Notes du cours de géométrie

Daniele Faenzi

16 mai 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.II. Barycentres

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

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

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

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

En effet,

1.III. Applications affines

1.IV. Théorèmes classiques de géométrie affine

1.V. Théorème fondamental de la géométrie affine

CHAPITRE 2

GÉOMÉTRIE PROJECTIVE

2.I. Espaces projectifs

Ici, $\mathbb{K}$ est un corps (commutatif).

2.I.A. Droites vectorielles. —

Définition 2.I.1. — Soit E un $\mathbb{K}$-espace vectoriel. 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 $\dim(E) = n+1$, on dit que $\mathbb{P}(E)$ est un espace projectif de dimension n.

2.I.B. Ouverts affines. — En cours de rédaction

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

2.I.D. Dualité. —

2.I.D.i. 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 2.I.2. — 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 2.I.3. — *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 $B = (e_1, \dots, e_n)$ de E, nous pouvons construire la base duale $B^\vee = (e_1^\vee, \dots, e_n^\vee)$ 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):

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

□

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

2.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 $\mathbb{P}(E)$.

2.I.E.i. Théorème de Pappus. —

2.I.E.ii. Théorème Désargues. —

Théorème 2.I.4. — *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.

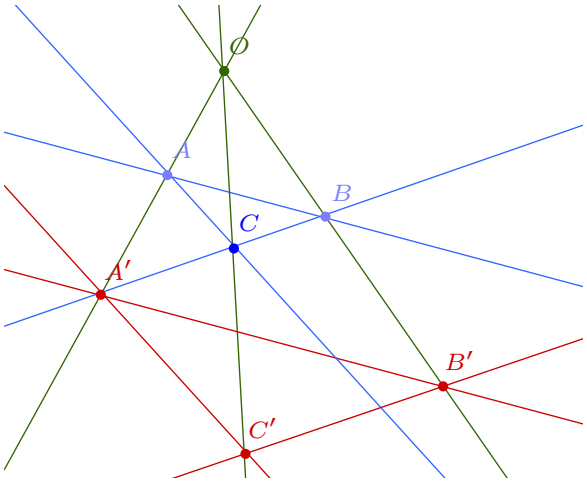


FIGURE 1. Théorème de Désargues en affine

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

$$\begin{aligned} X &= (BC)^\perp, & Y &= (AC)^\perp, & Z &= (AB)^\perp, \\ X' &= (B'C')^\perp, & Y' &= (A'C')^\perp, & Z' &= (A'B')^\perp. \end{aligned}$$

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. □

2.II. Applications projectives

2.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 2.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 2.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 2.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.

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

2.II.B.i. 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 2.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 2.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 $\hat{u}_{n+1} = \hat{u}_0 + \dots + \hat{u}_n$ et $\hat{v}_{m+1} = \hat{v}_0 + \dots + \hat{v}_m$ 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:

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

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

2.II.B.ii. 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 2.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. □

2.II.C. Homographies et repères. —

Définition 2.II.7. — Une homographie est une application projective bijective, i. e., une application projective induite par un isomorphisme linéaire.

Proposition 2.II.8. — *Soit $(A_0, \ldots, A_{n+1})$ et $(B_0, \ldots, B_{n+1})$ 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 $(u_0, \ldots, u_n)$ et $(v_0, \ldots, v_n)$ 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 $(v_0,\dots,v_n)$ 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 $\varphi=\psi$. □

2.II.D. Groupe des homographies. —

Définition 2.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 2.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 $(u_1,\dots,u_n)$ 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 $(u_1,\dots,u_n)$ est une base, que $\lambda=\lambda_i$ quelque soit $i\in[\![1,n]\!]$. Ceci montre que g est une homothétie, de rapport λ. □

2.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 2.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 2.II.12. — Par définition nous avons:

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

Proposition 2.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 2.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 2.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 2.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 $[x_1u_0'+x_0u_1']=D$ 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 $u_0'=x_0u_0$ et $u_1'=x_1u_1$ 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 3

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.

3.I. Propriétés de base

Définition 3.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 groupe 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.

