Université de Paris VI
D. Bertrand

Master M1 2009-2010
Algèbre géométrique

CHAPITRE III

GÉOMÉTRIE QUADRATIQUE

Dans tout ce chapitre, K est un corps commutatif de caractéristique $\neq 2$, et les K-espaces vectoriels sont de dimension finie. On suppose parfois K muni d'une involution $\sigma \neq id_K$. Alors, $K = K_0 \oplus K_0\omega$, où $\sigma(\omega) = -\omega$ et $K_0 = \{\lambda \in K, \sigma(\lambda) = \lambda\}$. Exemples : $K = \mathbb{C}, \sigma =$ la conjugaison complexe, $K_0 = \mathbb{R}$; ou $K = \mathbb{F}_5[T]/(T^2-2) := \mathbb{F}_{25}, \sigma(\lambda) = \lambda^5, \omega =$ classe de T, $K_0 = \mathbb{F}_5$.

1 Formes bilinéaires.

1.1 Vocabulaire

Soient E, E' deux espaces vectoriels sur K. Une application $b : E \times E \to E'$ est dite bilinéaire (resp. sesquilinéaire) si pour tout $y \in E$, l'application $x \mapsto b(x,y)$ est linéaire et pour tout $x \in E$, l'application $y \mapsto b(x,y)$ est linéaire (resp. σ-linéaire: $\forall \lambda \in K, b(x, \lambda y) = \sigma(\lambda) b(x,y)$). Lorsque $E' = K$, on parle de forme bi- resp. sesqui-linéaire.

Soient b une forme sesquilinéaire, et $\mathcal{B} = \{e_1, ..., e_n\}, n = dimE$, une base de E, dans laquelle x, y sont représentés par des vecteurs colonnes $X = {}^t(x_1, ..., x_n), Y$. Alors, $b(x,y) = {}^tXB\sigma(Y) \in K$, où $B = (b_{i,j} = b(e_i, e_j), 1 \leq i,j \leq n)$ est la matrice représentative de b dans la base $\mathcal{B}$. Si $\mathcal{B}' = (e_1, ..., e_n).P, P \in GL_n(K)$, désigne une autre base, b est représentée dans $\mathcal{B}'$ par la matrice $B' = {}^tPB\sigma(P)$. Idem (sans les σ) pour une forme bilinéaire : dans ce cas, on a $det(B') = det(B)(det(P))^2$, et la classe de $det(B)$ dans $K/(K^*)^2$ ne dépend pas de la base choisie; on l'appelle le *discriminant* $discr(b)$ de la forme bilinéaire b.

Une forme bilinéaire b fournit deux applications linéaires naturelles de E vers son dual E^* :

$$\phi_b : E \to E^* : x \mapsto \{\phi_b(x) : y \mapsto b(x,y)\},$$

et $\phi_b^t : x \mapsto \{\phi_b^t(x) : y \mapsto b(y,x)\}$, qui est la transposée de ϕ_b. Elles sont données, relativement à la base $\mathcal{B}$ et à sa base duale $\mathcal{B}^* = (e_1^*, ..., e_n^*)$, par les matrices ${}^tB$ et B. Ces applications (ou matrices) ont le même rang, qu'on appelle *le rang de b*. On dit que *la forme b est non dégénérée si* $rang(b) = n$, c-à-d. si $det(B) \neq 0$, c-à-d. si ϕ_b (ou, de façon équivalente, ϕ_b^t) est un isomorphisme[1]. Les noyaux de ϕ_b et de ϕ_b^t ont même dimension, égale à $n - rang(b)$. Sous les hypothèses qu'on va maintenant faire sur b, ils coïncident, et s'appellent alors *le noyau de b*.

On suppose désormais que l'une des conditions suivantes est satisfaite :

- b est *bilinéaire symétrique*[2] : $\forall x, y \in E, b(x,y) = b(y,x)$, c-à-d.: $\phi_b = \phi_b^t$;
- b est *bilinéaire antisymétrique* : $\forall x, y, b(x,y) = -b(y,x)$, c-à-d.: $\phi_b = -\phi_b^t$;
- b est *hermitienne* : b sesquilin. et $\forall x, y, b(x,y) = \sigma(b(y,x))$: $\phi_b = \sigma \circ \phi_b^t$.

ce qui, en termes matriciels, se traduit par ${}^tB = B$ (matrice symétrique), ${}^tB = -B$ (matrice antisymétrique) ou ${}^tB = \sigma(B)$ (matrice hermitienne).

Dans ces conditions, on dit que deux parties X, Y de E sont*orthogonales* relativement à b, notation : $X \perp Y$, si $\forall x \in X, y \in Y, b(x,y) = 0$. Alors $Y \perp X$. L'orthogonal $E^\perp$ de E est le noyau $Ker(\phi_b) = Ker(\phi_b^t)$ de b. On a donc $dim E^\perp + rang(b) = dim E$, et b est non dégénérée si et slt si $E^\perp = \{0\}$. Pour toute partie S de E, l'ensemble $S^\perp = \{y \in E, \forall x \in S, x \perp y\}$ est un sous-espace vectoriel de E, qui vérifie $S \subset (S^\perp)^\perp$. Une somme directe directe $E = E_1 \oplus ... \oplus E_k$ est dite orthogonale si $E_i \perp E_j$ pour tout $i \neq j$.

Si b est une forme bilinéaire symétrique ou hermitenne, on appelle *forme quadratique* ou quadratique hermitienne associée à b l'application $q = q_b : E \to K : x \mapsto q(x) := b(x,x)$. Les formules $b(x,y) = \frac{1}{4}(q(x+y) - q(x-y))$ (cas bilinéaire symétrique) et $b(x,y) = \frac{1}{4}(q(x+y) - q(x-y)) + \frac{1}{4\omega}(q(\omega x + y) - q(\omega x - y))$ (cas hermitien) permettent de retrouver b à partir de q. On dit que b est la forme polaire de q, et on appelle rang de q celui de b. Dans le cas bilinéaire symétrique, la formule $q(x+h) = q(x) + 2b(x,h) + q(h)$ permet d'interpréter $2b(x,.) = 2\phi_b(x)$ comme la differentielle de q en x.

On dit qu'une forme bilinéaire b est alternée si $\forall x \in E, b(x,x) = 0$. Comme $car K \neq 2$, cela équivaut à dire que b est antisymétrique (tandis que

[1] On pourra donner des énoncé similaires pour b sesquilinéaire, en introduisant le K-espace vectoriel $E^{*,\sigma}$ des formes σ-linéaires sur E. Par ailleurs, tout élément ϕ de $\mathcal{L}(E, E^*)$ fournit deux formes bilinéaires $b_\phi(x,y) = \phi(x)(y), b_{\phi^t}(x,y) = \phi(y)(x)$, et on peut ainsi retrouver b à partir de ϕ_b ou de ϕ_b^t. Quelle est la version sesquilinéaire ?

[2] En anglais : *symmetric*. Mais un seul m en français.

pour $carK = 2$, b est antisymétrique si et slt si elle est symétrique).

Un vecteur non nul $x \in E$ est dit *isotrope* si $q(x) = 0$. La droite qu'il porte est alors formée de vecteurs isotropes. L'ensemble $C(q) = \{x \in E, q(x) = 0\}$ s'appelle le *cône isotrope* de q. Un sous-espace vectoriel F de E est dit *totalement isotrope* si $\forall x, y \in F, b(x, y) = 0$, c-à-d. si $F \perp F$, ou encore $F \subset F^\perp$. Par exemple, $E^\perp$ (ou, plus généralement, dans le cas symétrique ou hermitien, tout sous-espace vectoriel F de E contenu dans $C(q)$) est totalement isotrope. *L'indice* $\nu(b)$ de b (ou : $\nu(q)$ de q dans le cas symétrique ou hermitien) est la dimension maximale des sous-espaces totalement isotropes de E.

Proposition 1.1. *: supposons que b soit* non-dégénérée. *Pour tous sous-espaces vectoriels F, G de E, on a :*
i) $dimF + dimF^\perp = dimE$; en particulier, $\nu(b) \leq \frac{1}{2}dimE$.
ii) $(F^\perp)^\perp = F$
iii) $(F + G)^\perp = F^\perp \cap G^\perp$ et $(F \cap G)^\perp = F^\perp + G^\perp$;
iv) si $F \cap F^\perp = \{0\}$, alors $E = F \perp F^\perp$.

Preuve : Pour i), soient B une matrice représentative de b et $\{f_1, ..., f_k\}$ des vecteurs de K^n représentant une base de F. Alors, $F^\perp$ s'identifie à l'ensemble de solutions $y \in K^n$ du système $\{\sigma({}^tf_i.B).y = 0, i = 1, ..., k\}$. Comme B est inversible, ce système est de rang $k = dimF$. Par conséquent, $codimF^\perp = k$. Les autres énoncés sont des exercices.

