteur colonne de M, on a:

$$\begin{aligned} L_i(A') &= L_i(A) + \lambda L_j(A), \\ C_j(A'') &= C_j(A) + \lambda C_i(A). \end{aligned}$$

En effet, notons $(a_{h,k})$ les coefficients de A, $(a'_{h,k})$ les coefficients de A', $(a''_{h,k})$ les coefficients de A''. On a :

$$a'_{h,k} = a'_{h,k} + \sum_{\ell \in [\![1,n]\!]} \lambda\delta_{i,h}\delta_{\ell,j}a_{\ell,k} = a_{h,k} + \lambda\delta_{i,h}a_{j,k}.$$

Ainsi, $a'_{h,k} = a_{h,k}$ pour $h \neq i$ et, pour $h = i$, $a'_{i,k} = a_{i,k} + \lambda a_{j,k}$, ce qui exprime $L_i(A') = L_i(A) + \lambda L_j(A)$. Pour les colonnes, c'est le même argument.

Nous posons maintenant $B = T_{i,j}(1)T_{j,i}(-1)T_{i,j}(1)A$. Nous allons montrer :

$$L_i(B) = L_j(A), \qquad L_j(B) = -L_i(A).$$

En effet, posons $B' = T_{i,j}(1)A$, $B'' = T_{j,i}(-1)B'$ donc $B = T_{i,j}(1)B''$. On a :

$$\begin{aligned} L_i(B') &= L_i(A) + L_j(A), & L_j(B') &= L_j(A); \\ L_i(B'') &= L_i(B') = L_i(A) + L_j(A), & L_j(B'') &= L_j(B') - L_i(B') = -L_i(A); \\ L_i(B) &= L_i(B'') + L_j(B'') = L_j(A), & L_j(B) &= L_j(B'') = -L_i(A). \end{aligned}$$

Nous pouvons alors montrer le résultat en appliquant le pivot de Gauss. En effet, on regarde $C_1(A) = (a_{1,1}, \ldots, a_{n,1})^t$. Si $a_{i,1} \neq 0$ pour un certain $i \in [\![2, n]\!]$, alors on peut obtenir A' ayant $a'_{1,1} = 1$ par la transformation :

$$L_1(A') = L_1(A) + \frac{1 - a_{1,1}}{a_{i,1}} L_i(A), \qquad \text{car alors : } \quad a'_{1,1} = a_{1,1} + \frac{1 - a_{1,1}}{a_{i,1}} a_{i,1} = 1$$

comme A est inversible, $C_1(A)$ n'est pas nulle donc si $a_{i,1} = 0$ pour tout $i \in [\![2, n]\!]$, c'est que $a_{1,1} \neq 0$, auquel cas on utilise B, i. e., on remplace L_1 par L_i et on revient à l'étape précédente pour avoir $a'_{1,1} = 1$.

On peut donc supposer $a_{1,1} = 1$. Par le procédé de Gauss on peut alors annuler tous les coefficients $a'_{1,i}$, quelque soit $i \in [\![2, n]\!]$. On peut donc supposer que $C_1(A)$ soit $(1, 0, \dots, 0)^t$.

On utilisera ensuite des transformations élémentaires sur les lignes $2, \dots, n$, puis $3, \dots, n$, et ainsi de suite, afin de trigonaliser A, i. e. on pourra trouver des matrices de transvection $T_1, \dots, T_s$ telles que $A' = T_1 \cdots T_s A$ soit triangulaire supérieure stricte avec des 1 sur la diagonale. Finalement, en opérant sur les colonnes, on pourra trouver des matrices de transvection $T'_1, \dots, T'_t$ telles que $A' T'_1 \cdots T'_t = \mathbb{1}_n$. Ainsi:

$$A = (T'_1)^{-1} \cdots (T'_1)^{-1} T_s^{-1} \cdots T_1^{-1}$$

est un produit de matrices de transvection.

On itère le procédé jusqu'à ce que la matrice obtenue soit $\mathbb{1}_n$. Nous venons de montrer que les transvections engendrent $\mathrm{SL}_n(\mathbb{K})$.

Pour $\mathrm{GL}_n(\mathbb{K})$, soit $A \in \mathrm{GL}_n(\mathbb{K})$ et $a = \det(A)$. Soit B une dilatation de déterminant $1/a$. Alors $C = AB \in \mathrm{SL}_n(\mathbb{K})$. Donc $A = CB^{-1}$ est produit de transvections et d'une dilatation, car B^{-1} est une dilatation (de rapport a). □

4.I.B. Groupe linéaire sur un corps fini. —

4.I.B.1. Ordre des groupes linéaires. — On note $\mu_n(\mathbb{K})$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{K}$.

Lemme 4.I.9. — *Tout sous groupe fini G de $\mathbb{K}^*$ est cyclique. Ensuite, soit $\mathbb{K} = \mathbb{F}_q$ et $d = \mathrm{pgcd}(n, q-1)$. Alors :*

$$\mu_n(\mathbb{K}) = \mu_d(\mathbb{K}).$$

En particulier, $\mu_n(\mathbb{K})$ est cyclique de cardinal d.

Démonstration. — Soit N l'ordre de G. Notons $\varphi(n)$ l'indicatrice d'Euler de $n \in \mathbb{N}$:

$$\varphi(n) = \#\{s \in [\![1, n]\!] \mid \mathrm{pgcd}(s, n) = 1\}.$$

Nous savons que $\varphi(n)$ est le nombre d'éléments d'ordre n dans $\mathbb{Z}/n\mathbb{Z}$, autrement dit le nombre de générateurs de ce groupe.

Aussi, considérons $\mathbb{Z}/N\mathbb{Z}$. L'ordre d'un élément dans ce groupe est un diviseur n de N : un tel élément engendre un sous groupe H de $\mathbb{Z}/N\mathbb{Z}$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$, constitué des multiples de N/n dans $\mathbb{Z}/N\mathbb{Z}$. Nous avons donc au moins $\varphi(s)$ éléments d'ordre s dans $\mathbb{Z}/N\mathbb{Z}$.

Or, si on considère $\mu_N(\mathbb{C}) = \{z \in \mathbb{C} \mid z^N = 1\}$, on a $\mu_N(\mathbb{C}) \simeq \mathbb{Z}/N\mathbb{Z}$, engendré par $\xi = e^{2i\pi/N}$. Comme les éléments d'ordre s de $\mu_N(\mathbb{C})$ satisfont $x^s = 1$, ils sont tous contenus dans l'ensemble, de cardinal s, des racines d'ordre s de 1. Cet ensemble coïncide avec le sous groupe de $\mu_N(\mathbb{C})$ engendré par $\xi^{N/s}$, car il contient évidemment ce dernier, et ce dernier a cardinal s.

Ceci montre que :

$$N = \sum_{n \mid N} \varphi(n).$$

Ainsi, soit $\alpha \in G$. L'ordre n de α divise N et $\langle \alpha \rangle$ est sous groupe H de G isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Or, le polynôme $x^n - 1$ possède au plus n racines dans $\mathbb{K}$. Par ailleurs, les éléments de H sont en nombre n et sont des racines de $x^n - 1$, donc H est l'ensemble de ces racines. Enfin, un élément $\beta \in G$ d'ordre n est racine de $x^n - 1$, donc appartient à H. Ainsi, s'il existe $\alpha \in G$ d'ordre n nous avons exactement $\varphi(n)$ éléments d'ordre n dans G, les générateurs de H.

Donc, du moment qu'on considère une partition de G selon l'ordre de chaque élément, on aura que N est la somme, pour tout $n \mid N$ d'un nombre qui vaut $\varphi(n)$ (s'il y a un élément

d'ordre n) ou 0 (s'il n'y en a pas). Mais comme $N = \sum_{n|N} \varphi(n)$, tous ces nombres doivent valoir $\varphi(n)$. En particulier le nombre d'éléments d'ordre N est $\varphi(N) \neq 0$, donc G est cyclique d'ordre N.

Soit maintenant $\mathbb{K} = \mathbb{F}_q$. Il existe, d'après Bezout, deux entiers u, v tels que :

$$un + v(q-1) = d.$$

Soit alors $\alpha \in \mathbb{F}_q$ avec $\alpha^n = 1$. Comme tout élément de $\mathbb{F}_q$, α satisfait $\alpha^{q-1} = 1$, donc :

$$\alpha^d = (\alpha^n)^u (\alpha^{q-1})^v = 1,$$

donc α est une racine d-ième de 1. Ceci montre $\mu_n(\mathbb{K}) \subset \mu_d(\mathbb{K})$.

Puis, comme d divise n, une racine d-ième de 1 est aussi une racine n-ième de 1, donc $\mu_d(\mathbb{K}) \subset \mu_n(\mathbb{K})$.

Enfin, $\mathbb{K}^*$ déjà est cyclique d'ordre $q-1$. Il est constitué des racines du polynôme $x^{q-1}-1$, qui sont toutes distinctes. Soit alors α une racine de x^d-1 dans une extension de $\mathbb{F}_q$. On a α racine de $x^{q-1}-1$ car $x^d = 1$ implique $x^{q-1} = 1$ du moment que $d \mid (q-1)$. Ainsi α est racine de $x^{q-1}-1$ donc $\alpha \in \mathbb{F}_q$. De plus les racines de x^d-1 sont aussi distinctes, i. e. x^d-1 possède d racines distinctes dans $\mathbb{F}_q$. Donc $\mu_d(\mathbb{F}_q)$ est d'ordre d, et on sait déjà qu'il est cyclique en tant que sous groupe fini de $\mathbb{K}^*$. □

Soit $q \geq 2$ et $n \geq 1$ entiers. Posons

$$N_{n,q} = (q^n - 1)(q^n - q)\cdots(q^n - q^{n-2})q^{n-1}.$$

Proposition 4.I.10. — *Soit $\mathbb{F}_q$ le corps à q éléments. Alors:*

$$\begin{aligned}
&\#\left(\mathrm{GL}_n(\mathbb{F}_q)\right) = N_{n,q}(q-1),\\
&\#\left(\mathrm{SL}_n(\mathbb{F}_q)\right) = N_{n,q},\\
&\#\left(\mathrm{PGL}_n(\mathbb{F}_q)\right) = N_{n,q},\\
&\#\left(\mathrm{PSL}_n(\mathbb{F}_q)\right) = N_{n,q}/\mathrm{pgcd}(n, q-1).
\end{aligned}$$

Démonstration. — Commençons par dénombrer les éléments de $\mathrm{GL}_n(\mathbb{F}_q)$. Les colonnes d'une matrice de $\mathrm{GL}_n(\mathbb{F}_q)$ sont exactement les n-tuplets de vecteurs libres, autrement dit les bases B de $\mathbb{F}_q^n$. L'on peut choisir pour premier vecteur u_1 de B un quelconque vecteur non nul de $\mathbb{F}_q^n$, d'où le premier facteur $q^n - 1$. Les choix de u_2 sont exactement tous les choix d'un deuxième vecteur qui n'est pas lié à u_1, i. e., qui n'appartient pas à $\mathrm{vect}(u_1)$, d'où le facteur $q^n - q$. En itérant le procédé, on arrive au nombre de choix $(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}) = N_{n,q}(q-1)$.

Pour $\mathrm{SL}_n(\mathbb{F}_q)$, nous avons $\mathrm{SL}_n(\mathbb{F}_q) = \ker(\det)$ où :

$$\det : \mathrm{GL}_n(\mathbb{F}_q) \to \mathbb{F}_q^*$$

est surjective, ce qui est clair en considérant la matrice $\mathrm{diag}(a, 1, \ldots, 1)$, $a \in \mathbb{K}^*$. Donc:

$$\#\left(\mathrm{SL}_n(\mathbb{F}_q)\right) = \#\left(\mathrm{GL}_n(\mathbb{F}_q)\right)/(q-1) = N_{n,q}.$$

Pour $\mathrm{PGL}_n(\mathbb{F}_q)$, on remarque que le centre $\mathbb{K}^*\mathbb{1}_n$ a cardinal $q-1$ donc $\mathrm{PGL}_n(\mathbb{K}) = \mathrm{GL}_n(\mathbb{K})/\mathbb{K}^*\mathbb{1}_n$ a cardinal $N_{n,q}$.

Pour $\mathrm{PSL}_n(\mathbb{F}_q)$, on remarque que le centre $\mathbb{K}^*\mathbb{1}_n \cap \mathrm{SL}_n(\mathbb{K})$ est constitué des matrices de la forme $a\mathbb{1}_n$, avec $a^n = 1$. La conclusion résulte aussitôt du lemme 4.I.9. □

4.I.B.2. Quelques rappels sur les groupes de permutation. — Soit $n \geq 1$ un entier.