3.I.A. Générateurs. —

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

$$D \not\subset H.$$

Définition 3.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 3.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 $\mathrm{diag}(1, \ldots, 1, \lambda)$;

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 $D = \mathrm{Im}(f - \mathrm{id}_E)$. □

3.I.A.ii. Transvections. — Soit H un hyperplan de E et D une droite de E, avec :

$$D \subset H.$$

Définition 3.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 3.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 $(u_1, \dots, u_n)$ 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 $(u_1, \dots, u_{n-1})$ de H. Soit $B = (u_1, \dots, u_n)$. La matrice $\mathrm{Mat}_B(f)$ a la forme voulue.

vii) ⇒ iii). Évident.

iii) ⇒ ii). Si f était diagonalisable, on aurait $\lambda_1, \dots, \lambda_n \in \mathbb{K}$ 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) ⇒ 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) ⇒ 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) ⇐ 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) ⇒ 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) ⇐ vi). Si f prend la forme décrite dans vi), alors $\mathrm{Im}(f - \mathrm{id}_E) = \mathrm{vect}(w) \subset H$. □

Remarque 3.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 3.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 :

$$\begin{aligned} v \in \mathrm{Im}(gfg^{-1} - \mathrm{id}_E) &\Leftrightarrow g(u) \in \mathrm{Im}(gfg^{-1} - \mathrm{id}_E) \\ &\Leftrightarrow \exists w \in E \mid g(u) = gfg^{-1}(w) - w \\ &\Leftrightarrow \exists w \in E \mid u = fg^{-1}(w) - g^{-1}(w) \quad \text{en posant } z = g^{-1}(w), \\ &\Leftrightarrow \exists z \in E \mid u = f(z) - z \\ &\Leftrightarrow u \in \mathrm{Im}(f - \mathrm{id}_E) = D \\ &\Leftrightarrow v \in g(D). \end{aligned}$$

Et bien sûr $D \subset H$ implique $f(D) \subset f(H)$, ce qui conclut la preuve. □

3.I.A.iii. Générateurs de $\mathrm{GL}(E)$ *et* $\mathrm{SL}(E)$. —

Théorème 3.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:

$$L_i(A') = L_i(A) + \lambda L_j(A),$$
$$C_j(A'') = C_j(A) + \lambda C_i(A).$$

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 $(1, 0, \ldots, 0)^t$.

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). □

3.I.B. Groupe linéaire sur un corps fini. —

3.I.B.i. Ordre des groupes linéaires. — On note $\mu_n(\mathbb{K})$ l'ensemble des racines n-ièmes de l'unité dans $\mathbb{K}$.

Lemme 3.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 maintenant G un sous groupe de $\mathbb{K}^*$ et soit N l'ordre de G. Notons $\varphi(n)$ l'indicatrice d'Euler d'un entier $n \in \mathbb{N}$, i. e.

$$\varphi(n) = \#\{s \in [\![1, n]\!] \mid \mathrm{pgcd}(s, n) = 1\}.$$

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 :

$$N = \sum_{n|N} \varphi(n).$$

Ainsi, soit $\alpha \in G$. L'ordre n de α divise N et α engendre un 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 ce polynôme, donc H est l'ensemble de ces racines. Par ailleurs, un élément $\beta \in G$ d'ordre n est racine de ce polynôme,

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 3.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 3.I.9. □

3.I.B.ii. Quelques rappels sur les groupes de permutation. — Soit $n \geq 1$ un entier.

Théorème 3.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 $H \simeq \mathfrak{S}_{n-1}$. □

3.I.B.iii. 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 3.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 $\mathrm{PSL}_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$. □

3.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 3.II.1. — *Le groupe* $\mathrm{PSL}_n(\mathbb{K})$ *est simple hormis dans les cas :*

$$\mathrm{PSL}_2(\mathbb{F}_2) \simeq \mathfrak{S}_3, \qquad \mathrm{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4.$$

3.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 3.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 3.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 3.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 3.I.5.

Dans les deux cas nous avons montré qu'il existe une transvection dans N, ce qui implique $N = \mathrm{SL}_n(\mathbb{K})$.