Proposition 1.2. *(On ne suppose plus b non dégénérée.) Soit F un sous-espace vectoriel supplémentaire de $E^\perp$ dans E. Alors, $E = F \perp E^\perp$, et la restriction $b_{|F}$ de b à F est non-dégénérée..*

Preuve : la somme directe $E = F \oplus E^\perp$ est orthogonale puisque $E^\perp \perp E$. Dans une base de E respectant cette décomposition, la matrice représentative de b est donnée par $B = \begin{pmatrix} B_1 & 0 \\ 0 & 0 \end{pmatrix}$, où B_1 représente $b_{|F}$. Alors, $rg(b_{|F}) = rg(B_1) = rg(B) = dimE - dimE^\perp = dimF$, donc $b_{|F}$ est non-dégénérée.

1.2 "Diagonalisation"

Soient q, q' deux formes quadratiques (resp. quadratiques hermitiennes) sur E, de formes polaires b, b'. On dit que q et q' sont *équivalentes* s'il existe un automorphisme $u \in GL(E)$ tel que $q' = q \circ u$, ou de façon équivalente: $\forall x, y, b'(x,y) = b(u(x), u(y))$. En termes des matrices représentatives B, B', U de b, b', u dans une base donnée de E, cela revient à demander que $B' = {}^tUBU$ (resp. $B' = {}^tUB\sigma(U)$). On a une notion similaire d'équivalence pour les couples b, b' de formes alternées.

Proposition 1.3. *i) Soit q une forme quadratique (resp. quadratique hermitienne) sur E, de rang r. Il existe des éléments $d_1, ..., d_r$ de K^* (resp. de K_0^*) tels que q est équivalente à la forme $q'(x) = d_1x_1^2 + ... + d_rx_r^2$ (resp. $d_1x_1\sigma(x_1) + ... + d_rx_r\sigma(x_r)$). Autrement dit, E admet une* base orthogonale *(c-à-d. formée de vecteurs deux à deux orthogonaux), et dont les $n - r$ derniers forment une base de $E^\perp$. Ou encore, si $B = {}^tB$ (resp. $\sigma({}^tB)$) désigne une matrice représentative de q, il existe $U \in GL_n(K)$ telle que ${}^tUBU$ (resp. ${}^tUB\sigma(U)$) =* $\begin{pmatrix} d_1 & 0 & 0 \\ 0 & d_r & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

ii) Soit b une forme bilinéaire alternée sur E, de matrice représentative $B = -{}^tB$. Alors, b est equivalente à $b'(x,y) = \Sigma_{i=1,..,m} x_iy_{m+i} - y_ix_{m+i}$. Autrement dit, il existe $U \in GL_n(K)$ telle que ${}^tUBU = \begin{pmatrix} 0 & \mathbf{I}_m & 0 \\ -\mathbf{I}_m & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. *En particulier, le rang $r = 2m$ de b est pair.*

Preuve i) Une preuve algorithmique a été vue en L3. En voici une autre. Le corollaire précédent permet de se ramener au cas où b est non dégénérée. Pour $e_1 \in E$ non isotrope, $E_1 = \{e_1\}^\perp$ est un hyperplan ne contenant pas e_1, donc $E = K.e_1 \perp E_1$, et la restriction de b à E_1 est non dégénérée. On itère.

ii) On se ramène de nouveau au cas non-dégénéré. Il existe alors deux vecteurs e_1, ϵ_1 tels que $b(e_1, \epsilon_1) = 1$. Ils sont forcément linéairement indépendants, et $b(\epsilon_1, e_1) = -1$, de sorte que la restriction de b au plan P_1 qu'ils engendrent, de matrice représentative $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, est non-dégénérée. On en déduit que $P_1 \cap P_1^\perp = \{0\}$, donc $E = P_1 \perp P_1^\perp$, et que la restriction de b à $E_1 = P_1^\perp$ est non-dégénérée. On peut donc itérer.

Remarques : i) Bien que le résulat de (i) soient souvent décrit comme une "diagonalisation" de la forme q, *il ne fournit pas une diagonalisation de la matrice* B, ce qui reviendrait à trouver une matrice $U \in GL_n(K)$ telle que $U^{-1}BU$ soit diagonale; les scalaires d_i de cet énoncé ne sont d'ailleurs pas uniques, et n'ont donc pas de rapport avec les valeurs propres de B. Bref, on prendra garde à ne pas confondre (i) avec le "théorème spectral", en vertu duquel les matrices symétriques réelles (resp. hermitiennes complexes) sont effectivement diagonalisables - et qui plus est, par une matrice $U = {}^tU^{-1}$ orthogonale (resp. $U = \sigma({}^tU^{-1})$ unitaire).

ii) Un *espace symplectique* est un couple (E, b) où b est une forme alternée non dégénérée. Tout plan symplectique est équivalent à l'espace vectoriel K^2, muni de la forme alternée $b(x, y) = x_1y_2 - x_2y_1 = det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$, et le resultat de (ii) exprime que E s'écrit comme une somme directe orthogonale de $E^\perp$ et de plans symplectiques. ll entraîne par ailleurs que tout espace symplectique (E, b) est de dimension $n = 2m$ paire, où $m = \nu(b)$, et admet une décomposition en somme directe (non orthogonale) de deux sous-espaces $W_1 =< e_1, ..., e_m >$, $W_2 =< \epsilon_1, ..., \epsilon_m >$ totalement isotropes de dimension $n/2$. De tels sous-espaces s'appellent des lagrangiens de (E, b), et les bases correspondantes $\{e_1, \epsilon_1, ..., e_m, \epsilon_m\}$ des bases symplectiques.

iii) Ne pas confondre (ii) avec les énoncés suivants. Un *espace hyperbolique* est un couple (E, b), où E est de dimension $n = 2m$ paire, et b est une forme bilinéaire symétrique non dégénéree d'indice $\nu(b) = m$. Tout plan hyperbolique (E, b) est équivalent à l'e-v K^2, muni de la forme bilinéaire de matrice représentative $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (ou de façon équivalente $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$). Tout espace hyperbolique est somme directe orthogonale de plans hyperboliques, et admet donc une décomposition en somme directe (non orthogonale) de deux sous-espaces W_1, W_2 totalement isotropes de dimension $n/2$. De tels sous-espaces s'appellent aussi des lagrangiens de (E, b).

2 Quadriques

Soient $\mathbb{P}(E)$ un espace projectif sur K de dimension n, et $q \neq 0$ une forme quadratique sur E, de forme polaire b. Dans une base de E, q s'exprime comme un polynôme homogène $Q(X_0, ..., X_n) = {}^tXBX$ de degré 2 en $n+1$ variables, et l'ensemble $Z(Q) := \Gamma$ des zéros de Q (au sens de la Note [(3)] du chapitre 2, §2.3) est bien défini. On l'appelle la quadrique définie par q. Ainsi, les points de Γ à coordonnées dans K correspondent exactement aux droites vectorielles du cône isotrope $C(q)$ de q.

Les multiples non nuls $\lambda q, \lambda \in K^*$, de q définissent la même quadrique, de sorte que la donnée de Γ équivaut à celle d'un point de l'espace projectif $\mathbb{P}(\mathcal{Q}(E))$, où $\mathcal{Q}(E)$ désigne le K-espace vectoriel, de dimension $\frac{(n+1)(n+2)}{2}$, formé par les formes quadratiques sur E (on retrouvera cet espace vectoriel sous le nom de code $Sym^2(E^*)$ au chapitre 4). Un changement de base fournit une nouvelle expression $Q'(X_0, ..., X_n)$ de q, où Q et Q' sont des formes quadratiques sur K^{n+1} équivalentes, et on dit que les quadriques correspondantes de $\mathbb{P}_n(K)$ sont équivalentes. Une classe d'équivalence de quadriques de $\mathbb{P}_n(K)$ correspond donc à une "classe d'équivalence projective" de matrices symétriques B , où $B \sim B'$ signifie : $\exists \lambda \in K^*, U \in GL_{n+1}(K), B' = \lambda {}^tUBU$.

Hyperplan tangent et tangentes

Soit $P \in \mathbb{P}(E)$ un point de la quadrique Γ définie par q. En coordonnées, si $P = (\gamma_0 : ... : \gamma_n)$ est représenté par un vecteur $\gamma = (\gamma_0, ..., \gamma_n)$ de E, $Q(\gamma_0, ..., \gamma_n) = 0$. Pour tout $i = 0, ..., n$, les dérivées partielles de Q s'écrivent: $Q'_{X_i}(\gamma_0, ..., \gamma_n) = 2b(\gamma, e_i)$, où $e_i = (0, .., 1_{(i)}, ...0)$. Donc P est lisse sur Γ (au sens du chapitre 2, proposition 2.7) si et seulement si ses représentants γ n'appartiennent pas au noyau de b, et pour un tel point P, l'hyperplan tangent à Γ en P admet pour équation

$$T_P(\Gamma) : b(\gamma, X) = 0.$$

Ainsi, $\mathbb{P}(E^{\perp(b)}) \subset \Gamma$ est l'ensemble des points non lisses (aussi appelés : singuliers) de Γ. On dit que la quadrique Γ est *non-singulière* (ou: *lisse*) si la forme bilinéaire b est non-dégénérée; tous ses points sont alors lisses.