Théorème 4.I.11. — *Le groupe $\mathfrak{A}_n$ est simple pour $n \geq 5$. De plus:*

i) le seul sous groupe de $\mathfrak{S}_n$ d'indice n est $\mathfrak{A}_n$, quelque soit n;

ii) les seuls sous groupe distingués de $\mathfrak{S}_n$ sont $\mathfrak{A}_n$, $\{\mathrm{id}\}$ et $\mathfrak{S}_n$, pour $n \geq 5$;

iii) le seul sous groupe distingué de $\mathfrak{A}_4$ est le groupe de Klein, engendré par les produits de deux transpositions disjointes.

Démonstration. — Montrons d'abord que $\mathfrak{A}_5$ est simple. Le plus facile, c'est d'analyser les classes de conjugaison dans $\mathfrak{A}_5$. On sait que les 3-cycles, au nombre de 20, forment une seule classe de conjugaison.

Pour les 5-cycles, au nombre de 24, c'est différent. Dans $\mathfrak{S}_5$ ils forment une seule classe, mais dans $\mathfrak{A}_5$ ils ne peuvent forment une seule classe car $24 \nmid 60$ et le cardinal de toute orbite est un diviseur de l'ordre du groupe, précisément celui-ci divisé par l'ordre du stabilisateur, qui divise l'ordre du groupe d'après le théorème de Lagrange.

On affirme que les 5-cycles forment alors deux classes. En effet, soit $\mathcal{O}(\gamma_1)$ et $\mathcal{O}(\gamma_2)$ deux orbites – il en existe au moins deux d'après ce que nous avons vu, et elles sont disjointes. Utilisons la notation exponentielle $\alpha^\beta = \beta\alpha\beta^{-1}$. On a $\gamma_1 = \gamma_2^\sigma$ avec σ impair car les 5-cycles γ_1 et γ_2 sont conjugués dans $\mathfrak{S}_5$ mais pas dans $\mathfrak{A}_5$.

Soit donc γ un 5-cycle. Alors $\gamma = \gamma_1^{\sigma_1}$ pour une certaine permutation σ_1. Aussi, si on pose $\sigma_2 = \sigma\sigma_1$, on trouve $\gamma = \gamma_1^{\sigma_2}$. On a $\gamma \in \mathcal{O}(\gamma_1)$ si et seulement si σ_1 est pair, et $\gamma \in \mathcal{O}(\gamma_2)$ si et seulement si σ_2 est pair. Mais, comme σ est impair, σ_1 est pair si et seulement si $\sigma_2 = \sigma\sigma_2$ est impair, donc γ appartient à $\mathcal{O}(\gamma_1)$ ou à $\mathcal{O}(\gamma_2)$, i. e. nous avons exactement deux orbites.

De plus, pour tout $\gamma \in \mathcal{O}(\gamma_1)$, on a $\gamma^\sigma \in \mathcal{O}(\gamma_2)$, et il est clair que l'application $\gamma \mapsto \gamma^\sigma$ définit une bijection de $\mathcal{O}(\gamma_1)$ sur $\mathcal{O}(\gamma_2)$. Nous avons donc 2 orbites de même cardinal, i.e. de cardinal 12 chacune.

Ce raisonnement montre que, étant donnée un classe de conjugaison $\mathcal{O} \subset \mathfrak{A}_n$ pour $\mathfrak{S}_n$, soit $\mathcal{O}$ forme aussi une classe de conjugaison pour $\mathfrak{A}_n$, soit $\mathcal{O}$ est la réunion de deux orbites pour $\mathfrak{A}_n$, de même cardinal. En particulier, si $\#(\mathcal{O})$ est impair, $\mathcal{O}$ est aussi une orbite pour $\mathfrak{A}_n$.

Pour les produit de deux transpositions, au nombre de 15, il y a une seule classe de conjugaison dans $\mathfrak{A}_5$ car 15 est impair.

Maintenant, si on avait un sous groupe distingué N de $\mathfrak{A}_5$, dès lors que N contient un élément, il contient toute sa classe de conjugaison. De plus, par le théorème de Lagrange, $|N|$ divise 60. Mais on ne saurait combiner 1, 12 (éventuellement deux fois), 15 et 20 de sorte à obtenir un diviseur de 60, autre que 1 ou 60.

Pour le cas $n \geq 6$, on prend $N \neq \{\mathrm{id}\}$ sous groupe distingué de $\mathfrak{A}_n$ et on cherche à montrer que N contient un 3-cycle. Il existe $\sigma \in N \setminus \mathrm{id}$, donc il existe $a \in [\![1, n]\!]$ tel que $b = \sigma(a) \neq a$. On choisit alors $c \in [\![1, n]\!] \setminus \{a, b, \sigma(b)\}$ et on pose $\tau = (acb)$ donc $\tau^{-1} = (abc)$. Ainsi $\tau^\sigma = (b\sigma(b)\sigma(c))$.

On a alors $[\tau, \sigma] = (acb)(b\sigma(b)\sigma(c))$, un élément de N qui laisse fixes tous les éléments hormis au plus 5, c'est-à-dire $\{a, b, c, \sigma(b), \sigma(c)\}$. Soit A une partie de $[\![1, n]\!]$ contenant ces éléments, ayant cardinal 5.

Les permutations paires de A forment un sous groupe de $\mathfrak{A}_n$ isomorphe à $\mathfrak{A}_5$, qui coupe N en un sous groupe distingué M contenant $[\tau, \sigma] \neq \mathrm{id}$, car $[\tau, \sigma](b) = \tau\sigma\tau^{-1}(a) = \tau\sigma(b) = b$ équivaut à $\sigma(b) = \tau^{-1}(b) = c$, ce qui n'est pas.

Or $\mathfrak{A}_5$ étant simple et $M \neq \{\mathrm{id}\}$ étant distingué, on a $M = \mathfrak{A}_5$, donc N contient des 3-cycles, ce qui achève la démonstration.

On peut montrer alors ii). Soit N un sous groupe distingué de $\mathfrak{S}_n$. Si $K = H \cap \mathfrak{A}_n \neq \{\mathrm{id}\}$, alors K étant distingué dans $\mathfrak{A}_n$ on a $K = \mathfrak{A}_n$. Or $H = K$ ou K a indice 2 dans H auquel cas

$H = \mathfrak{S}_n$. Sinon, $H \cap \mathfrak{A}_n \neq \{\mathrm{id}\}$, donc H s'envoie de manière injective sur $\{\pm 1\}$, ainsi $|H| = 2$ car $H \neq \{\mathrm{id}\}$, i. e. $H = \{\mathrm{id}, \sigma\}$. Pour tout $\tau \in \mathfrak{S}_n$, on a alors $\tau\sigma\tau^{-1} = \sigma$, autrement dit σ est central. Mais le centre de $\mathfrak{S}_n$ est trivial.

Démontrons maintenant i). Soit H un sous groupe d'indice n de $\mathfrak{S}_n$. Alors $\mathfrak{S}_n$ opère sur $X = \mathfrak{S}_n/H$, un ensemble de cardinal n, et nous avons un morphisme de groupes $\rho : \mathfrak{S}_n \to \mathfrak{S}(X)$. Si $n = 2$ ou $n = 3$, c'est clair. Si $n = 4$, un sous groupe d'indice 4 a ordre 6, donc il est isomorphe à $\mathfrak{S}_3$ ou alors il est cyclique, ce qui n'est pas.

Soit alors $n \geq 5$ et soit $\sigma \in \mathfrak{S}_n$ et $\bar{\sigma}$ sa classe dans X. Le stabilisateur de $\bar{\sigma}$ est $\{\tau \in \mathfrak{S}_n \mid \tau\sigma \in \sigma H\}$. Il s'agit de $\sigma H \sigma^{-1} = H^\sigma$. Donc le stabilisateur de la classe $\bar{\mathrm{id}}$ est H. On a $\ker(\rho)$ distingué dans $\mathfrak{S}_n$. Donc $\ker(\rho)$ est trivial, égal à $\mathfrak{A}_n$, ou ρ est trivial. Mais $\ker(\rho)$ est constitué de l'intersection de tous les stabilisateurs H^σ, donc $\ker(\rho) \subset H$, ainsi $\ker(\rho) \neq \mathfrak{A}_n$, $\ker(\rho) \neq \mathfrak{S}_n$.

Donc ρ est injective et H est isomorphe via ρ au stabilisateur du point $\bar{\mathrm{id}}$ de $\mathfrak{S}(X)$, ce qui implique $H \simeq \mathfrak{S}_{n-1}$. □

4.I.B.3. Groupes linéaires d'ordre petit. — Il ne manque plus que les cas $n = 2$ et $\mathbb{F}_q$ avec $q \in \{2, 3, 4, 5\}$. Au fait, pour $q = 4$ nous savons déjà que $\mathrm{PSL}_2(\mathbb{F}_4)$ est simple, mais nous pouvons le reconnaître comme un groupe déjà rencontré.

Proposition 4.I.12. — *On a :*

i) $\mathrm{PGL}_2(\mathbb{F}_2) \simeq \mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$,

ii) $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$, $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$,

iii) $\mathrm{PSL}_2(\mathbb{F}_4) \simeq \mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$,

iv) $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$, $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

Démonstration. — On sait que $G = \mathrm{PSL}_2(\mathbb{K})$ opère sur $\mathbb{P}^1 = \mathbb{P}^1_{\mathbb{K}}$. Cette droite projective possède $q+1$ points donc on a un morphisme de groupes :

$$\rho : G \to \mathfrak{S}_{q+1}.$$

Or ρ est injectif, car une homographie qui laisse fixes tous les points est l'identité.

Comme $|\mathrm{PSL}_2(\mathbb{F}_2)| = 6$ on trouve directement i) et $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$. De plus, si q est pair, $\mathrm{PGL}_2(\mathbb{F}_q) \simeq \mathrm{PSL}_2(\mathbb{F}_q)$ car $\mathrm{pgcd}(2, q-1) = 1$.

Pour ii), on sait que $\mathfrak{A}_4$ est le seul sous groupe de $\mathfrak{A}_4$ d'indice 2, et comme $\mathrm{PSL}_2(\mathbb{F}_3)$ a indice 2 dans $\mathrm{PGL}_2(\mathbb{F}_3)$, on voit que $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$.

Dans le cas iii), on a $|\mathrm{PSL}_2(\mathbb{F}_4)| = 60$ donc ρ exprime $\mathrm{PSL}_2(\mathbb{F}_4)$ comme un sous groupe d'indice deux de $\mathfrak{S}_5$. On sait que celui-ci est forcément $\mathfrak{A}_5$.

Pour iv), via ρ on a $\mathrm{PGL}_2(\mathbb{F}_5)$ d'indice 6 dans $\mathfrak{S}_6$, ce qui implique $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$. Puis $\mathrm{PSL}_2(\mathbb{F}_5)$ est distingué dans $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$, donc $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$. □

4.II. Simplicité du groupe linéaire projectif

On considère un espace vectoriel E de dimension n sur un corps $\mathbb{K}$ et le groupe $\mathrm{PSL}(E)$. On fixe une base de E et par conséquent un isomorphisme $\mathrm{PSL}(E) \simeq \mathrm{PSL}_n(\mathbb{K})$. Nous allons travailler avec cet isomorphisme implicitement fixé.

Théorème 4.II.1. — *Le groupe* $\mathrm{PSL}_n(\mathbb{K})$ *est simple hormis dans les cas :*

$$\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3, \qquad \mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4.$$

4.II.A. Démonstration pour $n \geq 3$. — Soit N_0 un sous groupe distingué de $\mathrm{PSL}_n(\mathbb{K})$, avec $N_0 \neq \{1\}$. Nous voulons montrer que $N_0 = \mathrm{PSL}_n(\mathbb{K})$. Dans ce but, on considère N, l'image réciproque de N dans $\mathrm{SL}_n(\mathbb{K})$. On a alors $N \neq \mathbb{K}^* \mathbb{1}_n$, et N est distingué dans $\mathrm{SL}_n(\mathbb{K})$. Il existe donc un automorphisme $g \in N$ qui n'est pas une homothétie. Le but est de montrer que l'on peut fabriquer, à partir de g, une transvection dans N. Comme celles-ci sont toutes conjuguées, N contiendra alors toutes les transvections. Du moment que celles-ci engendrent $\mathrm{SL}_n(\mathbb{K})$, on aura alors $N = \mathrm{SL}_n(\mathbb{K})$.