3.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 3.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 $N \notin \mathbb{K}^*\mathbb{1}_2$. Alors $N = \mathrm{SL}_2(\mathbb{K})$.*

Démonstration. — Soit $f \in N \setminus \mathbb{K}^*\mathbb{1}_2$, 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 3.II.1. En effet, le cas $n \geq 3$ étant montré, nous regardons le cas $n = 2$ où la proposition 3.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 3.I.12 montre que $\mathrm{PSL}_2(\mathbb{F}_5)$ est simple grâce au théorème 3.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 4

QUADRIQUES

Dans ce chapitre, $\mathbb{K}$ désigne un corps de caractéristique différente de 2.

4.I. Quadriques projectives

4.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.

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.

Définition 4.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 $X = (x_1, \dots, x_n) \in \mathbb{K}^n$, et $Y = (y_1, \dots, y_n) \in \mathbb{K}^n$ 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 4.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 $A^\perp = \{u \in E \mid \Phi_q(v, u) = 0, \forall v \in A\}$.

Proposition 4.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 $\mathbb{K} = \mathbb{F}_q$, $\lambda \in \mathbb{F}_q \setminus \mathbb{F}_q^{(2)}$ 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 $u = x_1 e_1 + \cdots + x_n e_n$, 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:

$$q(u) = q(x_1 e_1 + \cdots + x_n e_n) = \sum_{i=1}^{n} a_i \alpha_i(u)^2.$$

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 orthgonaux 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 instersecter 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.

□

4.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.

4.I.B.i. 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 4.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 4.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 4.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.

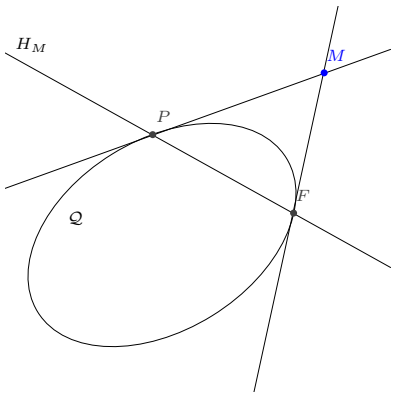


FIGURE 1. Polarité pour une conique

Démonstration. — Soit $[v] \in \mathbb{P}(E)$ et $[u] \in \mathcal{Q}$. On trouve :

$$\begin{aligned}[v] \in T_{[u]}\mathcal{Q} &\Leftrightarrow \Phi_q(v,u) = 0 \\ &\Leftrightarrow u \in \mathrm{Ker}(\Psi_q(v)) \\ &\Leftrightarrow [u] \in H_{[v]}.\end{aligned}$$

□

4.I.B.ii. 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 4.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 4.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 4.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 4.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 $x_1^2 + x_1^2 - x_0^2$. □

4.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 $\mathbb{K}$.

4.II.A. Quadriques affines et polynômes. —

Définition 4.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 4.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.

4.II.B. Quadriques à centre. —

Définition 4.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 4.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 4.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, $f(\varphi(P)) = f(O - \overrightarrow{OP}) = q(-\overrightarrow{OP}) + c = q(\overrightarrow{OP}) + c = f(P)$.

4.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 4.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 4.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 $\hat{q}$:

$$f(P) = f(x_0 e_0 + \cdots + e_n e_n) = p(x_1, \dots, x_n) + x_0\ell(x_1, \dots, x_n) + cx_0^2,$$

un polynôme homogène de degré 2 en $(x_0, \dots, x_n)$.

4.II.D. Coniques affines. —

4.II.D.i. 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 4.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 4.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:*

$$\mathbb{V}\left(ax_1^2 + bx_2\right), \qquad \textit{une parabole.}$$

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. □

4.II.D.ii. 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 4.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 cartésient $(O, \vec{e_1}, \vec{e_2})$ tel que $\mathcal{Q}$ soit l'ensemble des points $P = O + x_1\vec{e_1} + x_2\vec{e_2}$ tels que:*

$$x_1^2 + x_2^2 = 1, \qquad \textit{si } \hat{\mathcal{Q}} \cap H = \varnothing, \textit{ donc } \mathcal{Q} \textit{ est une ellipse,}$$
$$x_1^2 - x_2^2 = 1, \qquad \textit{si } \#\left(\hat{\mathcal{Q}} \cap H\right) = 2, \textit{ donc } \mathcal{Q} \textit{ est une hyperbole,}$$
$$x_1^2 - x_2 = 0, \qquad \textit{si } \#\left(\hat{\mathcal{Q}} \cap H\right) = 1, \textit{ donc } \mathcal{Q} \textit{ est une parabole.}$$