Soient P, P' deux points distincts de $\mathbb{P}(E)$, représentés par des vecteurs γ, γ', et $\Delta = \mathbb{P}(K\gamma \oplus K\gamma') =< P, P' >$ la droite projective qu'ils engendrent. En dehors de P', les points d'intersections de Γ et de Δ correspondent aux solutions en t de l'équation

$$Q(\gamma + t\gamma') := t^2 Q(\gamma') + 2tb(\gamma, \gamma') + Q(\gamma) = 0.$$

Supposons que P soit un point de Γ, et qu'il soit lisse. Alors, $b(\gamma, \gamma') = 0$ si et slt si la droite Δ est contenue dans l'hyperplan tangent $T_P(\Gamma)$; on dit alors que Δ *est tangente à* Γ *en* P. Dans ce cas, ou bien Δ est toute entière contenue dans Γ ($\Leftrightarrow P' \in \Gamma$), ou bien $\Delta \cap \Gamma$ est réduit à P, compté deux fois (car $t = 0$ est alors une racine double de l'équation). Ainsi, si Γ est une quadrique non singulière, une droite Δ de $\mathbb{P}(E)$ non contenue dans Γ rencontre Γ :

- soit en deux points distincts, et elle n'y est alors pas tangente à Γ;

- soit en un seul point, et elle y est alors tangente à Γ;

- soit en aucun point; ce dernier cas ne peut d'ailleurs pas se produire si $K = \mathbb{C}$ (plus généralement si K est algébriquement clos), l'équation précédente ayant forcément une solution si $P' \notin \Gamma$.

Si maintenant P est un point singulier de Γ, alors ou bien Δ est toute entière contenue dans Γ, ou bien elle ne rencontre (deux fois) Γ qu'au point P. En particulier, toute quadrique singulière non réduite à un point contient au moins une droite. Mais la réciproque est fausse : pour $n \geq 3$, toutes les quadriques de $\mathbb{P}_n(\mathbb{C})$ contiennent des droites.

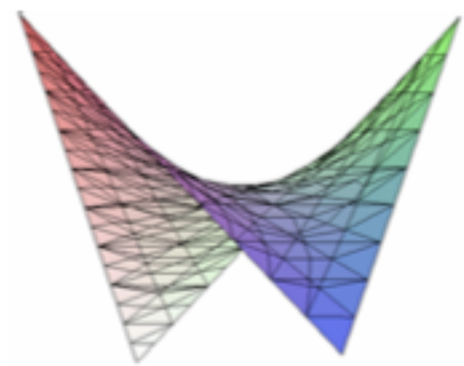
Classification

Décrivons tout d'abord les quadriques de $\mathbb{P}_1(K)$: une forme quadratique $q \neq 0$ en deux variables est projectivement équivalente à $X_0^2 + aX_1^2$, où $a \in K$ représente le discriminant $discr(q) \in K/(K^*)^2$ de q. Si les éléments de K ne sont pas tous des carrés, il y a donc trois classes d'équivalence de quadriques ponctuelles : un point double ($r = 1$), deux points distincts de $\mathbb{P}_1(K)$, ou un couple de points "conjugués" de $K(\sqrt{a})$.

Pour $K = \mathbb{C}$ ou $\mathbb{R}$, la proposition 1.3 fournit la classification suivante des quadriques projectives de $\mathbb{P}_n(K), n \geq 2$:

i) si $K = \mathbb{C}$ (ou plus généralement, si K est algébriquement clos) : la forme quadratique q est (projectivement ou pas) équivalente à $X_0^2 + ... + X_{r-1}^2$, où r est le rang de q. Les classes d'équivalence de quadriques sont donc en bijection avec les entiers $r \in [1, n+1]$. Comme $X_i^2 + X_j^2 = (X_i + \sqrt{-1}X_j)(X_i - \sqrt{-1}X_j)$, toute quadrique lisse de $\mathbb{P}_3(K)$ admet aussi pour équation $X_0X_1 - X_2X_3 = 0$, et contient donc les familles de droites Δ_λ : $X_0 - \lambda X_2 = \lambda X_1 - X_3 = 0; \Delta_\mu : X_0 - \mu X_4 = \mu X_1 - X_2 = 0$. Ces droites correspondent à des couples de lagrangiens de la forme quadratique q.

ii) si $K = \mathbb{R}$: la forme quadratique q est équivalente à $\Sigma_{i=0,..,s-1} X_i^2 - \Sigma_{i=s,...,s+t-1} X_i^2$, où $s + t = r$ est le rang de q. Le couple (s, t) ne dépend que de la classe d'équivalence de q (Sylvester), et s'appelle la *signature* de q. Les classes d'équivalence de quadriques sont donc en bijection avec les couples non ordonnés $\{s, t\}$. L'indice $\nu(q)$ d'une forme quadratique non dégénérée q est égal à $min(s, t)$. Ainsi, la condition $\{s, t\} \neq \{0, n+1\}$ suffit à assurer que les quadriques associées ont des points réels. La quadrique de $\mathbb{P}_3(\mathbb{R})$ de signature $(2, 2)$, qui admet pour équation $X_0X_1 - X_2X_3 = 0$, contient comme supra deux familles de droites (réelles); on l'appelle paraboloïde hyperbolique.



Signalons que si K est un corps fini, on démontre qu'une forme quadratique q de rang r est équivalente à $X_0^2 + ... + X_{r-2}^2 + aX_{r-1}^2$ où $a \in K^*$, et que toute quadrique de $\mathbb{P}_n(K), n \geq 2$, admet des points à coordonnées dans K.

Les quadriques de $\mathbb{P}_2(K)$ s'appellent des *coniques*. Pour $K = \mathbb{C}$, il y a trois types de coniques : une droite double ($r = 1, X_0^2 = 0$), la réunion de deux droites ($r = 2, X_0X_1 = 0$), une conique non singulière ($r = 3$). Pour $K = \mathbb{R}$, le cas $r = 2$ donne naissance à deux types : la réunion de deux droites réelles ($X_0X_1 = 0$), ou de deux droites complexes conjuguées ($X_0^2 + X_1^2 = 0$); le cas $r = 3$ à deux types, suivant que la conique admet des points réels ($X_0^2 + X_1^2 - X_2^2 = 0$) ou pas ($X_0^2 + X_1^2 + X_2^2 = 0$).

Remarque : on dit parfois que la quadrique Γ est impropre si elle contient un hyperplan $\mathbf{H} = \mathbb{P}(KerL)$, où $0 \neq L \in E^*$. Cela équivaut à dire que Q est divisible par L dans $K[X_0, ...X_n]$, soit $Q = LL'$, et Γ est alors la réunion de deux hyperplans $\mathbf{H}, \mathbf{H'}$ distincts, ou l'hyperplan $\mathbf{H}$ compté deux fois. Une telle quadrique n'est pas lisse (tous les points de $\mathbf{H} \cap \mathbf{H'}$ sont singuliers), mais pas inversement : par exemple, la quadrique de $\mathbb{P}_3(K)$ d'équation $X_0^2 + X_1^2 - X_2^2 = 0$ n'est pas lisse, mais ne contient pas de plan. En revanche, comme on vient de le voir, une conique Γ de $\mathbb{P}_2(\mathbb{C})$ est propre (au sens : Γ n'est pas une droite double ou la reunion de deux droites) si et slt si elle est lisse (au sens : la forme quadratique q est non dégénérée).

Retour à la géométrie

Soit Γ une conique propre de $\mathbb{P}_2(K)$ admettant un point M défini sur K, et soit $\mathcal{F}_M$ le faisceau de droites de centre M. Rappelons que $\mathcal{F}_M$ s'identifie par dualité à une droite $M^* \simeq \mathbb{P}_1(K)$ de l'espace projectif dual. D'après le §2.1, l'application de $\mathcal{F}_M$ dans Γ qui, à une droite Δ de $\mathcal{F}_M$ associe le point $P = \Gamma \cap \Delta$ (avec $P = M$ si D est la tangente à Γ en P) établit une bijection ϕ_M de M^* sur l'ensemble des points de Γ définis sur K. En d'autres termes, ϕ_M fournit un *paramétrage* de Γ, dont la preuve qui suit donne une expression explicite dans un choix convenable de coordonnées.

En convenant de remplacer la droite (MP_i) par la tangente $T_{P_i}(\Gamma)$ si $M = P_i$, on a :

Proposition 2.1. ("Chasles-Steiner") *soient* Γ *une conique propre du plan projectif* $\mathbb{P}_2(K)$*, et* $P_1, ..., P_4$ *quatre points distincts de* Γ*. Pour tout point* M *de* Γ*, le birapport des quatre droites* MP_1, MP_2, MP_3, MP_4 *ne dépend pas de* M*. On l'appelle birapport* $[P_1, P_2, P_3, P_4]_\Gamma$ *des quatre points sur la conique.*

Preuve : soit $M' \neq M$ un autre point de Γ, et $\phi_{M'}$ le paramétrage de Γ correspondant. Nous allons montrer que $\phi_{M'}^{-1} \circ \phi_M : M^* \to M'^*$ est une homographie. Par ailleurs (exercice), le birapport de 4 droites d'un faisceau est égal à celui de leurs images par la dualité δ_1. Comme les homographies préservent le birapport, le théorème sera établi.