Comme g n'est pas pas une homothétie, il existe $u \in E$ tel que $g(u)$ et u ne sont pas colinéaires. Soit $v = g(u)$. On a alors un plan $F = \mathrm{vect}(u, v) \subset E$.

Choisissons une transvection f de droite $A = \mathrm{vect}(u)$. Alors gfg^{-1} est une transvection de droite $B = \mathrm{vect}(g(u)) = \mathrm{vect}(v)$ d'après le lemme 4.I.7. Par conséquent, $gfg^{-1} \neq f$ i.e., $[g, f] = gfg^{-1}f^{-1} \neq \mathrm{id}_E$. On pose alors $h = [g, f]$. On a $fg^{-1}f^{-1} \in N$ car N est distingué dans $\mathrm{SL}_n(\mathbb{K})$; aussi $g^{-1} \in N$ donc $h \in N$.

Remarquons que $\mathrm{Im}(h - \mathrm{id}_E) \subset F$. En effet, un élément de $\mathrm{Im}(h - \mathrm{id}_E)$ s'écrit:

$$h(x) - x = gfg^{-1}f^{-1}(x) - x = gfg^{-1}f^{-1}(x) - f^{-1}(x) + f^{-1}(x) - x,$$

pour un certain $x \in E$. Or si on pose $y = gfg^{-1}f^{-1}(x) - f^{-1}(x)$ et $z = f^{-1}(x) - x$, on voit que y s'obtient en appliquant à $f^{-1}(x)$ l'endomorphisme $gfg^{-1} - \mathrm{id}_E$ d'image $\mathrm{vect}(v)$ et $z = f^{-1}(x) - x$ appartient à l'image de $f^{-1} - \mathrm{id}_E$, i. e. à $\mathrm{vect}(u)$, cf. la remarque 4.I.6. Ainsi $h(x) - x = y + z \in F$.

Maintenant nous utilisons l'hypothèse $n \geq 3$. Il existe un hyperplan H de E contenant F. Nous avons alors deux cas:

Cas 1 : *il existe une transvection t de E, d'hyperplan H, qui ne commute pas à h.* Dans ce cas $s = [h, t] \neq \mathrm{id}_E$, et de nouveau $s \in N$. Aussi, $s = hth^{-1}t^{-1}$ et $t' = hth^{-1}$ est une transvection d'hyperplan $h(H)$. Mais nous avons montré que $\mathrm{Im}(h - \mathrm{id}_E) \subset F \subset H$ donc $h(H) = H$, i. e. t' est une transvection d'hyperplan H. Donc $s = t't^{-1}$ est un produit de transvections d'hyperplan H, ainsi $s \neq \mathrm{id}_E$ est aussi une transvection d'hyperplan H, cf. la remarque 4.I.6.

Cas 2 : *toute transvection t de E d'hyperplan H commute à h.* Dans ce cas, nous prenons toutes les transvections t d'hyperplan $H = \ker(\alpha)$. Chacune d'elles s'écrit, pour un certain $w \in H$ sous la forme $t(x) = x + \alpha(x)w$. Écrivons que t commute avec h:

$$th(x) = h(x) + \alpha(h(x))w = h(x) + \alpha(x)h(w) = ht(x), \qquad \forall x \in E.$$

Il en résulte que, pour tout $x \in E$ et tout $w \in H$, on a:

$$\alpha(h(x))w = \alpha(x)h(w).$$

Or, on sait que $\mathrm{Im}(h - \mathrm{id}_E) \subset H$ donc $h(x) - x \in H$, ce qui implique $\alpha(h(x) - x) = 0$, i. e. $\alpha(h(x)) = \alpha(x)$. L'équation précédente devient :

$$\alpha(x)w = \alpha(x)h(w), \qquad \forall (x, w) \in E \times H.$$

Mais si on prend $x \notin H$, alors $\alpha(x) \neq 0$ donc $h(w) = w$, et cela pour tout $w \in H$. Il en résulte que $H \subset \ker(h - \mathrm{id}_E)$. De plus, $h \neq \mathrm{id}_E$ et $h \in N \subset \mathrm{SL}_n(\mathbb{K})$ donc $\det(h) = 1$. Ainsi h est une transvection d'après la proposition 4.I.5.

Dans les deux cas nous avons montré qu'il existe une transvection dans N, ce qui implique $N = \mathrm{SL}_n(\mathbb{K})$.

4.II.B. Le cas $n = 2$ et la fin de la démonstration. — Pour étudier le cas $n = 2$, nous allons montrer le résultat suivant.

Proposition 4.II.2. — *Soit N un sous groupe distingué de $\mathrm{SL}_2(\mathbb{K})$, où $\mathbb{K} \neq \mathbb{F}_p$, $p \in \{2, 3, 5\}$, avec $N \not\subset \mathbb{K}^* \mathbb{1}_2$. Alors $N = \mathrm{SL}_2(\mathbb{K})$.*

Démonstration. — Soit $f \in N \smallsetminus \mathbb{K}^* \mathbb{1}_2$, i. e. f n'est pas une homothétie. Il existe alors $u \in E$ tel que u et $v = f(u)$ forment une base B de E. Comme $\det(f) = 1$, il existe $a \in \mathbb{K}$ tel que :

$$\mathrm{Mat}_B(f) = \begin{pmatrix} 0 & -1 \\ 1 & a \end{pmatrix}.$$

Notons P la matrice ci-dessus.

Soit $c \in \mathbb{K}^*$. Considérons $g \in \mathrm{SL}(E)$ défini par:

$$g(u) = \frac{1}{c}u, \qquad g(v) = cv.$$

Comme N est distingué dans $\mathrm{SL}(E)$, on a $h = [f, g] \in N$. Soit $Q = \mathrm{Mat}_B(g)$. On a:

$$P^{-1} = \begin{pmatrix} -a & 1 \\ -1 & 0 \end{pmatrix}, \qquad Q = \begin{pmatrix} c^{-1} & 0 \\ 0 & c \end{pmatrix}, \qquad \mathrm{Mat}_B(h) = PQP^{-1}Q^{-1} = \begin{pmatrix} c^{-2} & 0 \\ a(c^2-1) & c^2 \end{pmatrix}.$$

Soit R la matrice ci-dessus. Nous répétons maintenant le procédé de passer au commutateur, cette fois en fixant $b \in \mathbb{K}$ et en définissant l'élément $t \in \mathrm{SL}(E)$ par $t(u) = u + bv$, $t(v) = v$. Donc nous calculons:

$$R^{-1} = \begin{pmatrix} c^2 & 0 \\ a(1-c^2) & c^{-2} \end{pmatrix}, \qquad \mathrm{Mat}_B(t) = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}.$$

Soit T la matrice ci-dessus. On calcule:

$$TRT^{-1}R^{-1} = \begin{pmatrix} c^2 & 0 \\ bc^2 + a(1-c^2) & c^{-2} \end{pmatrix} \begin{pmatrix} c^{-2} & 0 \\ -bc^{-2} + a(c^2-1) & c^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b(1-c^{-4}) & 1 \end{pmatrix}.$$

Soit S la matrice ci-dessus. Encore une fois, $[t, h] \in N$, quelque soient b et c.

S'il existe un élément $c \in \mathbb{K}^*$ tel que $c^4 \neq 1$, alors on pose $b = 1/(1-c^{-4})$ et S est une matrice de transvection, donc N contient une transvection, ce qui implique $N = \mathrm{SL}(E)$, comme dans le cas $n \geq 3$.

Or si $\mathbb{K}$ a au moins 7 éléments, il existe bien $c \in \mathbb{K}^*$ tel que $c^4 \neq 1$, car l'équation $x^4 = 1$ a au plus 4 solutions dans $\mathbb{K}$. Pour $\mathbb{K} = \mathbb{F}_4$, on a $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, où $\alpha^2 + \alpha + 1 = 0$. Si on avait $\alpha^4 = 1$ alors α serait racine de $x^4 + 1 = (x+1)^4$ sur $\mathbb{F}_2[x]$ i. e. $\alpha = 1$, ce qui n'est pas. Ainsi sur tout corps $\mathbb{K}$ hormis $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_5$ on peut trouver c tel que $c^4 \neq 1$, ce qui achève la démonstration. □

Nous pouvons maintenant compléter la démonstration du théorème 4.II.1. En effet, le cas $n \geq 3$ étant montré, nous regardons le cas $n = 2$ où la proposition 4.II.2 montre la simplicité de $\mathrm{PSL}_2(\mathbb{K})$ hormis dans les cas où $\mathbb{K}$ est $\mathbb{F}_2$ ou $\mathbb{F}_3$ ou $\mathbb{F}_5$. Ensuite, la proposition 4.I.12 montre que $\mathrm{PSL}_2(\mathbb{F}_5)$ est simple grâce au théorème 4.I.11, aussi bien que les isomorphismes $\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$ et $\mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$. Il est clair que ces deux dernier groupes ne sont pas simples.

CHAPITRE 5

QUADRIQUES

Dans ce chapitre, $\mathbb{K}$ désigne un corps de caractéristique différente de 2.

5.I. Quadriques projectives

5.I.A. Formes quadratiques. — Soit E un espace vectoriel de dimension $n < \infty$ sur $\mathbb{K}$. Nous allons voir la classification des formes quadratiques dans trois cas principaux : lorsque $\mathbb{K}$ est algébriquement clos, ou un corps fini, ou le corps des nombres réels.

5.I.A.1. Équivalence des formes quadratiques. —

Définition 5.I.1. — Soit q, q' formes quadratiques sur E. Alors q est équivalente à q' si il existe $\varphi \in \mathrm{GL}(E)$ tel que $q' = q \circ \varphi$. On note $q \simeq q'$.

Les formes q et q' sont équivalentes si et seulement si, étant fixée une base B de E, étant données les matrices $M = \mathrm{Mat}_B(q)$ et $M' = \mathrm{Mat}_B(q')$, il existe $P \in \mathrm{GL}_n(\mathbb{R})$ telle que:

$$M' = P^t M P, \qquad \text{où } P = \mathrm{Mat}_B(\varphi).$$

En effet, une première remarque fondamentale est que, si on se donne des vecteurs $u = BX$ et $v = BY$ pour des vecteurs colonne $X = (x_1, \ldots, x_n) \in \mathbb{K}^n$, et $Y = (y_1, \ldots, y_n) \in \mathbb{K}^n$ alors la forme bilinéaire :

$$\Phi_q(u, v) = \frac{1}{2}(q(u+v) - q(u) - q(v))$$

satisfait :

$$\Phi_q(u, v) = X^t M Y.$$

De plus, on a $\varphi(u) = BPX$. Ainsi, on trouve $q' = q \circ \varphi$ si et seulement si $\Phi_{q'}(u, v) = \Phi_q(\varphi(u), \varphi(v))$, si et seulement si :

$$\Phi_{q'}(u, v) = X^t M' Y = X^t P^t M P Y = \Phi_q(\varphi(u), \varphi(v)),$$

ce qui équivaut à $M' = P^t M P$. Le rang de $\mathrm{Mat}_B(q)$ ne dépend pas de la base B.

Définition 5.I.2. — Le *rang* de q est le rang de $\mathrm{Mat}_B(q)$. On dit que q est *dégénérée* si le rang de q est strictement inférieur à n. Sinon, si le rang de q est égal à n, on dit que q est *non dégénérée*.

L'*orthogonal* d'une partie A de E est $A^\perp = \{u \in E \mid \Phi_q(v, u) = 0, \forall v \in A\}$.

5.I.A.2. Carrés dans un corps fini. — Pour étudier le cas des corps finis, nous faisons d'abord quelques considérations très simples sur les carrés dans un corps fini. Notons $\mathbb{K}^{(2)}$ l'ensemble des carrés de $\mathbb{K}$. Rappelons que, si $\mathbb{F}_q$ est un corps fini à q éléments, q étant impair, alors:

$$|\mathbb{F}_q^{(2)}| = \frac{q+1}{2}.$$

En effet, l'application $f : x \mapsto x^2$ est un morphisme de groupes:

$$f : \mathbb{F}_q^* \to \mathbb{F}_q^*, \qquad \text{et } \mathrm{Im}(f) = \mathbb{F}_q^{(2)} \smallsetminus \{0\}.$$

Le noyau de f est $\{\pm 1\}$. Donc:

$$|\mathbb{F}_q^{(2)} \smallsetminus \{0\}| = \frac{q-1}{2},$$

ce qui donne $|\mathbb{F}_q^{(2)}| = \frac{q+1}{2}$. Remarquons que :

$$\mathbb{F}_q^{(2)} \smallsetminus \{0\}/\mathbb{F}_q^* \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

Ceci montre que, si a et b ne sont pas des carrés dans $\mathbb{F}_q^*$, alors ab l'est. En effet les classes $[a]$ et $[b]$ de a et b dans le quotient ci-dessus sont toutes les deux -1, donc leur produit $[ab]$ et 1, i.e., ab est un carré.