Si $\mathcal{Q}$ est une ellipste, il existe un repère où l'équation de $\mathcal{Q}$ prend la forme $x_1x_2 - 1$.

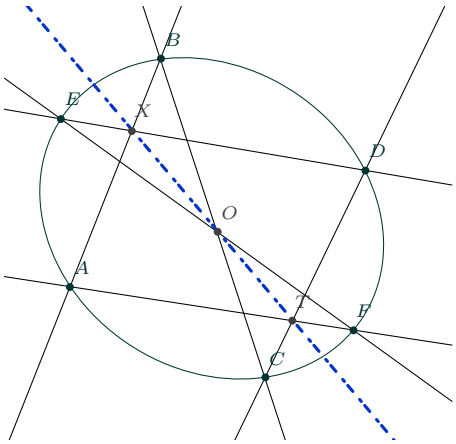
****

4.II.D.iii. 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 4.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'ensembles 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 4.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
T
F
C

CHAPITRE 5

GROUPE ORTHOGONAL

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.

5.I. Automorphismes orthogonaux, réflexions, générateurs

5.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 5.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 $q|_F = 0$.

Remarque 5.I.2. — On a F non nul 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 5.I.3. — Soit q une forme quadratique sur E. On dit que q est anisotrope si E n'admet pas d'espace vectoriel non nul isotrope.

Définition 5.I.4. — On note $\mathrm{O}(q)$ l'ensemble des automorphismes orthogonaux de E, 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 :

$$\Phi_q(u, v) = \Phi_q(f(u), f(v)).$$

5.I.B. Symétries, réfléxions. —

Définition 5.I.5. — 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 réfléxion orthogonale si H est un hyperplan. On parle de renversement si H a codimension 2.

Lemme 5.I.6. — *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 réfléxion ou un produit de deux réfléxions. Si q est anisotrope et $u \neq v$, la réfléxion 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 réfléxion 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 :

$$\tau_{H_2}\tau_{H_1}(u) = v.$$

□

5.I.C. Générateurs. —

Théorème 5.I.7. — *Le groupe* $\mathrm{O}(q)$ *est engendré par des réfléxions. Si* q *est anisotrope, tout élément* f *de* $\mathrm{O}(q)$ *s'écrit comme produit de* m *réfléxions, où l'on peut choisir* $m \leq \dim(\mathrm{Fix}(f)^\perp) \leq n$.

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 réfléxion et le résultat est vrai. Sinon $f = -\mathrm{id}_E$, et la réfléxion 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 réfléxions.

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 5.I.6, il existe donc $g \in \mathrm{O}(q)$ qui est une réfléxion ou un produit de deux réfléxions, 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 réfléxions orthogonales $\tau_1, \ldots, \tau_m$ de F telles que $h|_F = \tau_1 \circ \cdots \circ \tau_m$. Nous avons donc $\tilde{\tau}_1, \ldots, \tilde{\tau}_m$ réfléxions de E obtenues par linéarité en définissant pour tout $i \in [\![1, m]\!]$:

$$\begin{aligned} &\tilde{\tau}_i(v) = \tau_i(v), && \text{pour tout } v \in F; \\ &\tilde{\tau}_i(u) = u. \end{aligned}$$

Il s'agit bien sûr de réflexions, et $h = \tilde{\tau}_1 \circ \cdots \circ \tilde{\tau}_m$, car ceci est vrai sur F et sur u, donc sur une base de E, donc sur E. Finalement:

$$f = g^{-1} \circ h = g^{-1} \circ \tilde{\tau}_1 \circ \cdots \circ \tilde{\tau}_m,$$

ce qui donne le résultat. En effet, g étant produit de réfléxions, g^{-1} est aussi un produit de réfléxions 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 réfléxion.