Choisissons comme repère projectif du plan les points $M = (0 : 1 : 0)$, $M' = (1 : 0 : 0)$, un troisième point $N' = (1 : 1 : 1)$ de Γ, et le point d'intersection $N = (0 : 0 : 1)$ des tangentes à Γ en M et M', et déterminons l'équation $a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + 2b_0X_1X_2 + 2b_1X_0X_2 + 2b_2X_0X_1 = 0$ de Γ dans ce repère. La tangente $(MN) = \{X_0 = 0\}$ à Γ en M a pour équation: $a_1X_1 + b_2X_0 + b_0X_2 = 0$, donc $a_1 = b_0 = 0$. En considérant la tangente $(M'N) = \{X_1 = 0\}$, on voit de même que $a_0 = b_1 = 0$. De $N' \in \Gamma$, on déduit alors que l'équation de Γ est $X_0X_1 - X_2^2 = 0$.

Dans ce repère, une droite Δ du faisceau $\mathcal{F}_M$ a pour équation $\lambda X_0 + \mu X_2 = 0$, correspondant au point $(\lambda : \mu)$ de $\mathbb{P}_1(K) \simeq M^*$, et rencontre Γ aux points $M = (0 : 1 : 0)$ et $P = (\mu^2 : \lambda^2 : -\lambda\mu)$. Ainsi,

$$\phi_M\big((\lambda : \mu)\big) = (\mu^2 : \lambda^2 : -\lambda\mu),$$

ou en coordonnées affines, avec $t = -\frac{\mu}{\lambda}$: $\phi_M(t) = (t^2 : 1 : t)$. On trouve de même, en repérant les droites de $\mathcal{F}_{M'}$ par les équations $X_1 - t'X_2 = 0$, que $\phi_{M'}(t') = (1 : t'^2 : t')$, d'où $\phi_{M'}^{-1} \circ \phi_M(t) = 1/t$. Ainsi, $\phi_{M'}^{-1} \circ \phi_M$ est bien une homographie.

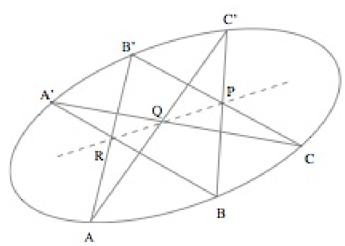
Nous sommes maintenant en mesure d'établir l'un des énoncés du chapitre II, p. 22 :

Exercice : Justifier, puis traduire, le texte suivant (cours de H. Umemura, Nagoya):

Pascal の定理. 射影平面 $P_2(R)$ 内の非特異円錐曲線 Γ 上の相異なる 6 点 A, B, C, A', B', C' を考える. 3 点 P, Q, R を次のように定める:

$$P = (BC') \cap (B'C), \quad Q = (CA') \cap (C'A), \quad R = (AB') \cap (A'B).$$

このとき、3 点 P, Q, R は同一直線上にある.



Indication: supposer par l'absurde que le point $P' = (RQ) \cap (B'C)$ soit différent de P. Posant $x = (AB') \cap (A'C), y = (AC') \cap (B'C)$, vérifier que

$$[A, R, x, B'] = [A'A, A'B, A'C, A'B'] = [C'A, C'B, C'C, C'B'] = [y, P, C, B'].$$

Puis considérer la perspective de centre Q de $(B'A)$ sur $(B'C)$, qui envoie A sur y, R sur P', x sur C et B' sur B'. En déduire que

$$[A, R, x, B'] = [y, P', C, B'],$$

et conclure.

Polarité.

Dans ce paragraphe, on fixe une forme quadratique non dégénérée q sur l'espace vectoriel E, de forme polaire b. Soient Γ la quadrique lisse correspondante, $\phi_b : E \to E^*$ l'isomorphisme de E vers son dual associé à b, et $\phi := \mathbb{P}(\phi_b) : \mathbb{P}(E) \to \mathbb{P}(E^*)$ la transformation projective que définit ϕ_b. Pour tout point M de $\mathbb{P}(E)$, le point $\phi(M)$ de $\mathbb{P}(E^*)$ fournit par dualité un hyperplan de E, qu'on appelle l'hyperplan *polaire* de M par rapport à Γ, et qu'on note $M^{\perp_\Gamma}$, ou plus simplement $M^\perp$. Si $M = \mathbb{P}(K.\gamma)$, où $\gamma \in E$, on a

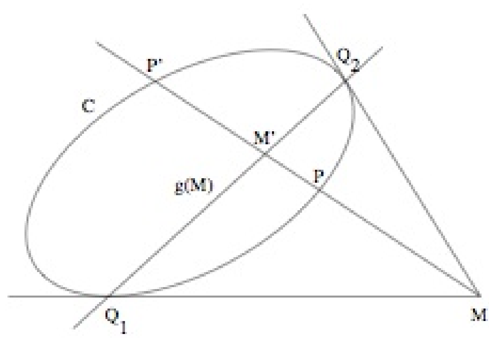
$$M^\perp = \{P' = \mathbb{P}(K.\gamma') \in \mathbb{P}(E), b(\gamma, \gamma') = 0.\}$$

Autrement dit, $M^\perp = \mathbb{P}((K.\gamma)^{\perp_b})$. De même, pour tout hyperplan $\mathbf{H} = \mathbb{P}(H)$ de $\mathbb{P}(E)$ (c'est-à -dire pour tout point de $\mathbb{P}(E^*)$), l'orthogonal $H^\perp$ de H dans E relativement à b est une droite de E, qui définit un point $\mathbf{H}^\perp = \mathbb{P}(H^\perp)$ de $\mathbb{P}(E)$, qu'on appelle le *pôle* de H par rapport à Γ. On a $(M^\perp)^\perp = M, (\mathbf{H}^\perp)^\perp = \mathbf{H}$.

Si $M \in \Gamma$, son hyperplan polaire, d'équation $b(\gamma, X) = 0$, est l'hyperplan tangent à Γ en M (et le pôle de $T_M(\Gamma)$ est le point M). Par conséquent, l'ensemble des hyperplans de $\mathbb{P}(E)$ tangents à Γ est l'image Γ^* de Γ dans $\mathbb{P}(E^*)$ par la transformation projective $\phi = \mathbb{P}(\phi_b)$. C'est donc une quadrique Γ^*, appelée *quadrique duale* de Γ, et l'on a $(\Gamma^*)^* = \Gamma$.

Proposition 2.2. *i) Si dim*$(E) = 2$, *et si* $\Gamma = \{P, P'\}$, *deux points* $M \notin \Gamma$ *et* M' *de la droite* $\mathbb{P}(E)$ *sont pôles l'un de l'autre par rapport à* Γ *si et seulement si* $[P, P', M, M'] = -1$.

ii) Si dim$(E) = 3$, *la droite polaire* $M^\perp = g(M)$ *d'un point* $M \notin \Gamma$ *du plan* $\mathbb{P}(E)$ *par rapport à la conique* Γ *est donnée par la construction de la figure ci-dessous, et l'on a :* $[P, P', M, M'] = -1$.



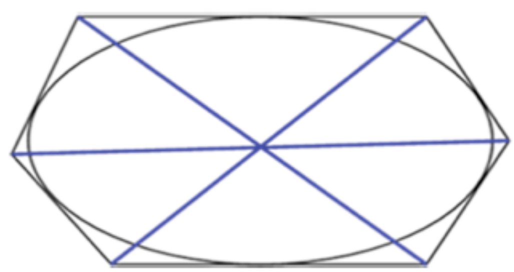
Preuve : i) Par hypothèse, Γ contient deux points, donc q est équivalente à X_0X_1 et on peut supposer que $P = (1 : 0) = \infty, P' = (0 : 1) = 0$ sur $\mathbb{P}_1(K) \simeq K \cup \infty$. Alors, les points $M = (x_0 : x_1) = (x : 1)$ et $M' = (y_0 :$

$y_1) = (y : 1)$ sont en polarité si et seulement si $x_0y_1 + x_1y_0 = 0$, soit $x + y = 0$, autrement dit ssi P' est le milieu du segment $[MM']$ de la droite affine K, soit $[M, M', P', P] = -1 = [M, M', P, P']$.

ii) Vérifions tout d'abord que le faisceau $\mathcal{F}_M$ des droites passant par M possède bien deux tangentes à Γ (tout au moins si K est algébriquement clos) . Ce faisceau donne par dualité une droite Δ^* de $\mathbb{P}(E^*)$, et les tangentes recherchées sont par définition les points d'intersection de la droite Δ^* avec la conique duale Γ^*. Comme $(\Gamma^*)^* = \Gamma$, Δ^* est tangente à Γ^* si et slt si M appartient à Γ, de sorte que sous l'hypothèse $M \notin \Gamma$ de la proposition, on peut tirer de M deux tangentes distinctes[3] $(MQ_1), (MQ_2)$ à Γ.

Comme dans la preuve du théorème 2.1, choisissons alors comme repère projectif du plan $Q_1 = (0 : 1 : 0), Q_2 = (1 : 0 : 0), M = (0 : 0 : 1)$, et $P = (1 : 1 : 1)$. L'équation de Γ devient $X_0X_1 - X_2^2 = 0$, et la droite $(MP) : \{X_0 - X_1 = 0\}$ coupe $(Q_1Q_2) : \{X_2 = 0\}$ en $M' = (1 : 1 : 0)$ et recoupe Γ en $P' = (1 : 1 : -1)$. Ainsi, (Q_1Q_2) admet bien $(0 : 0 : 1) = M$ pour pôle, donc est la polaire de M, et $[P, P', M, M'] = [1, -1, 0, \infty] = -1$.