5.I.A.3. Trois classifications des formes quadratiques. —

Proposition 5.I.3. — *Soit q et q' formes quadratiques sur E.*

i) Si $\mathbb{K}$ est algébriquement clos, $q \simeq q'$ si et seulement si q et q' ont le même rang.

ii) Soit $\mathbb{K} = \mathbb{R}$. Alors $q \simeq q'$ si et seulement si q et q' ont la même signature.

iii) Soit $\mathbb{K} = \mathbb{F}_q$, $\lambda \in \mathbb{F}_q \smallsetminus \mathbb{F}_q^{(2)}$ et $B = (e_1, \dots, e_n)$ une base de E. Supposons q non dégénérée. Alors q est équivalente à q_1 ou à q_λ où:

$$\begin{aligned} &q_1(e_i) = 1, && \text{pour tout } i \in [\![1, n]\!], \\ &q_\lambda(e_i) = 1, && \text{pour tout } i \in [\![1, n-1]\!], \\ &q_\lambda(e_n) = \lambda. \end{aligned}$$

Démonstration. — Soit $B = (e_1, \dots, e_n)$ une base de E et $u = x_1e_1 + \cdots + x_ne_n$, pour $(x_1, \dots, x_n) \in \mathbb{K}^n$. Alors $q(u)$ s'écrit comme un polynôme homogène de degré 2 en les variables $x_1, \dots, x_n$. En complétant les carrés de ce polynôme par l'algorithme de Gauss, on trouve $(a_1, \dots, a_n) \in \mathbb{K}^n$ et n formes linéaires indépendantes $\alpha_1, \dots, \alpha_n$, i. e. telles que $(\alpha_1, \dots, \alpha_n)$ soit une base de $E^\vee$, avec:

$$q(u) = q(x_1e_1 + \cdots + x_ne_n) = \sum_{i=1}^{n} a_i \alpha_i(u)^2.$$

Le rang r de q est le nombre de $i \in [\![1, n]\!]$ tels que $a_i \neq 0$ et, quitte à permuter les indices, on pourra supposer que $a_i = 0$ si et seulement si $i > r$.

i) Si $\mathbb{K}$ est algébriquement clos, on choisit des racines $\sqrt{a_i}$ de $x^2 - a_i$ et on pose, pour $i \in [\![1, r]\!]$:

$$\beta_i = \frac{1}{\sqrt{a_i}} \alpha_i.$$

On obtient $q = \beta_1^2 + \cdots + \beta_r^2$. Il s'en suit que $q \simeq q'$ ont le même rang r si et seulement si elles sont toutes les deux équivalentes à $u \mapsto x_1^2 + \cdots + x_r^2$. Autrement dit, $q \simeq q'$ ont le même rang r si et seulement si elles sont équivalentes.

ii) Si $\mathbb{K} = \mathbb{R}$, on peut supposer de plus $a_i > 0$ si et seulement si $i > p$, où la signature de q est $(p, r-p)$.

$$\beta_i = \frac{1}{\sqrt{a_i}}\alpha_i, \qquad \text{pour } i \in [\![1, p]\!],$$
$$\beta_i = \frac{1}{\sqrt{-a_i}}\alpha_i, \qquad \text{pour } i \in [\![p+1, r]\!].$$

Il s'en suit que $q \simeq q'$ ont la même signature $(p, r-p)$ si et seulement si elles sont toutes les deux équivalentes à :

$$u = (x_1 e_1 + \cdots + x_n e_n) \mapsto \sum_{i=1}^{p} x_i^2 - \sum_{i=p+1}^{r} x_i^2.$$

iii) On raisonne par récurrence sur n.

Soit $n = 1$, $e = e_1 =$ et $a = q(e)$. On a $q(xe) = ax^2$. Si a est un carré, on prend c une racine de a puis $f = (1/c)\, e$ et en utilisant la base (f) on voit que q est équivalente à q_1. Si a n'est pas un carré, nous avons vu que λa l'est, aussi bien que a/λ. On prend donc c racine de a/λ et on considère $f = (1/c)\, e$. On trouve $q(xf) = \lambda x^2$ donc q est équivalente à q_λ.

Soit $n \geq 2$. On peut supposer que e_1 et e_2 soient orthogonaux, i. e. $\Phi_q(e_1, e_2) = 0$. En effet, comme q est non dégénérée, on peut se ramener au cas où les deux premiers vecteurs de base sont orthogonaux et non isotropes. On écrit donc $q(x_1 e_1 + x_2 e_2) = a_1 x_1^2 + a_2 x_2^2$, avec a_1 et a_2 non nuls. On peut également supposer que $e_2, \ldots, e_n$ appartiennent à $\mathrm{vect}(e_1, e_2)^\perp$.

De plus, on peut trouver $(x_1, x_2) \in \mathbb{F}_q^2$ tels que $a_1 x_1^2 + a_2 x_2^2 = 1$. En effet, pour x_2 fixé, il s'agit de résoudre :

$$x_1^2 = \frac{1 - a_2 x_2^2}{a_1}$$

Or, comme $a_2 \neq 0$, si on laisse varier $y = x_2^2$ parmi les $\frac{q+1}{2}$ éléments de $\mathbb{F}_q^{(2)}$, comme la fonction $g : y \mapsto (1 - a_2 y)/a_1$ est une bijection (c'est une application affine non constante de $\mathbb{K}$ dans $\mathbb{K}$), l'image via g des carrés de $\mathbb{F}_q$ doit intercepter l'ensemble des carrés de $\mathbb{F}_q$.

Ceci permet de choisir un vecteur f_1 de $\mathrm{vect}(e_1, e_2)$ tel que $q(f_1) = 1$. Sur l'orthogonal $f_1^\perp$, de dimension $n-1$, par hypothèse de récurrence on peut trouver une base $(f_2, \ldots, f_n)$, sur laquelle la matrice de la restriction de q devienne $\mathbb{1}_{n-1}$ ou $\mathrm{diag}(\mathbb{1}_{n-2}, \lambda)$. Ainsi, la matrice de q en la base $(f_1, \ldots, f_n)$ devient $\mathbb{1}_n$ ou $\mathrm{diag}(\mathbb{1}_{n-1}, \lambda)$, ce qui montre que q est équivalente à q_1 ou à q_λ.

□

5.I.B. Quadriques projectives. — Pour ce paragraphe, E aura dimension $n+1$. Soit q une forme quadratique sur E et considérons l'ensemble $\mathcal{Q}$ des vecteurs isotropes de q. Nous le notons $\mathbb{V}(q)$:

$$\mathcal{Q} = \mathbb{V}(q) = \{u \in E \mid q(u) = 0\}.$$

Il s'agit des solutions d'une équation polynomiale quadratique homogène en n variables. Selon le corps de base, l'ensemble des ces solutions peut être vide, par exemple si $\mathbb{K} = \mathbb{R}$, $E = \mathbb{R}^3$ et $q(x_0, x_1, x_2) = x_0^2 + x_1^2 + x_2^2$. En revanche, l'ensemble de ces solutions n'est jamais vide si $n \geq 1$ et $\mathbb{K}$ est algébriquement clos.

5.I.B.1. Polarité. — Fixons une forme quadratique non dégénérée q sur E, donc la quadrique lisse $\mathcal{Q} = \mathbb{V}(q) \subset \mathbb{P}^n$.

Nous avons une application linéaire :

$$\begin{aligned}\Psi_q : E &\to E^\vee,\\ u &\mapsto (v \mapsto \Phi_q(v,u)).\end{aligned}$$

Si $B^\vee$ est la base duale de B, on trouve:

$$\mathrm{Mat}_{B^\vee,B}(\Psi_q) = \mathrm{Mat}_B(q).$$

On voit donc que, du fait que q est non dégénérée, Ψ_q est un isomorphisme.

Définition 5.I.4. — L'homographie $\mathbb{P}(E) \mapsto \check{\mathbb{P}}(E)$ définie par :

$$[u] \mapsto H_{[u]} = \mathbb{P}(\ker(\Psi_q(u)))$$

est la *polarité* associée à la quadrique $\mathcal{Q}$.

Remarque 5.I.5. — Soit $[u] \in \mathcal{Q}$, i. e. $q(u) = 0$. On peut penser à $H_{[u]}$ comme l'*espace tangent à* $\mathcal{Q}$ en $[u]$. En effet si $\mathbb{K} = \mathbb{R}$, on peut écrire :

$$\lim_{t\to 0} \frac{q(u+tv)}{t} = \lim_{t\to 0} \frac{q(u) + 2t\Phi_q(u,v) + t^2 q(v)}{t} = 2\Phi_q(u,v) = 2\Phi_q(v,u).$$

Donc $\Phi_q(v,u) = 0$ si et seulement si le point $[v]$ appartient à l'espace tangent $T_{[u]}\mathcal{Q}$ à $\mathcal{Q}$ en $[u]$.

Proposition 5.I.6. — *Soit* $[v] \in \mathbb{P}(E)$. *Alors* $\mathcal{Q} \cap H_{[v]} = \{[u] \in \mathcal{Q} \mid v \in T_{[u]}\mathcal{Q}\}$.

Cette proposition affirme que, si M est un point de $\mathbb{P}^n$ et $\mathcal{Q}$ est une quadrique lisse, l'hyperplan polaire à $\mathcal{Q}$ en M coupe sur $\mathcal{Q}$ l'ensemble des points P dont l'hyperplan tangent à $\mathcal{Q}$ passe par M.

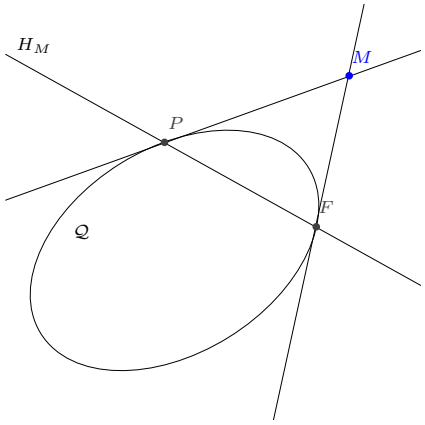


FIGURE 1. Polarité pour une conique

Démonstration. — Soit $[v] \in \mathbb{P}(E)$ et $[u] \in \mathcal{Q}$. On trouve :

$$\begin{aligned}[v] \in T_{[u]}\mathcal{Q} &\Leftrightarrow \Phi_q(v,u) = 0\\ &\Leftrightarrow u \in \mathrm{Ker}(\Psi_q(v))\\ &\Leftrightarrow [u] \in H_{[v]}.\end{aligned}$$

□

5.I.B.2. Quadriques lisses. — Nous avons vu que, si $[u] \in \mathcal{Q} = \mathbb{V}(q)$, l'espace tangent à $\mathcal{Q}$ est $H_{[v]}$. Cet espace est toujours bien défini si q est non dégénérée. En effet, dans ce cas, pour tout vecteur isotrope $u \neq 0$ de q, $\Psi_q(u)$ est toujours une forme linéaire non nulle, donc son noyau définit un hyperplan. Ceci justifie la définition suivante.

Définition 5.I.7. — Une quadrique $\mathcal{Q} = \mathbb{V}(q)$ est *lisse* si q est non dégénérée. Une quadrique est un *cône de sommet* $\mathbb{P}(F)$ s'il existe une base $B = (e_0, \dots, e_n)$ telle que $q(x_0e_0 + \cdots + x_ne_n)$ ne dépende pas de $x_{m+1}, \dots, x_n$ et $F = \mathrm{vect}(e_{m+1}, \dots, e_n)$, avec $m \in [\![0, n-1]\!]$.

Remarque 5.I.8. — La forme q est dégénérée si et seulement si $\mathcal{Q}$ est un cône.

Démonstration. — Si $\mathcal{Q}$ est un cône et on écrit le polynôme associé à q en la base B, celui-ci ne dépend pas de x_n, donc la dernière ligne de $\mathrm{Mat}_B(q)$ est nulle. Ainsi, q est dégénérée.

Réciproquement, si q est dégénérée, donc de rang $m < n$ et on considère une base orthogonale de q et, quitte à en permuter les vecteurs, on peut supposer que le polynôme décrivant q en cette base ne dépende pas de $x_{m+1}, \dots, x_n$. Donc $\mathcal{Q}$ est un cône. □

Remarque 5.I.9. — Si $\mathbb{K}$ est algébriquement clos, $q \neq 0$ et $n = 2$, $\mathcal{Q}$ est dégénérée si et seulement si $\mathcal{Q}$ est la réunion de deux droites, éventuellement confondues.