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 5.I.6, il la réfléxion $g = \tau_H$, 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 :

$$\Phi_q(w, u - v) = \Phi_q(w, u) - \Phi_q(w, v) = \\ = \Phi_q(w, u) - \Phi_q(f(w), f(u)) = \Phi_q(w, u) - \Phi_q(w, u) = 0.$$

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 $u \in \mathrm{Fix}(h) \smallsetminus \mathrm{Fix}(f)$. 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 $\tau_1, \dots, \tau_m$ réfléxions de E telles que $h = \tau_1 \circ \cdots \circ \tau_m$ avec $m \leq n_0 - 1$. Donc $f = g^{-1} \circ \tau_1 \circ \cdots \circ \tau_m$. Ainsi f s'éxprime comme produit d'un nombre $m + 1$ de réfléxions, où $m + 1 \leq n_0 - 1 + 1 = n_0$. □

5.I.D. Groupe orthogonal positif, renversements. —

Proposition 5.I.8. — *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 réfléxions.

Si $n = 3$ et τ est une réfléxion, alors $-\tau$ est un renversement. En effet, si H est un hyperplan $-\tau_H = \tau_{H^\perp}$ 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 τ_{H_1} et τ_{H_2} deux réfléxions 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 τ_{H_1} et τ_{H_2} à F coïncident avec id_F, tandis que leurs restrictions à $F^\perp$ sont des réfléxions.

D'après ce que nous avons vu pour la dimension 3, on a deux renversements σ_1 et σ_2 de F tels que $\tau_{H_1}\tau_{H_2}|_F = \sigma_1\sigma_2$. On définit des extensions $\tilde{\sigma}_1$ et $\tilde{\sigma}_2$ de σ_1 et σ_2 à E en posant, pour $i \in [\![1, 2]\!]$:

$$\tilde{\sigma}_i(v) = \sigma_i(v), \qquad \text{pour tout } v \in F^\perp;$$
$$\tilde{\sigma}_i(v) = v, \qquad \text{pour tout } v \in F.$$

On a $\sigma_1\sigma_2 = \tau_{H_1}\tau_{H_2}$, car ceci est vrai sur F et sur $F^\perp$ et $E = F \oplus F^\perp$. De plus, $\tilde{\sigma}_1$ et $\tilde{\sigma}_2$ sont des renversements.

Maintenant le résultat est clair : nous écrivons $f \in \mathrm{SO}(q)$ comme produit d'un nombre pair de réfléxions, chaque couple de réfléxions pouvant s'écrire comme produit de deux renversements, f s'écrit comme produit (d'un nombre pair) de renversements. □

5.II. Groupe euclidien

5.II.A. Simplicité de $\mathrm{SO}(3,\mathbb{R})$. — A rédiger.

5.II.B. Simplicité de $\mathrm{SO}(n,\mathbb{R})$. —

Lemme 5.II.1. — *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 5.II.2. — *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 5.II.1.

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 $H = \mathrm{SO}(E, q)$. □

5.III. Groupe orthogonal général

5.III.A. Plans hyperboliques. —

Définition 5.III.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 5.III.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 5.III.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 5.III.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 $a_1a_2 = -\varepsilon^2$ 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 :

$$q(x_1u_1 + x_2u_2) = a_1(x_1^2 - \varepsilon_0^2x_2^2) = a_1(x_1 + \varepsilon_0x_2)(x_1 - \varepsilon_0x_2),$$

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. □

5.III.B. Espaces hyperboliques. — Un espace hyperbolique est une somme directe orthogonale de plans hyperboliques.

Proposition 5.III.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 5.III.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 5.III.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 5.III.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 $\dim(F) = r$, $\dim(H) = 2r$. □

5.III.C. Théorème de Witt. — Soit q forme quadratique non dégénérée sur E.

Théorème 5.III.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 5.III.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 5.III.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 5.III.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 5.I.6 qu'il existe un automorphisme orthogonal f, plus précisément une réfléxion ou un produit de deux réfléxions, 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 5.III.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 5.III.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 Will, 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.