Comme la dualité, la polarité préserve les relations d'incidence. En voici une application classique : six points A, B, C, A', B', C' d'une conique lisse Γ admettent pour polaires par rapport à Γ les tangentes a, b, c, a', b', c' à Γ en ces points. Le pôle de $(A'B')$ est le point $a' \cap b'$, le pôle de (BC) est le point $b \cap c$, la diagonale joignant ces points est la polaire du point $(A'B') \cap (BC)$. D'après Pascal, les trois points de ce type sont alignés. Par conséquent, leurs polaires, c-à-d. les trois diagonales de ce type, sont concourantes (théorème de Brianchon, dual du théorème de Pascal).



[3] Si $M = (0 : 0 : 1)$ et si $\{X_0 = 0\}$ n'est pas tangente à Γ, leurs équations sont données par $X_1 = tX_0$, où t est tel que le discriminant de la forme quadratique $q_t(X_0, X_2) := Q(X_0, tX_0, X_2)$ s'annule.

Quadriques affines

Soit $\Gamma = Z(Q)$ une quadrique de $\mathbb{P}_n(K)$ ne contenant pas l'hyperplan $\mathbf{H}_0$ d'équation $X_0 = 0$, c-à-d. telle que X_0 ne divise pas Q dans l'anneau $K[X_0, ..., X_n]$. D'après le chapitre II, p. 21, Γ induit sur l'ouvert affine $\mathcal{H}_0 \simeq K^n$ complémentaire de $\mathbf{H}_0$ une hypersurface $\mathcal{Z}(f)$ d'équation $f(x_1, ..., x_n) = 0$, où $f(\frac{X_1}{X_0}, ..., \frac{X_n}{X_0}) = \frac{1}{X_0^2}Q(X_0, ..., X_n)$ est un polynôme de degré total δ égal à 2 . Plus précisément, la forme quadratique en n variables $\Phi(X_1, ...X_n) = F(0, X_1, ..., X_n)$ coïncide avec la somme des monômes de degré 2 de f, et on dit que $\mathcal{Z}(f)$ est une quadrique de l'espace affine K^n, de forme initiale Φ. On a :

$$f(x_1, ..., x_n) = \Phi(x_1, ..., x_n) + L(x_1, ..., x_n) + c,$$

où L est une forme linéaire en n variables et $c \in K$.

En effectuant des changements de coordonnées affines, ce qui ne change pas le rang ρ de Φ, on peut mettre l'équation de toute quadrique affine $\mathcal{Z}(f)$ de $\mathbb{C}^n$, sous l'une des formes suivantes :

$$\Sigma_{i=1,...,\rho}\ x_i^2 = 0 \quad (1 \leq \rho \leq n)\ ;$$
$$\Sigma_{i=1,...,\rho}\ x_i^2 - 1 = 0 \quad (1 \leq \rho \leq n)\ ;$$
$$\Sigma_{i=1,...,\rho}\ x_i^2 + x_{\rho+1} = 0 \quad (1 \leq \rho \leq n-1).$$

Pour $n = 2$ et $K = \mathbb{R}$, on peut mettre l'équation de toute conique affine réelle $\mathcal{C}$ sous l'une des formes : $x_1^2 = 0; x_1^2 - x_2^2 = 0, x_1^2 + x_2^2 = 0, x_1^2 - 1 = 0, x_1^2 + 1 = 0; x_1^2 + x_2^2 + 1 = 0$, et les classiques $x_1^2 + x_2^2 - 1 = 0$ (ellipse), $x_1^2 - x_2^2 + 1 = 0$ (hyperbole), et $x_1^2 + x_2 = 0$ (parabole).

Inversement, toute quadrique affine $\mathcal{C} = \mathcal{Z}(f)$ donne lieu à une quadrique projective $\Gamma = Z(F)$ par le procédé d'homogénisation décrit au chapitre II. Dans le cas $n = 2$, les paraboles $\mathcal{C}$ sont caractérisées par le fait que la droite à l'infini $\Delta = \{X_0 = 0\}$ est tangente à Γ. Lorsque l'espace affine $\mathbb{R}^2$ est muni de sa métrique usuelle, les cercles $\mathcal{C}$ sont caractérisés par le fait que l'intersection de Γ avec la droite à l'infini est formée des points complexes $P_+ = (0 : i : 1), P_- = (0 : i : 1)$, qu'on appelle les *points cycliques* à l'infini. En appliquant la Proposition 2.2.ii aux points de la droite à l'infini $M = (0 : x_1 : x_2), P = P_+, P' = P_-$ et $M' = M^{\perp_\Gamma} \cap \Delta = (0 : y_1 : y_2)$, on voit que $[P_+, P_-, M, M'] = -1$ si et seulement si $x_1y_1 + x_2y_2 = 0$. Ainsi, deux droites D, D' du plan euclidien sont orthogonales si et seulement si leurs points à l'infini $\infty_D, \infty_{D'}$ forment avec les points cycliques P_+, P_- une division harmonique sur la droite à l'infini Δ :

$$D \perp D' \quad \Leftrightarrow \quad [P_+, P_-, \infty_D, \infty_{D'}] = -1.$$

3 Groupes d'isométries

3.1 Les "groupes classiques"

Soit E un espace vectoriel de dimension n muni d'une forme b vérifiant l'une des trois hypothèses du §1.1, et non dégénérée. On dit qu'une application de E dans E est une *isométrie* si

$$\forall x, y \in E \ , \ b(u(x), u(y)) = b(x, y).$$

Dans les cas symétrique ou hermitien, cela revient à demander que $\forall x \in E, q(u(x)) = q(x)$, où q désigne la forme quadratique ou quadratique hermitienne associée à b.

Proposition 3.1. *Soit u une isométrie de (E, b). Alors, u est un automorphisme K-linéaire de E.*

Preuve : dans le cas symétrique ou hermitien, E admet une base $\{e_1, ..., e_n\}$ orthogonale (cf. Prop. 1.3.i), avec $q(e_i) := d_i \neq 0$ pour tout i puisque b est non dégénérée, et tout $x \in E$ s'écrit $\Sigma_{i=1,\dots,n} x_i e_i$, où $d_i x_i = b(x, e_i)$. Comme u est une isométrie, $\{u(e_1), ..., u(e_n)\}$ forme également une système orthogonal, avec $q(u(e_i)) = q(e_i) \neq 0$, donc (exercice) est une base de E, et $u(x) = \Sigma_{i=1,\dots,n} d_i^{-1} b(u(x), u(e_i)) u(e_i) = \Sigma_i d_i^{-1} b(x, e_i) u(e_i) = \Sigma_i x_i u(e_i)$, ce qui montre que u est bien linéaire. Comme elle applique une base sur une base, c'est de plus un automorphisme.

Dans le cas antisymétrique, choisissons la base symplectique $e_1, \epsilon_1, ..., e_m$, ϵ_m donnée par la proposition 1.3.ii. Son image par u vérifie les mêmes relations d'orthogonalité. On en déduit que c'est aussi une base de E, et pour tout $x \in E$, on a : $u(x) = \Sigma_{i=1,\dots,m} b(u(x), u(\epsilon_i)) u(e_i) - b(u(x), u(e_i)) u(\epsilon_i)$. Le même raisonnement montre que u est linéaire, et que c'est un automorphisme.

Les isométries forment donc un sous-groupe de $GL(E)$, qu'on note $O(q)$ dans le cas bilinéaire symétrique (*groupe orthogonal*), $U(q)$ dans le cas hermitien (*groupe unitaire*), $Sp(b)$ dans le cas bilinéaire antisymétrique (*groupe* *symplectique*), ou simplement $O(E)$ lorsque b est donnée. Pour tout $u \in \mathcal{L}(E,E)$, de transposée ${}^t u \in \mathcal{L}(E^*, E^*)$ (remplacer E^* par $E^{*\sigma}$ dans le cas hermitien), on note $u^* = \phi_b^{-1} \circ {}^t u \circ \phi_b$ *l'adjoint* de u, c-à-d. l'unique endomorphisme de E tel que $b(u^*x, y) = b(x, uy)$ pour tout $x, y \in E$. Alors, u est une isométrie si et slt si $u^*u = id_E$. Lorsque b est le produit scalaire usuel, de matrice représentative $\mathbf{I}_n$ sur K^n, ou la forme symplectique usuelle sur K^{2m}, de matrice $\mathbf{J}_{2m} = \begin{pmatrix} 0 & \mathbf{I}_m \\ -\mathbf{I}_m & 0 \end{pmatrix}$, on désigne ces groupes par

$$O_n(K) = \{P \in GL_n(K), {}^t PP = \mathbf{I}_n\}, U_n(K) = \{P \in GL_n(K), \sigma({}^t P)P = \mathbf{I}_n\},$$

$Sp_{2m}(K) = \{P \in GL_{2m}(K), {}^t P\mathbf{J}_{2m}P = \mathbf{J}_{2m}\}$. Les matrices de $O(n) := O_n(\mathbb{R})$ sont dites orthogonales, celles de $U(n) := U_n(\mathbb{C})$ unitaires. Lorsque $E = \mathbb{R}^n$, et b est de signature $(s, t = n - s)$, on pose $O(E) = O(s,t)$. Par exemple, $O(3,1)$ est le groupe de Lorentz des physiciens.