Démonstration. — Si q est dégénérée, q a rang 2 ou 1. Si q a rang 2, on écrit $q(u) = \alpha_0(u)^2 + \alpha_1(u)^2$, pour certaines formes linéaires α_1 et α_2. Donc $q = (\alpha_0 + \sqrt{-1}\alpha_1)(\alpha_0 - \sqrt{-1}\alpha_1)$ et $\mathcal{Q}$ est la réunion de deux droites. Si q a rang 1, $\mathcal{Q}$ est une seule droite.

Si $\mathcal{Q}$ est la réunion de deux droites distinctes $\mathbb{P}(\ker(\alpha_0))$ et $\mathbb{P}(\ker(\alpha_1))$, on considère une base de E dont la duale est $(\alpha_0, \alpha_1, \alpha_2)$ (on complète α_0, α_1 à une base de $E^\vee$). Si le polynôme $p(x_0, x_1, x_2)$ représente q en cette base, on a $x_0 = 0 \Rightarrow p(x_0, x_1, x_2) = 0$, i. e. p s'annule modulo x_0. Donc x_0 divise p. De même x_1 divise p, donc x_0x_1 divise p, par factorialité, car ces éléments sont irréductibles. Ainsi p est un multiple scalaire de x_0x_1, c'est donc un cône. □

Proposition 5.I.10. — *Toute conique projective lisse sur $\mathbb{K}$ algébriquement clos est équivalente à $\mathbb{V}(x_0x_2 - x_1^2) \subset \mathbb{P}^2$.*

Toute conique lisse non vide de $\mathbb{P}^2(\mathbb{R})$ est équivalente à $\mathbb{V}(x_1^2 + x_1^2 - x_0^2)$.

Démonstration. — En effet, si $\mathbb{K}$ est algébriquement clos et q a rang 3, il existe une base de E telle que le polynôme représentant q en cette base s'écrive $x_0x_2 - x_1^2$.

Si $\mathbb{K} = \mathbb{R}$, comme q est de rang 3 nous pouvons avoir signature $(3,0)$ ou $(2,1)$ ou $(1,2)$ ou $(0,3)$. Mais en remplaçant q par $-q$ on ne change pas $\mathcal{Q}$, alors que la signature passe de $(0,3)$ à $(3,0)$ et de $(1,2)$ à $(2,1)$. On peut donc regarder uniquement $(3,0)$ et $(2,1)$, mais le premier cas est exclu car $\mathcal{Q}$ est non vide. Ainsi le seul cas qui reste exprime, quitte à permuter les vecteurs de base, la polynôme $x_1^2 + x_1^2 - x_0^2$. □

5.II. Quadriques affines

Fixons un espace affine $\mathcal{E}$ de dimension n sur $\mathbb{K}$ et de direction E, un espace vectoriel de dimension n sur $\mathbb{K}$.

5.II.A. Quadriques affines et polynômes quadratiques. —

Définition 5.II.1. — Soit $q \neq 0$ une forme quadratique sur E, $\alpha \in E^\vee$ et $c \in \mathbb{K}$. Une fonction quadratique sur $\mathcal{E}$ est $f : \mathcal{E} \to \mathbb{K}$ qui s'écrit :

$$f(P) = q(\overrightarrow{OP}) + \alpha(\overrightarrow{OP}) + c.$$

Ici, c et α dépendent du choix du point origine O, parfois on écrit donc $\alpha = \alpha_O$ et $c = c_O$. Si on change O par O' on aura:

$$\begin{aligned} f(P) &= q(\overrightarrow{OO'} + \overrightarrow{O'M}) + \alpha_O(\overrightarrow{OO'} + \overrightarrow{O'M}) + c_O = \\ &= q(\overrightarrow{O'M}) + 2\Phi_q(\overrightarrow{OO'}, \overrightarrow{O'M})) + q(\overrightarrow{OO'}) + \alpha_O(\overrightarrow{OO'}) + \alpha_O(\overrightarrow{O'M}) + c_O = \\ &= q(\overrightarrow{O'M}) + \alpha_{O'}(\overrightarrow{O'M}) + c_{O'}, \end{aligned}$$

où on aurait posé :

$$\alpha_{O'} = \alpha_O + 2\Psi_q(\overrightarrow{OO'}), \qquad c_{O'} = c_O + \alpha_O(\overrightarrow{OO'}) + q(\overrightarrow{OO'}).$$

La forme quadratique q ne dépend pas du choix de l'origine.

Définition 5.II.2. — La quadrique affine $\mathcal{Q}$ de $\mathcal{E}$, définie par une fonction quadratique f, est l'ensemble $\mathbb{V}(f)$ des points de $\mathcal{E}$ qui satisfont $f(P) = 0$.

En coordonnées, étant fixé un repère $(O, \vec{e}_1, \dots, \vec{e}_n)$ de $\mathcal{E}$, on écrit P comme $P = O + x_1\vec{e}_1 + \cdots + x_n\vec{e}_n$ et on trouve :

$$f(P) = p(x_1, \dots, x_n) + \ell(x_1, \dots, x_n) + c,$$

où p et ℓ sont polynômes homogènes de degré 2 et 1 en les variables $x_1, \dots, x_n$. Une quadrique affine est donc l'ensemble des solutions d'un polynôme (homogène ou pas) de degré 2.

5.II.B. Quadriques à centre. —

Définition 5.II.3. — Si O est tel que $\alpha_O = 0$, alors O est appelé un *centre* de $\mathcal{Q} = \mathbb{V}(f)$. On dit que $\mathcal{Q}$ est une *quadrique à centre* si elle admet un et un seul centre.

Proposition 5.II.4. — *La quadrique $\mathcal{Q} = \mathbb{V}(f)$ est à centre si et seulement si q est non dégénérée.*

Démonstration. — Soit $O \in \mathcal{E}$ et regardons quand O' est un centre de $\mathcal{Q}$. Nous avons calculé :

$$\alpha_{O'} = \alpha_O + 2\Psi_q(\overrightarrow{OO'}).$$

Donc $\alpha_{O'} = 0$ si et seulement si $\alpha_O = -2\Psi_q(\overrightarrow{OO'})$.

Si q est non dégénérée, Ψ_q est un isomorphisme donc l'équation ci-dessus est satisfaite pour un et un seul point O' de $\mathcal{E}$, i. e. $\mathcal{Q}$ est à centre. Sinon, si Ψ_q n'est pas bijective, soit il n'y pas de solution, soit les solutions sont paramétrées par $\mathrm{Ker}(\Psi_q)$, auquel cas la solution n'est pas unique. □

Remarque 5.II.5. — Si la quadrique $\mathcal{Q}$ est à centre, O étant son centre, alors P appartient à $\mathcal{Q}$ si et seulement si son antipode $\varphi(P) = O - \overrightarrow{OP}$ appartient à $\mathcal{Q}$. En effet, $f(\varphi(P)) = f(O - \overrightarrow{OP}) = q(-\overrightarrow{OP}) + c = q(\overrightarrow{OP}) + c = f(P)$.

5.II.C. Complété projectif d'une quadrique affine. — Soit $\mathcal{E}$ un espace affine, $\hat{\mathcal{E}}$ son complété projectif, et $\mathcal{Q}$ une quadrique de $\mathcal{E}$ définie par le polynôme f.

Définition 5.II.6. — Le complété projectif $\hat{\mathcal{Q}}$ de $\mathcal{Q}$ est la quadrique de $\hat{\mathcal{E}}$ définie par la forme quadratique $\hat{q}$ suivante :

$$\hat{q}(\lambda, \overrightarrow{OP}) = q(\overrightarrow{OP}) + \lambda\alpha(\overrightarrow{OP}) + \lambda^2 c.$$

Remarque 5.II.7. — On a $\hat{\mathcal{Q}} \cap \mathcal{E} = \mathcal{Q}$.

Démonstration. — L'intersection $\hat{\mathcal{Q}} \cap \mathcal{E}$ est constituée des points $(1 : \overrightarrow{OP})$ de $\hat{\mathcal{E}}$ qui annulent $\hat{q}$. Comme $\hat{q}(1, \overrightarrow{OP}) = f(P)$, ces points sont ceux qui annulent f, i. e. les points de $\mathcal{Q}$. □

En coordonnées, on écrit le polynôme qui représente $\hat{q}$:

$$f(P) = f(x_0e_0 + \cdots + e_ne_n) = p(x_1, \ldots, x_n) + x_0\ell(x_1, \ldots, x_n) + cx_0^2,$$

un polynôme homogène de degré 2 en $(x_0, \ldots, x_n)$.

5.II.D. Coniques affines. —

5.II.D.1. Classification des coniques euclidiennes. — Ici, nous prenons $\mathcal{E}$ un plan affine euclidien, autrement dit $\mathcal{E}$ est un espace affine réel de dimension 2, dirigé par un espace vectoriel réel E muni d'un produit scalaire, c'est-à-dire une forme bilinéaire symétrique définie positive. Notons $\langle \vec{u}, \vec{v} \rangle$ le produit scalaire de deux vecteurs $\vec{u}$ et $\vec{v}$ de E.

Nous allons classifier les coniques du plan euclidien à isométrie près, autrement dit nous allons dire que deux coniques associées aux polynômes quadratiques f et g sont équivalentes au sens euclidien s'il existe une transformation affine φ de $\mathcal{E}$, dont la partie linéaire est orthogonale, telle que $g = f \circ \varphi$. L'isométrie φ envoyant une repère orthonormé dans un repère orthonormé, f et g sont équivalente si et seulement si il existe deux repères orthonormés tels que l'expression polynomiale de f et de g en ce repère soient les mêmes.

Proposition 5.II.8. — *Toute conique lisse non vide à centre est équivalente, à isométrie près et pour certains $a_1, a_2 \in \mathbb{R}^*$, à:*

$$\mathbb{V}\left(\frac{x_1^2}{a_1^2} + \frac{x_2^2}{a_2^2} - 1\right), \qquad \textit{une ellipse, ou}$$

$$\mathbb{V}\left(\frac{x_1^2}{a_1^2} - \frac{x_2^2}{a_2^2} - 1\right), \qquad \textit{une hyperbole.}$$

Démonstration. — Le fait que la conique $\mathcal{Q}$ soit à centre implique que la forme quadratique q en deux variables qui lui est associée soit non dégénérée. On se fixe donc un repère $(O, \vec{e_1}, \vec{e_2})$ où O est le centre de la conique et $(\vec{e_1}, \vec{e_2})$ est une base orthonormée de E qui soit orthogonale pour q, ce qui est possible d'après le théorème de diagonalisation des matrices symétriques. On aura donc, si $P = O + x_1\vec{e_1} + x_2\vec{e_2}$, l'expression :

$$f(P) = b_1x_1^2 + b_2x_2^2 + b_0,$$

pour certains $b_0, b_1, b_2 \in \mathbb{R}^*$. En effet, $b_1 \neq 0 \neq b_2$ car sinon q serait dégénérée, tandis que $b_0 \neq 0$ sinon la conique ne serait pas lisse. Ainsi :

$$\mathcal{Q} = \mathbb{V}\left(\frac{-b_1}{b_0}x_1^2 + \frac{-b_2}{b_0}x_2^2 - 1\right)$$

On raisonne ensuite simplement sur le signe de b_1/b_0 et b_2/b_0. En effet, ces deux nombres ne peuvent pas être tous les deux négatifs, sinon la conique serait vide ; supposons alors $b_1/b_0 > 0$ et posons $a_1 = \sqrt{b_0/b_1}$. Puis, si $b_2/b_0 > 0$ on pose $a_2 = \sqrt{b_0/b_2}$, sinon $a_2 = \sqrt{-b_0/b_2}$. On obtiens alors les deux formes souhaitées. □

Considérons $\mathcal{Q} = \mathbb{V}(\hat{q}) \subset \mathbb{P}^2$. Soit $H_i = \mathbb{V}(x_i)$ et regardons $\mathcal{Q} \cap H_i$. On trouve, si la conique est une ellipse :

$$\mathcal{Q} \cap H_0 = \varnothing,$$
$$\mathcal{Q} \cap H_1 = \{(1 : 0 : \pm a_2)\},$$
$$\mathcal{Q} \cap H_2 = \{(1 : \pm a_1 : 0)\}.$$

Si la conique est une hyperbole :

$$\mathcal{Q} \cap H_0 = \{(0 : a_1 : \pm a_2)\},$$
$$\mathcal{Q} \cap H_1 = \varnothing,$$
$$\mathcal{Q} \cap H_2 = \{(1 : \pm a_1 : 0)\}.$$

Proposition 5.II.9. — *Si $\mathcal{Q}$ est lisse mais pas à centre, alors $\mathcal{Q}$ est équivalente, à isométrie près et pour certains $a, b \in \mathbb{R}^*$ et $c \in \mathbb{R}$, à:*

$$\mathbb{V}\left(ax_1^2 + bx_2\right), \qquad \text{une parabole.}$$

Démonstration. — Comme $\mathcal{Q}$ n'est pas à centre, la forme q est dégénérée, donc de rang 1 car elle ne peut pas être nulle. □

5.II.D.2. Classification des coniques affines. — A terminer.