Soit $SL(E) = \{u \in GL(E), det(u) = 1\}$ (noté $SL_n(K)$ quand $E = K^n$) le groupe spécial linéaire. Son intersection avec chacun de groupes supra en fournit des sous-groupes normaux, notés $SO(q)$ (d'indice 2 dans $O(q)$, car $(det(u))^2 = 1$ pour u orthogonale), $SU(q)$, etc. Le groupe $Sp(b)$ est déjà contenu dans $SL(E)$ (ce n'est pas immédiat, mais pour $m = 1$, on vérifie facilement que $Sp_2(K) = SL_2(K)$.)

Remarque 1 (*algèbres de Lie*) : lorsque $K = \mathbb{R}$ ou $\mathbb{C}$, chacun de ces groupes G est naturellement muni de la topologie induite par celle de l'espace vectoriel $Mat_{n,n}(K)$, et on peut parler de la composante connexe G^+ de $\mathbf{I}_n$ dans G. On verra plus loin que $O(n)^+ = SO(n)$. En revanche, $U(n)$ est connexe. On peut également considérer l'application exponentielle, définie par la série normalement convergente

$$exp : Mat_{n,n}(K) \to GL_n(K) : X \mapsto exp(X) = \Sigma_{n \geq 0} \frac{1}{n!} X^n$$

et associer à G son *algèbre de Lie*

$$Lie(G) := \{X \in Mat_{n,n}(K), \forall t \in \mathbb{R}, exp(tX) \in G\},$$

qui est un $\mathbb{R}$-sous-espace vectoriel de $Mat_{n,n}(K)$, muni de la loi de composition interne $(X,Y) \mapsto [X,Y] := XY - YX \in Lie(G)$. Par exemple,

$Lie(SL_n(K)) = \{X \in Mat_{n,n}(K), tr(X) = 0\}$ (matrices de trace nulle);

$Lie(O(n)) = \{X \in Mat_{n,n}(\mathbb{R}),\ {}^tX + X = 0\}$ (X est antisymétrique);

$Lie(U(n)) = \{X \in Mat_{n,n}(\mathbb{C}),\ {}^tX + \overline{X} = 0\}$ (X est "antihermitienne");

Puisque *exp* est continue, $Lie(G^+) = Lie(G)$. La dimension du $\mathbb{R}$-espace vectoriel $Lie(G)$ s'appelle la *dimension* du groupe G.

Remarque 2 (*quaternions*) : ils fournissent de nouvelles familles de groupes, et des isomorphismes entre certains des groupes précédents, en basse dimension. Le corps (non commutatif) des quaternions de Hamilton est $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$, muni de la loi de multiplication définie par $\mathbb{R}$-bilinéarité à partir des relations $i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j$ (on vérifie qu'elle est bien associative, et que tout élément non nul de $\mathbb{H}$ est inversible). Soit σ l'anti-involution (c-à-d. $\sigma(h_1h_2) = \sigma(h_2)\sigma(h_1)$) de $\mathbb{H}$ définie par $\sigma(x + yi + zj + tk) = x - yi - zj - tk$, de sorte que $q(h) := \sigma(h).h := ||h||^2$ fournit une structure euclidienne à $\mathbb{H} \simeq \mathbb{R}^4$, et soit $U := U_1(\mathbb{H})$ le sous-groupe du groupe multiplicatif $\mathbb{H}^*$ formé par les quaternions de norme 1. On peut voir $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j \simeq \mathbb{C}^2$ comme un $\mathbb{C}$-espace vectoriel de dimension 2, que $||.||$ munit d'une structure hermitienne. Alors, l'application $\rho : U \to GL_2(\mathbb{C})$ qui attache à $u \in U$ l'automorphisme $\mathbb{C}$-linéaire de $\mathbb{H} : h \to \rho(u)(h) := hu^{-1}$ est un homomorphisme de groupes injectif. Comme $||hu|| = ||h||.||u|| = ||h||$ pour tout $h \in \mathbb{H}$, son image est contenue dans le groupe unitaire $U(2)$. En fait, pour $u^{-1} = \alpha + \beta j \in \mathbb{C} \oplus \mathbb{C}j$ de norme $\alpha\overline{\alpha} + \beta\overline{\beta} = 1$, la matrice représentative de $\rho(u)$ dans la base $\{1, j\}$ de $\mathbb{H}$ est donnée par $\begin{pmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ -\beta & \alpha \end{pmatrix}^{-1}$, de sorte que ρ établit un isomorphisme de U sur $U(2)$.

L'espace $\mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ des quaternions purs, muni de $||.||$, s'identifie à l'espace euclidien usuel $\mathbb{R}^3$. Pour tout $u \in U$, l'application $Int(u) : h \mapsto uhu^{-1}$ de $\mathbb{H}$ induit une isométrie de $\mathbb{R}^3$, d'où un homomorphisme de groupe $\pi : U \to SO(3)$, appliquant u sur $\pi(u) = (Int(u))|_{\mathbb{R}^3}$, de noyau $U\cap$ centre de $\mathbb{H}^* = \{\pm 1\}$. La théorie des algèbres de Lie permet de montrer que π est surjective, de sorte que $SO(3) \simeq SU(2)/\{\pm \mathbf{I}_2\}$.

Dans le même ordre d'idée, considérons $\mathbb{H}^n$ comme un espace vectoriel à droite sur $\mathbb{H}$, et soit $GL_n(\mathbb{H})$ le groupe des automorphismes $\mathbb{H}$-linéaires de $\mathbb{H}^n$. Avec l'identification $\mathbb{H}^n = \mathbb{C}^n + j\mathbb{C}^n$, on a $GL_n(\mathbb{H}) = \{P \in GL_{2n}(\mathbb{C}), P\mathbf{J}_{2n} = \mathbf{J}_{2n}\overline{P}\}$. Son sous-groupe $U_n(\mathbb{H}) = U(2n) \cap Sp_{2n}(\mathbb{C})$ coïncide avec à $U \simeq SU(2)$ pour $n = 1$, mais c'est en général un nouveau groupe.

3.2 Géométrie euclidienne

Nous nous restreignons désormais au cas euclidien : $K = \mathbb{R}$, et b est un produit scalaire sur $E \simeq \mathbb{R}^n$, c'est-à-dire une forme bilinéaire symétrique définie positive (= de signature $(n, 0)$). Alors, E admet des bases $\{e_1, ..., e_n\}$ orthonormées (= orthogonales et pour tout i, $q(e_i) = 1$), et on peut sans restreindre la généralité supposer que $q(x) = x_1^2 + ... + x_n^2 := ||x||^2$, ce qui identifie $O(E)$ à $O(n)$. Les éléments de $SO(n) = \big\{u \in O(n), det(u) = 1\big\} = O(n)^+$ s'appellent les *rotations* de E. Le complémentaire de $SO(n)$ dans $O(n)$ est noté $O(n)^-$. Pour n impair, il contient $-\mathbf{I}_n$, de sorte que $O(2m+1) \simeq SO(2m+1) \times \{\pm 1\}$; pour n pair, il contient des éléments d'ordre 2, mais aucun n'est central, donc on a seulement : $O(2m) \simeq SO(2m) \rtimes \{\pm 1\}$.

Dans le cas $n = 2$, le groupe $SO(2) = \{R_\theta = \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}, \theta \in \mathbb{R}/2\pi\mathbb{Z}\}$ est commutatif (et isomorphe à $U(1) = \{z \in \mathbb{C}^*, |z| = 1\}$). Tout élément de $O(2)^-$ est une symétrie orthogonale S_D par rapport à une droite vectorielle D de $\mathbb{R}^2$, et $O(2) = SO(2) \rtimes_\tau \{\pm 1\}$, où -1, représentable par n'importe quelle symétrie $S_D = S_D^{-1}$, agit sur $SO(2)$ par $\tau(-1)(R_\theta) = R_{-\theta}$ (c-à-d. $S_D R_\theta S_D^{-1} = R_{-\theta}$). La composée $S_{D'} \circ S_D$ de deux symétries dont les droites forment un angle $(D, D') \equiv \theta$ mod $(\pi\mathbb{Z})$ est la rotation $R_{2\theta}$.

Soit W un sous-espace vectoriel de E, d'orthogonal $W^\perp$. La relation $E = W \oplus W^\perp$ permet de définir la *projection orthogonale* π_W sur W (c-à-d. parallèlement à $W^\perp$) et de même, la *symétrie orthogonale* σ_W par rapport à W; si W est un hyperplan H, cette symétrie s'appelle la *réflexion* τ_H par rapport à H. Toute symétrie orthogonale σ_W est une isométrie, et vérifie $\sigma_W^2 = id_E$. Inversement :

Lemme 3.2. *i) Pour toute isométrie u d'un espace vectoriel euclidien E, on a : $E = Ker(u - id_E) \perp Im(u - id_E)$*

ii) Pour tout automorphisme u d'ordre 2 d'un espace vectoriel E , on a $E = Ker(u - id_E) \oplus Im(u - id_E)$, et $Im(u - id_E) = Ker(u + id_E)$.

iii) Tout élément u d'ordre 2 de $O(n)$ est une symétrie orthogonale.