On peut classifier les coniques affines en considérant la classification euclidienne et en admettant des transformations affines quelconques au lieu de n'autoriser que des isométries affines. Le résultat est le suivant.

Proposition 5.II.10. — *Soit $\mathcal{Q}$ une conique affine lisse non vide, $\hat{\mathcal{Q}}$ son complété projectif et H la droite à l'infini. Alors il existe un repère cartésien $(O, \vec{e_1}, \vec{e_2})$ tel que $\mathcal{Q}$ soit l'ensemble des points $P = O + x_1\vec{e_1} + x_2\vec{e_2}$ tels que:*

$$x_1^2 + x_2^2 = 1, \qquad \text{si } \hat{\mathcal{Q}} \cap H = \varnothing, \text{ donc } \mathcal{Q} \text{ est une ellipse,}$$
$$x_1^2 - x_2^2 = 1, \qquad \text{si } \#\left(\hat{\mathcal{Q}} \cap H\right) = 2, \text{ donc } \mathcal{Q} \text{ est une hyperbole,}$$
$$x_1^2 - x_2 = 0, \qquad \text{si } \#\left(\hat{\mathcal{Q}} \cap H\right) = 1, \text{ donc } \mathcal{Q} \text{ est une parabole.}$$

Si $\mathcal{Q}$ est une ellipse, il existe un repère où l'équation de $\mathcal{Q}$ prend la forme $x_1x_2 - 1$.

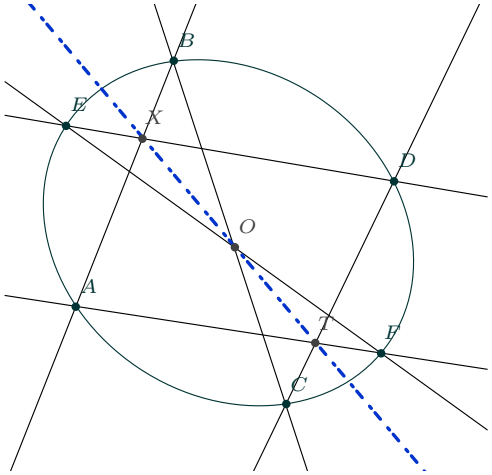
****

5.II.E. Théorème de Pascal. — Revenons sur les coniques projectives pour montrer le théorème de Pascal. Nous utilisons la classification affine des coniques. Fixons un plan projectif $\mathbb{P}(E)$ sur le corps $\mathbb{R}$ une conique lisse non vide $\mathcal{Q} = \mathbb{V}(q)$.

Proposition 5.II.11. — *Soit $M \in \mathcal{Q}$ et considérons $M^\perp \subset \check{\mathbb{P}}(E)$ et l'application $\varphi_M : \mathcal{Q} \to M^\perp$, définie par $P \mapsto (MP)$ pour tout $P \in \mathcal{Q} \setminus \{M\}$ et $\varphi_M(M) = T_M\mathcal{Q}$. Alors φ_M est une bijection et, pour tout $N \in \mathcal{Q}$, $\varphi_M \circ \varphi_N^{-1}$ est une homographie.*

Démonstration. — Soit $N \in \mathcal{Q} \setminus \{M\}$. Prenons (MN) comme droite à l'infini donc considérons le plan affine $\mathcal{E} = \mathbb{P}(E) \setminus (MN)$. Dans ce plan, la conique est une ellipse, car elle est lisse non vide et elle recoupe la droite à l'infini en deux points distincts.

On choisit donc un repère cartésien $(O, \vec{e_1}, \vec{e_2})$ de $\mathcal{E}$ tel que O est le centre de l'ellipse $\mathcal{Q}$ et $\mathcal{Q}$ est l'ensemble des points $P = O + x_1\vec{e_1} + x_2\vec{e_2}$ tels que $x_1x_2 = 1$. Ceci est possible car, d'après la proposition 5.II.8, il existe un repère cartésien $(O, \vec{e_1'}, \vec{e_2'})$ tel que l'équation de $\mathcal{Q}$ soit $x_1^2 - x_2^2 - 1$, donc en posant $\vec{e_1} = \vec{e_1'} + \vec{e_2'}$, □


B
E
X
D
O
A
I
F
C

CHAPITRE 6

GROUPE ORTHOGONAL GÉNÉRAL

Ce chapitre est très proche de [**Per96**]. Soit $\mathbb{K}$ un corps de caractéristique différente de 2 et E un espace vectoriel de dimension $n < \infty$ sur $\mathbb{K}$. La notation q sera réservée à une forme quadratique non dégénérée sur E.

6.I. Automorphismes orthogonaux, réflexions, générateurs

6.I.A. Formes quadratiques, isotropie. — Soit F un sous espace vectoriel de E. Le noyau de $q|_F$ est $F \cap F^\perp$. On a aussi, du moment que q est non dégénérée:

$$\dim(F^\perp) = n - \dim(F), \qquad F^{\perp\perp} = F.$$

Définition 6.I.1. — Un sous espace vectoriel $F\{0\}$ de E est *isotrope* si $q|_F$ est dégénérée. On dit que F est *totalement isotrope* si $q|_F = 0$. On dit que q est *anisotrope* si E n'admet pas d'espace vectoriel non nul isotrope.

Remarque 6.I.2. — On a $F \neq \{0\}$ isotrope si et seulement si $F \cap F^\perp \neq 0$. On en déduit que $F^\perp$ est isotrope si et seulement si $F^\perp$ l'est. Ainsi, F est non isotrope si et seulement si $E = F \oplus F^\perp$, la somme étant orthogonale. Nous notons alors :

$$E = F \overset{\perp}{\oplus} F^\perp.$$

De plus, F est totalement isotrope si et seulement si $F \subset F^\perp$.

Définition 6.I.3. — On note $\mathrm{O}(q)$ l'ensemble des automorphismes orthogonaux de (E, q), i.e. les éléments $f \in \mathrm{GL}(E)$ tels que, pour tout $u \in E$:

$$q(u) = q(f(u)).$$

En passant à la polarisation, ceci équivaut à ce que, pour tout $u, v \in E$, on ait :

$$\Phi_q(u, v) = \Phi_q(f(u), f(v)).$$

6.I.B. Symétries, réflexions. —

Définition 6.I.4. — Soit F un sous espace non isotrope de E. Alors nous avons la symétrie orthogonale τ_F définie par :

$$\tau_F(u) = u' - u'', \qquad \text{où } (u', u'') \text{ est l'unique couple de } F \times F^\perp \text{ tel que } u = u' + u''.$$

On parle de réflexion orthogonale si H est un hyperplan. On parle de renversement si H a codimension 2.

Lemme 6.I.5. — *Soit u, v vecteurs de E tels que $q(u) = q(v) \neq 0$. Alors il existe $f \in \mathrm{GL}(E)$ telle que $f(u) = v$, où f est une réflexion ou un produit de deux réflexions. Si q est anisotrope et $u \neq v$, la réflexion d'axe $(u-v)^\perp$ convient.*

Démonstration. — Remarquons que $(u-v) \perp (u+v)$, car:

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

La raison de distinguer deux cas est l'alternative $u - v$ isotrope ou pas.

Si $q(u-v) \neq 0$, nous définissons $H = (u-v)^\perp$. Il s'agit d'un hyperplan non isotrope, donc nous avons la réflexion τ_H. On a Donc on a $u + v \in H$ et on écrit la décomposition de u en $E = H^\perp \oplus H$:

$$u = \frac{1}{2}(u+v) + \frac{1}{2}(u-v).$$

On en obtient :

$$\tau_H(u) = \frac{1}{2}(u+v) - \frac{1}{2}(u-v) = v.$$

Bien sûr, nous sommes dans ce cas si q est anisotrope et $u \neq v$, i. e. $u - v \neq 0$.

Maintenant si $q(u-v) = 0$, on trouve $q(u+v) \neq 0$. En effet:

$$0 = q(u-v) = q(u) - 2\Phi_q(u,v) + q(v),$$

donc $q(u) = \Phi_q(u,v)$, ainsi :

$$q(u+v) = q(u) + 2\Phi_q(u,v) + q(v) = 4q(u) \neq 0.$$

Dans ce cas, on considère $H_1 = (u+v)^\perp$. On écrit la décomposition de u en $E = H_1^\perp \oplus H_1$:

$$u = \frac{1}{2}(u-v) + \frac{1}{2}(u+v).$$

On en obtient :

$$\tau_{H_1}(u) = \frac{1}{2}(u-v) - \frac{1}{2}(u+v) = -v.$$

On considère ensuite $H_2 = v^\perp$. On a $v \in H_2^\perp$ donc $\tau_{H_2}(v) = -v$. Finalement :

$$\tau_{H_2}\tau_{H_1}(u) = v.$$

□

6.I.C. Générateurs. —

6.I.C.1. Génération par des réflexions. —

Théorème 6.I.6. — *Le groupe $\mathrm{O}(q)$ est engendré par des réflexions. Si q est anisotrope, $f \in \mathrm{O}(q)$ peut s'écrire comme produit de m réflexions, avec $m \leq \dim(\mathrm{Fix}(f)^\perp) \leq n$.*

Démonstration. — Regardons le premier énoncé. On raisonne par récurrence sur $n = \dim(E)$. Si $n = 1$, nous avons $\mathrm{O}(q) = \{\pm \mathrm{id}_E\}$. Si $f = \mathrm{id}_E$, nous n'avons besoin d'aucune réflexion et le résultat est vrai. Sinon $f = -\mathrm{id}_E$, et la réflexion d'hyperplan $H = \{0\}$ convient.

Pour $n \geq 2$, nous supposons donc que, pour tout espace vectoriel F muni d'une forme quadratique non dégénérée, le groupe orthogonal associé soit engendré par des réflexions.

D'abord, comme q est non dégénérée, il existe $u \in E$ tel que $q(u) \neq 0$. En effet, il existe $v_1, v_2 \in E$ tels que :

$$0 \neq \Phi_q(v_1, v_2) = \frac{1}{2}(q(v_1+v_2) - q(v_1) - q(v_2)),$$

donc au moins l'une des valeurs $q(v_1+v_2)$, $q(v_1)$, $q(v_2)$ est non nulle : on choisit donc u parmi v_1, v_2 et $v_1 + v_2$.

Soit donc $f \in \mathrm{GL}(E)$. Comme f est orthogonale, $v = f(u)$ satisfait $q(u) = q(v)$. D'après le lemme 6.I.5, il existe donc $g \in \mathrm{O}(q)$ qui est une réflexion ou un produit de deux réflexions, tel que $g(u) = v$. Soit $h = g \circ f$. On a $h(u) = g(f(u)) = g(v) = u$.

Ainsi, nous considérons $F = u^\perp$. Il s'agit d'un sous espace non isotrope de E de dimension $n-1$, ce qui veut dire $q|_F$ non dégénérée.

Comme h est orthogonale, F est stable par h, donc $h|_F$ est un automorphisme orthogonale de $(F, q|_F)$. Par hypothèse de récurrence, il existe des réflexions orthogonales $\sigma_1, \dots, \sigma_m$ de F telles que $h|_F = \sigma_1 \circ \cdots \circ \sigma_m$. Nous avons donc $\tilde{\sigma}_1, \dots, \tilde{\sigma}_m$ réflexions de E obtenues par linéarité en définissant pour tout $i \in [\![1, m]\!]$:

$$\begin{aligned} &\tilde{\sigma}_i(v) = \sigma_i(v), && \text{pour tout } v \in F; \\ &\tilde{\sigma}_i(u) = u. \end{aligned}$$

Il s'agit bien sûr de réflexions, et $h = \tilde{\sigma}_1 \circ \cdots \circ \tilde{\sigma}_m$, car ceci est vrai sur F et sur u, donc sur une base de E, donc sur E. Finalement:

$$f = g^{-1} \circ h = g^{-1} \circ \tilde{\sigma}_1 \circ \cdots \circ \tilde{\sigma}_m,$$

ce qui donne le résultat. En effet, g étant produit de réflexions, g^{-1} est aussi un produit de réflexions et f est donc exprimé comme produit de réflexions.

Pour montrer le deuxième énoncé, si q est anisotrope on considère $f \in \mathrm{O}(q)$, on pose $E_0 = \mathrm{Fix}(f)^\perp$ et on raisonne par récurrence sur $n_0 = \dim(E_0)$. Si $n_0 = 0$, on a $f = \mathrm{id}_E$ et le résultat est clair, car nous n'avons besoin d'aucune réflexion.

Si $n_0 \geq 1$, on prend $u \in E_0 \setminus \{0\}$, donc $v = f(u)$ est différent de u. Ainsi, d'après le lemme 6.I.5, il la réflexion $g = \sigma_H$, où $H = (u-v)^\perp$, satisfait $g(u) = v$.

De nouveau on pose $h = g \circ f$. Si $w \in \mathrm{Fix}(f)$, alors $w \perp (u - v)$ car :

$$\begin{aligned} \Phi_q(w, u-v) &= \Phi_q(w,u) - \Phi_q(w,v) = \\ &= \Phi_q(w,u) - \Phi_q(f(w), f(u)) = \Phi_q(w,u) - \Phi_q(w,u) = 0. \end{aligned}$$

Ainsi, si $w \in \mathrm{Fix}(f)$, on a $w \in (u-v)^\perp = H$, donc w est fixé par g, réflexion d'axe H. Nous avons donc $\mathrm{Fix}(f) \subset \mathrm{Fix}(h)$.

De plus, $\mathrm{Fix}(f) \subsetneq \mathrm{Fix}(h)$ car $u \in \mathrm{Fix}(h) \setminus \mathrm{Fix}(f)$. Donc $\mathrm{Fix}(h)^\perp \subsetneq F_0$, c'est-à-dire l'espace fixe de h est de dimension au plus $n_0 - 1$. Par hypothèse de récurrence (forte), il existe donc $\sigma_1, \dots, \sigma_m$ réflexions de E telles que $h = \sigma_1 \circ \cdots \circ \sigma_m$ avec $m \leq n_0 - 1$. Donc $f = g^{-1} \circ \sigma_1 \circ \cdots \circ \sigma_m$. Ainsi f s'exprime comme produit d'un nombre $m+1$ de réflexions, où $m+1 \leq n_0 - 1 + 1 = n_0$. □

6.I.C.2. Groupe orthogonal positif, renversements. —

Proposition 6.I.7. — *Si $n \geq 3$, $\mathrm{SO}(q)$ est engendré par les renversements.*

Démonstration. — Soit $f \in \mathrm{SO}(q)$. Alors f est produit d'un nombre pair réflexions.

Si $n = 3$ et σ est une réflexion, alors $-\sigma$ est un renversement. En effet, si H est un hyperplan $-\sigma_H = \sigma_{H^\perp}$ et $H^\perp$ a dimension 1, i.e., codimension 2. Donc f est le produit (d'un nombre pair de) renversements.

Soit $n \geq 4$ et considérons σ_{H_1} et σ_{H_2} deux réflexions d'hyperplans non isotropes $H_1 = u_1^\perp$ et $H_2 = u_2^\perp$, que l'on peut supposer distincts.

Si $H_1 \cap H_2$ est non isotrope, en choisissant les premiers $n-3$ vecteurs d'une base orthogonale de $H_1 \cap H_2$ on trouve un sous espace non isotrope de dimension $n-3$.

Sinon, soit $K = \mathrm{vect}(u_1, u_2)$. Le noyau K_0 de la restriction de q à est $K^\perp \cap K$, ce qui est aussi le noyau de la restriction de q à $K^\perp$. Or $q|_K \neq 0$ car u_1 et u_2 ne sont pas isotropes. Donc le noyau K_0 de $q|_{K^\perp}$ a dimension 1. Un supplémentaire orthogonal F de K_0 dans $K^\perp = H_1 \cap H_2$ a dimension $n-3$ et n'est pas isotrope.

En définitive, on peut choisir un sous espace F non isotrope de codimension 3 de $H_1 \cap H_2$. Ainsi $F^\perp \subset E$ est un sous espace de dimension 3 contenant u_1 et u_2. Les restrictions de σ_{H_1} et σ_{H_2} à F coïncident avec id_F, tandis que leurs restrictions à $F^\perp$ sont des réflexions.

D'après ce que nous avons vu pour la dimension 3, on a deux renversements ρ_1 et ρ_2 de F tels que $\sigma_{H_1}\sigma_{H_2}|_F = \rho_1\rho_2$. On définit des extensions $\tilde{\rho}_1$ et $\tilde{\rho}_2$ de ρ_1 et ρ_2 à E en posant, pour $i \in [\![1,2]\!]$:

$$\tilde{\rho}_i(v) = \rho_i(v), \qquad \text{pour tout } v \in F^\perp;$$
$$\tilde{\rho}_i(v) = v, \qquad \text{pour tout } v \in F.$$

On a $\rho_1\rho_2 = \sigma_{H_1}\sigma_{H_2}$, car ceci est vrai sur F et sur $F^\perp$ et $E = F \oplus F^\perp$. De plus, $\tilde{\rho}_1$ et $\tilde{\rho}_2$ sont des renversements.

Maintenant le résultat est clair : nous écrivons $f \in \mathrm{SO}(q)$ comme produit d'un nombre pair de réflexions, chaque couple de réflexions pouvant s'écrire comme produit de deux renversements, f s'écrit comme produit (d'un nombre pair) de renversements. □

6.II. Groupe orthogonal général

6.II.A. Isotropie, hyperbolicité. —

6.II.A.1. Plans hyperboliques. —

Définition 6.II.1. — Soit P un espace vectoriel sur $\mathbb{K}$ de dimension 2 et q une forme quadratique non dégénérée sur P. On dit que (P,q) est un plan hyperbolique s'il existe $u \in P \setminus \{0\}$ tel que $q(u) = 0$. Dans ce cas, si $B = (u,v)$ est une base de P telle que

$$\mathrm{Mat}_B(q) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

alors on dit que B est une base hyperbolique de (P,q).

Lemme 6.II.2. — *Soit (P,q) un plan hyperbolique et $u \in P \setminus \{0\}$ isotrope. Alors il existe v tel que $B = (u,v)$ soit une base hyperbolique de (P,q).*

Démonstration. — Soit v_1 un vecteur indépendant de u. Il existe alors $a, b \in \mathbb{K}$ tels que:

$$\mathrm{Mat}_{(u,v_1)}(q) = \begin{pmatrix} 0 & a \\ a & b \end{pmatrix},$$

avec $a \neq 0$ car q est non dégénérée. Quelque soit $\lambda \in \mathbb{K}$, on a $v_2 = \lambda u + v_1$ indépendant de u et $\Phi_q(u, v_2) = a$ et $q(v_2) = 2\lambda a + b$. Si on choisit $\lambda = -b/2a$, on trouve :

$$\mathrm{Mat}_{(u,v_2)}(q) = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix},$$

Maintenant, on écrit $v = u + (1/a)v_2$. C'est encore un vecteur indépendant de u. On obtient $\Phi_q(u,v) = 1$ et $q(v) = 0$ donc (u,v) est la base cherchée. □

Remarque 6.II.3. — Soit q non dégénérée sur E et B une base de E. La valeur $\delta = \det(\mathrm{Mat}_B(q))$ est non nulle et, si B' est une autre base de E et $\delta' = \det(\mathrm{Mat}_{B'}(q))$ alors il existe un carré de $\mathbb{K}$, i.e. un élément ε^2, où $\varepsilon \in \mathbb{K}$ tel que $\delta' = \varepsilon^2\delta$. La valeur δ, définie à un carré près, est appelée le discriminant de q.

Lemme 6.II.4. — *Soit q une forme quadratique sur un plan P. Alors (P,q) est un plan hyperbolique si et seulement si $\det(q) = -1$ à un carré de $\mathbb{K}^*$ près.*

Démonstration. — Si (P,q) est un plan hyperbolique, on peut en choisir une base hyperbolique B et bien sûr $\det(M_B(q)) = -1$.

Réciproquement, soit $B = (u_1, u_2)$ une base de E orthogonale pour q et $\varepsilon \in \mathbb{K}^*$ tel que $\det(\mathrm{Mat}_B(q)) = -\varepsilon^2$. Ainsi il existe $a_1, a_2 \in \mathbb{K}$ avec $a_1 a_2 = -\varepsilon^2$ et tels que, pour tout $(x_1, x_2) \in \mathbb{K}^2$, on ait $q(x_1u_1 + x_2u_2) = a_1x_1^2 + a_2x_2^2$. Forcément a_1 et a_2 sont non nul. Soit $\varepsilon_0 = \varepsilon/a_1 \in \mathbb{K}^*$, donc $a_2/a_1 = -\varepsilon_0^2$. On trouve ainsi :

$$q(x_1u_1 + x_2u_2) = a_1(x_1^2 - \varepsilon_0^2 x_2^2) = a_1(x_1 + \varepsilon_0 x_2)(x_1 - \varepsilon_0 x_2),$$

donc $u = \varepsilon_0 u_1 + u_2$ est un vecteur non nul (car u_1 et u_2 sont indépendants) et isotrope (car $q(u) = a_1(\varepsilon_0 + \varepsilon_0)(\varepsilon_0 - \varepsilon_0) = 0$).

Finalement q est non dégénérée (car son discriminant vaut -1) avec un vecteur isotrope non nul, ainsi (P,q) est un plan hyperbolique. □

6.II.A.2. Espaces hyperboliques. — Un espace hyperbolique est une somme directe orthogonale de plans hyperboliques.

Proposition 6.II.5. — *Soit F un sous espace de E, F_0 le noyau de $q|_F$ et $(u_1, \dots, u_r)$ une base de F_0. Soit U un supplémentaire orthogonal de F_0 dans F. Alors il existe $(v_1, \dots, v_r)$ vecteurs de E tels que pour tout $i \in [\![1, r]\!]$, (u_i, v_i) soit une base hyperbolique de $P_i = \mathrm{vect}(u_i, v_i)$ et que l'on ait une somme directe orthogonale :*

$$G = U \overset{\perp}{\oplus} P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r.$$

Démonstration. — On raisonne par récurrence sur r. Si $r = 0$, il n'y a rien à démontrer. Soit alors $r \geq 1$ et supposons l'énoncé valide pour tout sous espace où la restriction de q possède un noyau de dimension strictement inférieure à r.

Considérons $F' = U \oplus \mathrm{vect}(u_2, \dots, u_r)$. On a $F' \subsetneq F$ donc $F^\perp \subsetneq (F')^\perp$ car si $F^\perp = (F')^\perp$ on trouverait $F' = F$ en prenant encore les orthogonaux. On peut alors choisir $v \in (F')^\perp \setminus F^\perp$. Ainsi, $v \perp F'$, donc $v \perp U$ et $v \perp u_i$ pour tout $i \in [\![2, r]\!]$ mais $v \notin F^\perp$ donc forcément $\Phi_q(v, u_1) \neq 0$.

Le plan $P_1 = \mathrm{vect}(u_1, v)$ est donc hyperbolique car la restriction de q à ce plan est non dégénérée contient le vecteur isotrope $u_1 \neq 0$ et $\Phi_q(v, u_1) \neq 0$. On peut alors trouver une base hyperbolique (u_1, v_1) de ce plan d'après le lemme 6.II.2.

Soit alors $F'' = F' \oplus P_1$. Le noyau de la restriction q'' de q à F'' est $F_0'' = \mathrm{vect}(u_2, \dots, u_n)$. En effet, on peut en construire une base en juxtaposant une base de U, $(u_2, \dots, u_r)$ et (u_1, v_1), en obtenant une matrice diagonale par blocs de noyau $\mathrm{vect}(u_2, \dots, u_r)$.