Preuve : i) D'une part, $Ker(u - id_E)$ et $Im(u - id_E)$ sont de dimensions complémentaires. D'autre part, pour tout $(x \in Ker(u - id_E), z \in E)$: $b(x, u(z)-z) = b(u^{-1}x, z)-b(x, z) = b(x, z)-b(x, z) = 0$, d'où $Ker(u-id_E) \perp Im(u - id_E)$.

ii) Montrer, plus généralement, que si $P, Q \in K[T]$ sont des polynômes premiers entre eux tels que $P(u)Q(u) = 0$, on a $E = W \oplus W'$, où $W =$

$Ker(P(u)) = Im(Q(u)), W' = Ker(Q(u)) = Im(P(u))$. On pourra partir d'une relation de Bézout : il existe $A, B \in K[T]$ tels que $AP + BQ = 1$.

iii) Posant $W = Ker(u - id_E)$, on voit que $u = \begin{pmatrix} id_W & 0 \\ 0 & -id_{W^\perp} \end{pmatrix} = \sigma_W$.

Proposition 3.3. *Soit u une isométrie sur $E \simeq \mathbb{R}^n$.*

i) Il existe des entiers $a, b, c \geq 0$, avec $a + b + 2c = n$, et une base orthonormée de E, dans laquelle u est représentée par une matrice du type $\begin{pmatrix} \mathbf{I}_a & 0 & 0 & 0 \\ 0 & -\mathbf{I}_b & 0 & 0 \\ 0 & 0 & R_{\theta_1} & 0 \\ 0 & 0 & 0 & R_{\theta_c} \end{pmatrix}$*, où $a + b + 2c = n$, et pour tout i, $\theta_i \notin \pi\mathbb{Z}$.*

ii) Il existe un entier $p \leq n$ et des reflexions $\tau_{H_1}, ..., \tau_{H_p}$, telles que $u = \tau_{H_p} \circ ... \circ \tau_{H_1}$. En particulier :

iii) tout élément de $O(2)^-$ est une reflexion; les points fixes d'un élément $u \neq id_E$ de $SO(3)$ forment une droite, qu'on appelle l'axe de la rotation u; $SO(n)$ est connexe par arcs, donc connexe.

La partie (i) signifie que pour tout $U \in O(n)$, il existe $P \in O(n)$ telle que $P^{-1}UP$ soit une matrice du type indiqué. Ou encore : il existe une décomposition orthogonale $E = V^+ \perp V^- \perp \Pi_1 \perp ... \perp \Pi_c$, en sous espaces stables sous u, tels que $u|V^+ = id, u|V^- = -id$, les Π_i sont des plans , et u y induit des rotations d'angles $\theta_i \not\equiv 0, \pi \bmod 2\pi$.

Preuve i) Par récurrence sur n. Le cas $n = 1$, resp. 2, est trivial, resp. classique. Pour $n \geq 3$, soient $\lambda_1, ..., \lambda_m, m \leq n$ les valeurs propres de u dans $\mathbb{C}$, c'est-à-dire les racines de $det(u - \lambda id_E) = 0$. Si l'une, soit λ_1, est réelle, il lui correspond un vecteur propre $v_1 \in E$, qu'on peut supposer de norme 1 et qui vérifie $q(v_1) = q(u(v_1)) = \lambda^2 q(v_1)$, donc $\lambda = \pm 1$. Comme les isométries préservent la relation d'orthogonalité, l'hyperplan $E_1 := (\mathbb{R}v_1)^\perp$ est alors stable sous u, et on peut appliquer l'hypothèse de récurrence à $u_1 = u_{|E_1}$.

Si en revanche aucune valeur propre n'est réelle, deux au moins, soit λ_1 et $\lambda_2 = \overline{\lambda_1}$, sont complexes conjuguées. Considérons alors le complexifié $E_\mathbb{C}$ de E, sur lequel b s'étend en un produit scalaire hermitien $b_\mathbb{C}$, et notons $u_\mathbb{C}$ l'automorphisme $\mathbb{C}$-linéaire que u induit sur $E_\mathbb{C}$. Il est unitaire, et admet λ_1, λ_2 parmi ses valeurs propres. Donc $|\lambda_1| = |\lambda_2| = 1$, et on peut écrire $\lambda_1 = e^{i\theta_1}, \lambda_2 = e^{-i\theta_1}$, où $\theta_1 \not\equiv 0, \pi$. Les vecteurs propres $v_1, v_2 \in E_\mathbb{C}$ correspondant sont linéairement indépendants sur $\mathbb{C}$ (ils sont même orthogonaux pour $b_\mathbb{C}$, puisque $\lambda_1^{-1} b_\mathbb{C}(v_1, v_2) = b_\mathbb{C}(u_\mathbb{C}^{-1}(v_1), v_2) = b_\mathbb{C}(v_1, u_\mathbb{C}(v_2)) = \overline{\lambda_2} b_\mathbb{C}(v_1, v_2) =$

$\lambda_1 b_{\mathbb{C}}(v_1, v_2)$, tandis que $\lambda_1^{-1} \neq \lambda_1$). De plus, $E_{\mathbb{C}}$ admet une involution σ semilinéaire $(\forall(\lambda, v) \in \mathbb{C} \times E_{\mathbb{C}}, \sigma(\lambda v) = \overline{\lambda} v$), qui vérifie $Ker(\sigma - id_{E_{\mathbb{C}}}) = E$ et qui commute à $u_{\mathbb{C}}$. On peut donc choisir $v_2 = \sigma(v_1)$ comme vecteur propre pour λ_2. Dans ces conditions, le plan $\Pi_{\mathbb{C}}$ engendré par v_1, v_2 dans $E_{\mathbb{C}}$ contient les vecteurs $w_1 = \frac{1}{2}(v_1 + \sigma(v_1)), w_2 = \frac{1}{2i}(v_1 - \sigma(v_1))$, qui appartiennent à E. Ainsi, $\Pi_{\mathbb{C}} \cap E$ est un plan réel Π_1 de E stable sous u. Les valeurs propres de l'isométrie $u^1 := u_{|\Pi_1}$ sont $e^{i\theta_1}, e^{-i\theta_1}$, donc u^1 est la rotation d'angle θ_1 (qui est représentée par R_{θ_1} dans toute base orthonormée de Π_1), et le sous-espace $E_1 = \Pi_1^{\perp}$ de E, de dimension $n-2$, est stable sous u. On peut donc appliquer l'hypothèse de récurrence à $u_1 = u_{|E_1}$.

ii) C'est un corollaire de (i) : chaque R_{θ_i} peut s'écrire comme composée de deux reflexions $\tau_{D_i^+} \circ \tau_{D_i^-}$ du plan Π_i, qui sont induites par les reflexions $\tau_{H_i^{\pm}}$ de E d'hyperplans $H_i^{\pm} = D_i^{\pm} \oplus_{j \neq i} \Pi_j \oplus V^+ \oplus V^-$. Toute droite D de V^- fournit de même une reflexion τ_H relative à l'hyperplan $H = D^{\perp}$ de E. En choisissant b droites de V' orthogonales, on obtient b hyperplans $H_1, ..., H_b$ tels que $u = \tau_{H_1} \circ ... \circ \tau_{H_b} \circ \tau_{H_1^+} \circ \tau_{H_1^-} ... \circ \tau_{H_c^+} \circ \tau_{H_c^-}$, d'où les $p = b + 2c \leq n$ réflexions recherchées.

iii) Les décompositions ci-dessus ne sont pas uniques, mais la parité de b et de p ne dépend que de u, puisque $det(u) = (-1)^b = (-1)^p$. Pour $n = 2$ et $det(u) = -1$, cela impose $p = 1$, et u est une réflexion (en fait, nous avons utilisé cette propriété de $O(2)^-$ au démarrage de la récurrence de (i)). Pour $n = 3$ et $det(u) = 1$, cela impose $p = 2$, $u = \tau_{H_2} \circ \tau_{H_1}$: si $H_1 = H_2$, $u = id_E$ (et $a = 3$); sinon, $a = 1$, donc $Ker(u - id_E)$ est une droite Δ, qui contient, donc coïncide avec la droite $H_1 \cap H_2$, et u est la rotation d'axe Δ, d'angle deux fois l'angle de (H_1, H_2). Enfin, tout élément u de $SO(n)$ admet un $b = 2b'$ pair, pour lequel $-\mathbf{I}_b$ s'écrit comme la matrice à b' blocs diagonaux $\begin{pmatrix} R_\pi & 0 \\ 0 & R_\pi \end{pmatrix}$. Après conjugaison par une matrice de changement de base P, l'application $t \in [0, 1] \mapsto (R_{t\pi}, ..., R_{t\pi}, R_{t\theta_1}, ..., R_{t\theta_c})$ fournit alors un chemin continu reliant $\mathbf{I}_n$ à u dans $SO(n)$. Donc $SO(n)$ est contenu dans la composante connexe $O(n)^+$ de $\mathbf{I}_n$ dans $O(n)$. Puisque cette dernière est contenue dans l'image inverse de 1 par l'application continue $det : O(n) \to \{1, -1\}$, on a bien $SO(n) = O(n)^+$, comme annoncé plus haut.