Ainsi, nous pouvons appliquer l'hypothèse de récurrence à F'', en prenant le supplémentaire $U'' = U \oplus P_1$ de F_0'' dans F''. On en obtient $(v_2, \dots, v_r)$ vecteurs de E tels que pour tout $i \in [\![2, r]\!]$ on ait (u_i, v_i) base hyperbolique de $P_i = \mathrm{vect}(u_i, v_i)$ et que l'on ait la somme directe orthogonale :

$$G = U'' \overset{\perp}{\oplus} P_2 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r = U \overset{\perp}{\oplus} P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r.$$

□

Remarque 6.II.6. — Le noyau de $q|_G$ est trivial, i. e. G est non isotrope. En effet, soit C une base de U et :

$$\mathrm{Mat}_{(C,u_1,\dots,u_r)}(q|_F) = \mathrm{diag}(M, 0), \qquad \text{où } M = \mathrm{Mat}_C(q|_U).$$

Comme le noyau de $q|_F$ est $\mathrm{vect}(u_1, \dots, u_r)$, on a M inversible. Ainsi, on a :

$$\mathrm{Mat}_{(C,u_1,v_1\dots,u_r,v_r)}(q|_F) = \mathrm{diag}(M, M_1, \dots, M_r), \qquad \text{où } M_i = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

pour tout $i \in [\![1, r]\!]$. Cette matrice est donc inversible.

Corollaire 6.II.7. — *Soit F totalement isotrope. Alors il existe H hyperbolique contenant F tel que* $\dim(H) = 2\dim(F)$.

Soit H sous espace de E. Alors H est hyperbolique si et seulement si H admet un sous espace totalement isotrope F tel que $\dim(H) = 2\dim(F)$.

Démonstration. — Si F est totalement isotrope, on a $U = 0$, en la notation de la proposition précédente. Ainsi, le premier énoncé est évident.

Si H admet un sous espace totalement isotrope F tel que $\dim(H) = 2\dim(F)$, encore une fois en utilisant la proposition précédente avec $F = F_0$, il existe $G \subset H$ hyperbolique contenant F, mais $G = H$ car $\dim(G) = 2\dim(F) = \dim(H)$.

Si H est hyperbolique, somme directe orthogonale des plans $P_1, \dots, P_r$ ayant bases hyperboliques $(u_1, v_1), \dots, (u_r, v_r)$, on a $F = \mathrm{vect}(u_1, \dots, u_r)$ sous espace totalement isotrope et $\dim(F) = r$, $\dim(H) = 2r$. □

6.II.B. Théorème de Witt. — Soit q forme quadratique non dégénérée sur E.

Théorème 6.II.8. — *Soit F, F' sous espaces vectoriels de E. Les affirmations suivantes sont équivalentes:*

i) Il existe $f \in \mathrm{O}(q)$ tel que $f(F) = F'$.

ii) Les formes quadratiques $q|_F$ et $q|_{F'}$ sont équivalentes.

Remarque 6.II.9. — Voici une liste d'observations sur ce théorème.

1) On peut dire aussi que les formes quadratiques $q|_F$ et $q|_{F'}$ sont équivalentes si et seulement si il existe une isométrie entre $(F, q|_F)$ sur $(F', q|_{F'})$.
2) L'implication i) ⇒ ii) est claire. En effet, $f|_F$ est l'isométrie entre $(F, q|_F)$ et $(F', q|_{F'})$.

Réduction au cas F non isotrope. — Supposons que l'énoncé est valide pour le cas des sous espaces non isotropes et montrons qu'il est alors valide en général.

Soit donc F isotrope. Alors $q|_F$ possède un noyau F_0 de dimension $r \neq 0$. Soit $(u_1, \dots, u_r)$ une base de F_0. Soit U un supplémentaire orthogonal de F_0 dans F. D'après la proposition 6.II.5, il existe r vecteurs $(v_1, \dots, v_r)$ de E tels que, pour tout $i \in [\![1, r]\!]$ les plans $P_i = \mathrm{vect}(u_i, v_i)$, muni des formes quadratiques $q_i = q|_{P_i}$ admettent (u_i, v_i) comme base hyperbolique et que l'on ait une somme directe orthogonale :

$$G = U \overset{\perp}{\oplus} P_1 \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r.$$

Maintenant G n'est pas isotrope.

Supposons alors qu'il existe $h : F \to F'$ isomorphisme isométrique par rapport à $q|_F$ et $q|_{F'}$ et montrons qu'il existe alors $f \in \mathrm{O}(q)$ tel que $f(F) = F'$. Comme h est isométrique, i.e., $q|_F$ et $q|_{F'}$ sont équivalentes, le noyau F_0' de $q|_{F'}$ est aussi de dimension r et h induit un isomorphisme de F_0 sur F_0'. Soit alors, pour $i \in [\![1, r]\!]$, $u_i' = h(u_i)$, donc $(u_1', \dots, u_r')$ est une base de F_0'. Aussi, $U' = h(U)$ est un supplémentaire orthogonal de F_0' dans F'.

Or, de nouveau par la proposition 6.II.5, il existe $(v_1', \dots, v_r')$ tels que, $\forall i \in [\![1, r]\!]$, on ait des bases hyperboliques (u_i', v_i') des plans $P_i' = \mathrm{vect}(u_i', v_i')$, muni des formes quadratiques $q_i' = q|_{P_i'}$. On obtient une somme directe orthogonale :

$$G' = U' \overset{\perp}{\oplus} P_1' \overset{\perp}{\oplus} \cdots \overset{\perp}{\oplus} P_r'.$$

On peut alors définir $\tilde{h}$ en posant $\tilde{h}(v_i) = v_i'$ pour tout $i \in [\![1, r]\!]$ et $\tilde{h}(u) = h(u)$ pour tout $u \in F$. On trouve ainsi un isomorphisme de G sur G', qui est une isométrie car $\tilde{h}$ se restreint à une isométrie de U sur U' et aussi de P_i sur P_i', puisque $\tilde{h}$ envoie bases hyperboliques en bases hyperboliques.

Comme G et G' sont non isotropes, on a la conclusion générale si l'énoncé est valable pour les sous espaces non isotropes. □

Preuve pour sous espaces non isotropes. — Soit F non isotrope de dimension m. Montrons le théorème de Witt par récurrence sur m. Bien sûr, F' doit aussi avoir dimension 1.

Soit $m = 1$ et u un générateur de F, u non isotrope i. e. $q(u) \neq 0$. Soit h un isomorphisme de F sur F' et $u' = h(u)$ donc $q(u') = q(u)$. Nous avons montré au lemme 6.I.5 qu'il existe un automorphisme orthogonal f, plus précisément une réflexion ou un produit de deux réflexions, tel que $f(u) = u'$. Ainsi le résultat est montré si $m = 1$.

Soit maintenant $m \geq 2$ et supposons que le théorème de Witt soit valide pour tout sous espace non isotrope de dimension au plus $m - 1$ d'un espace vectoriel muni d'une forme quadratique non dégénérée.

Choisissons un vecteur u non isotrope de F (ce qui existe car $q|_F$ est non dégénérée) et écrivons F comme somme directe orthogonale de $F_1 = \mathrm{vect}(u)$ et d'un supplémentaire orthogonal F_2. Notons $h_1 = h|_{F_1}$ et $h_2 = h|_{F_2}$.

D'après le cas $m = 1$, h_1 s'étend à $f_1 \in \mathrm{O}(q)$, i. e. $f_1|_{F_1} = h_1$. Considérons alors :

$$k : F \to F, \qquad k = f_1^{-1}|_F \circ h.$$

On a $k|_{F_1} = \mathrm{id}_{F_1}$ et $k|_{F_2} = f_1^{-1}|_{F_2} \circ h_2$.

On considère donc $F_1^\perp \subset E$, muni de la forme non dégénérée $q|_{F_1^\perp}$. Bien sûr, $F_2 \subset F_1^\perp$. Donc, comme $k|_{F_1} = \mathrm{id}_{F_1}$, on a $k(F_2) \subset F_1^\perp$. En effet, si $v_1 \in F_1$ et $v_2 \in F_2$, on trouve:

$$\Phi_q(v_1, k(v_2)) = \Phi_q(k(v_1), k(v_2)) = \Phi_q(v_1, v_2) = 0.$$

Nous avons donc F_2 sous espace de dimension $n - 1$ de $F_1^\perp$ et $k : F \to F$ isométrie $F_2 \to k(F_2)$. D'après l'hypothèse de récurrence, il existe alors g automorphisme orthogonal de $F_1^\perp$ tel que $g|_{F_1^\perp} = k$. On étend alors g à $f_2 \in \mathrm{O}(q)$ en posant $f_2(u) = u$ pour tout $u \in F_1$. Du moment que $E = F_1 \oplus F_1^\perp$, la somme étant orthogonale, ceci définit bien f_2 comme un automorphisme orthogonal de E.

Posons $f = f_1 \circ f_2$. Pour F_1, on a $f_2|_{F_1} = \mathrm{id}_{F_1}$ et $f_1|_{F_1} = h_1$, donc:

$$f|_{F_1} = f_1|_{F_1} \circ f_2|_{F_1} = h_1.$$

Pour F_2, on a $f_2|_{F_2} = k|_{F_2} = f_1^{-1}|_{F_2} \circ h_2$. Donc :

$$f|_{F_2} = f_1|_{F_2} \circ f_2|_{F_2} = f_1|_{F_2} \circ f_1^{-1}|_{F_2} \circ h_2 = h_2.$$

Autrement dit, $f \in \mathrm{O}(q)$ et $f|_F = h$. Le théorème est démontré. □

Corollaire 6.II.10. — *Tout sous espace totalement isotrope est contenu dans un sous espace totalement isotrope maximal, et ces derniers ont tous dimension $\nu(q)$.*

Démonstration. — Soit F un sous espace totalement isotrope. Soit F est maximal, soit il est strictement contenu dans un sous espace totalement isotrope, qui a son tour est maximal ou pas. Ce processus se termine car $\dim(E) < \infty$, donc F est contenu dans un sous espace isotrope maximal G. Soit m sa dimension.

Soit H un autre sous espace isotrope maximal, de dimension p et supposons $p < m$. Tout sous espace K de G de dimension p est isotrope. Ainsi, $q|_K$ et $q|_H$ sont équivalentes, à savoir, elles sont toutes deux nulles.

D'après le théorème de Witt, il existe alors $f \in \mathrm{O}(q)$ tel que $f(H) = K$. Mais K n'est pas maximal, étant strictement contenu dans G, alors que H l'était, contradiction. □

Corollaire 6.II.11. — *On peut écrire $E = H \oplus F$, la somme étant orthogonale, avec H hyperbolique et $q|_F$ anisotrope. On a:*

i) $\dim(H) = 2\nu(q)$*;*

ii) si $E = H' \oplus F'$ somme orthogonale avec avec H' hyperbolique et $q|_{F'}$ anisotrope, alors il existe $f \in \mathrm{O}(q)$ tel que:

$$f(H) = H', \qquad f(F) = F'.$$

En particulier, la forme anisotrope $q|_F$ est uniquement déterminée à équivalence près.

Démonstration. — On part de G, un sous espace totalement isotrope maximal de E. Nous pouvons compléter G en un espace hyperbolique H, donc non isotrope. On pose alors $F = H^\perp$ et on a $E = H \oplus F$, la somme étant orthogonale. Notons que $q|_F$ est anisotrope. En effet, si F contenait un vecteur isotrope u non nul, on aurait $G' = \mathrm{vect}(G, u)$ totalement isotrope, ce qui contredirait la maximalité de G.

Étant donné une décomposition $E = H \oplus F$, comme H est hyperbolique de dimension $2m$ il contient un sous espace isotrope G de dimension $m \leq \nu(q)$, donc $\dim(H) \leq 2\nu(q)$, et G est maximal dans H, i. e. pour tout u' isotrope de $G^\perp \cap H$, on a $u' \in G$.

Or G est maximal aussi dans E. En effet, pour tout vecteur u isotrope de $G^\perp$, on a $u = u' + u''$, avec $u' \in H$ et $u'' \in F$. Mais si $v \in G$ on a $0 = \Phi_q(u, v) = \Phi_q(u', v)$ donc $u' \in G^\perp \cap H$, ainsi $u' \in G$. On a donc $0 = q(u) = q(u') + q(u'') = q(u'')$, et par anisotropie de $q|_F$ on a $u'' = 0$, i.e. $u \in G$. Autrement dit, G est totalement isotrope maximal. Donc $\dim(G) = \nu(q)$.

Étant donnée une autre décomposition $E = H' \oplus F'$, il est clair que $q|_H$ et $q|_{H'}$ sont équivalentes, car H et H' sont hyperboliques de même dimension. Il existe donc, d'après le théorème de Witt, un automorphisme orthogonal f de E tel que $f(H) = H'$. Par conséquent $f(F) = F'$, car $F = H^\perp$ et $F = (H')^\perp$. □

BIBLIOGRAPHIE

[Aud06] Michèle Audin, *Géométrie*, EDP Sciences, Les Ulis, France, 2006.

[Per96] Daniel Perrin, *Cours d'algèbre*, Ellipses, Paris, 1996.