Espaces affines euclidiens

Un espace affine euclidien $\mathcal{E}$ est un espace affine réel dont l'espace vectoriel directeur est un espace euclidien (E, b). Pour $P, Q \in \mathcal{E}$, on appelle distance de P à Q le nombre $d(P,Q) = (q(\overrightarrow{PQ}))^{\frac{1}{2}}$. Une *isométrie affine* de $\mathcal{E}$ est une application $f : \mathcal{E} \to \mathcal{E}$ qui conserve les distances. Ainsi, les translations $t_{\overrightarrow{v}}, \overrightarrow{v} \in E$ sont des isométries affines. L'énoncé suivant montre que les isométries affines de $\mathcal{E}$ forment un sous-groupe, noté $OA(\mathcal{E})$, du groupe affine $GA(\mathcal{E})$, et que $OA(\mathcal{E}) \simeq E \rtimes_\tau O(E)$, pour l'action naturelle τ de $O(E)$ sur E (voir chapitre I, §3.2).

Proposition 3.4. *Soit f une isométrie affine de $\mathcal{E}$. Alors,*
i) f est un automorphisme affine de $\mathcal{E}$; c-à-d. $f \in GA(\mathcal{E})$. On note $\overrightarrow{f} \in GL(E)$ l'application linéaire correspondante;
ii) Il existe une unique couple $(\overrightarrow{v}, g) \in E \times OA(\mathcal{E})$ vérifiant les 3 propriétés suivantes :
(a) $f = t_{\overrightarrow{v}} \circ g$; donc $\overrightarrow{g} = \overrightarrow{f}$;
(b) $Fix(g) = \{P \in \mathcal{E}, g(P) = P\}$ est non vide; donc c'est un sous-espace affine de $\mathcal{E}$, d'espace vectoriel directeur $Ker(\overrightarrow{f} - id_E)$;
(c) $\overrightarrow{v} \in Ker(\overrightarrow{f} - id_E)$.
De plus, on a alors automatiquement : $t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$.

Preuve : i) Fixons une origine O de $\mathcal{E}$. Alors, $f' = t_{\overrightarrow{f(O)O}} \circ f$ est une isométrie affine de $\mathcal{E}$ qui fixe O. En identifiant le vectorialisé $\mathcal{E}_O$ de $\mathcal{E}$ à E, on peut donc voir f' comme une application de E dans E telle que $f'(\overrightarrow{0}) = \overrightarrow{0}$. Pour tout $\overrightarrow{x} \in E$, on a alors : $q(f'(\overrightarrow{x})) = q(f'(\overrightarrow{x}) - f'(\overrightarrow{0})) = q(\overrightarrow{x})$, et la Proposition 3.1 entraîne que f' est linéaire. Donc $f' \in GA(\mathcal{E})$, et de même pour f.

ii) Montrons tout d'abord que si une décomposition $f = t_{\overrightarrow{v}} \circ g$ vérifie (a) et (b), elle vérifie (c) si et seulement si $t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$. En effet, $g t_{\overrightarrow{v}} g^{-1} = t_{\overrightarrow{g}(\overrightarrow{v})}$ est égal à $t_{\overrightarrow{v}}$ si et slt si $\overrightarrow{v} \in Ker(\overrightarrow{g} - id_E) = Ker(\overrightarrow{f} - id_E)$.

Montrons maintenant qu'une décomposition $f = t_{\overrightarrow{v}} \circ g = g \circ t_{\overrightarrow{v}}$ vérifiant (a), (b), (c) est unique. Soit B un point fixe de g, et $B' = f(B) = B + \overrightarrow{v}$ son image par f. Pour tout $P \in \mathcal{E}$, d'image $P' = f(P)$, on a $\overrightarrow{PP'} = \overrightarrow{BP'} - \overrightarrow{BP} = \overrightarrow{BB'} + (\overrightarrow{f} - id_E)(\overrightarrow{BP}) = \overrightarrow{v} + (\overrightarrow{f} - id_E)(\overrightarrow{BP})$, où $v \in Ker(\overrightarrow{f} - id_E)$. Mais d'après le lemme 3.2.i, une telle décomposition de $\overrightarrow{PP'}$ est unique, donc $\overrightarrow{v}$, et par conséquent $g = f \circ t_{-\overrightarrow{v}}$, sont entièrement déterminés par f.

Construisons enfin une décomposition, en fixant une origine O de $\mathcal{E}$, d'image $O' = f(O)$ sous f. Selon le lemme 3.2.i, $\overrightarrow{OO'} = \overrightarrow{v} + (\overrightarrow{f} - id_E)(\overrightarrow{w}) \in Ker(\overrightarrow{f} - id_E) \oplus Im(\overrightarrow{f} - id_E)$. Soit $B = O - \overrightarrow{w}$, et soit $g \in OA(\mathcal{E})$ l'(unique) isométrie affine fixant B et de partie linéaire $\overrightarrow{g} = \overrightarrow{f}$. Alors f et $t_{\overrightarrow{v}} \circ g$ ont mêmes parties linéaires, et valent au point B

$$f(B) = O' + \overrightarrow{f}(\overrightarrow{OB}) = O + \overrightarrow{OO'} + \overrightarrow{f}(\overrightarrow{OB}) = O + \overrightarrow{v} + (\overrightarrow{f} - id_E)(\overrightarrow{BO}) + \overrightarrow{f}(\overrightarrow{OB})$$

$$= B + \overrightarrow{v} = t_{\overrightarrow{v}} \circ g(B), \text{ donc coïncident sur tout } \mathcal{E}.$$

Parmi les isométries affines f, on distingue en particulier :

- les *déplacements* (resp. antidéplacements), dont la partie linéaire $\overrightarrow{f} \in O(n)^+$ est une rotation vectorielle (resp. $\overrightarrow{f} \in O(n)^-$). Le groupe $OA(n)^+ \simeq E \rtimes_\tau O(n)^+$ des déplacements contient les translations, et est encore connexe.

- les *rotations*, qui sont les déplacements f possédant au moins un point fixe. Si $n = 2$, $f \neq id_{\mathcal{E}}$ est une rotation affine si et slt si $\overrightarrow{f}$ est une rotation vectorielle $\neq id_E$: alors, $Ker(\overrightarrow{f} - id_E) = 0$, et $f \neq id_{\mathcal{E}}$ a un unique point fixe, appelé centre de la rotation.

- les *symétries orthogonales* $\sigma_{\mathcal{W}}$ par rapport à un sous-espace affine $\mathcal{W}$ de $\mathcal{E}$: $\sigma_{\mathcal{W}}$ est la symétrie affine par rapport à $\mathcal{W}$ parallèlement à l'orthogonal $W^\perp$ de la direction W de $\mathcal{W}$. Quand $\mathcal{W} = \mathcal{H}$ est un hyperplan de $\mathcal{E}$, on parle de la *réflexion* $\tau_{\mathcal{H}}$ par rapport à $\mathcal{H}$; c'est un antidéplacement, d'ordre 2 dans le groupe $OA(n)$. Le composé de deux réflexions par rapports à des hyperplans parallèles de direction H est une translation par un vecteur $\overrightarrow{v} \in H^\perp$.

Si $n = 2$ et si f est un antidéplacement, alors $\overrightarrow{f}$ est une réflexion vectorielle (Prop. 3.3.iii) par rapport à la droite $D = Ker(\overrightarrow{f} - id_E)$. Si $Fix(f) \neq \emptyset$, c-à-d. si, dans la décomposition canonique $f = t_{\overrightarrow{v}} \circ g$ donnée par la Prop. 3.4.ii, le vecteur $\overrightarrow{v}$ est nul, f est une réflexion par rapport une droite $\mathcal{D} = Fix(f)$ de direction D. En revanche, si $Fix(f) = \emptyset$, f n'est pas une réflexion, mais une symétrie glissée (voir chap. I, §3.2, exemple iii). Comme la translation $t_{\overrightarrow{v}}$ est le produit de deux reflexions par rapport à des droites perpendiculaires à D, on voit qu'une symétrie glissée est la composée de p réflexions, avec $p = 2 + 1$, et que p ne peut être choisi < 3. En fait :

Proposition 3.5. *Soit f une isométrie affine d'un espace affine euclidien $\mathcal{E}$ de dimension n. Il existe un entier $p \leq n + 1$ et des reflexions $\tau_{\mathcal{H}_1}, ..., \tau_{\mathcal{H}_p}$ telles que $f = \tau_{\mathcal{H}_p} \circ ... \circ \tau_{\mathcal{H}_1}$.*

Preuve : si f admet un point fixe O, f s'interprète comme une isométrie vectorielle du vectorialisé $\mathcal{E}_O$, et on peut lui appliquer la Proposition 3.3.ii. Sinon, $Ker(\overrightarrow{f} - id_E)$ n'est *pas* inversible, de sorte que l'entier a apparaissant dans la décomposition de l'isométrie vectorielle $\overrightarrow{f}$ à la Proposition 3.3.i est nécessairement ≥ 1. Considérons alors la décomposition canonique $f = t_{\overrightarrow{v}} \circ g$ de f : comme $\overrightarrow{g} = \overrightarrow{f}$, son a est aussi ≥ 1, et comme g admet un point fixe, on peut, en passant au vectorialisé, écrire g comme un produit d'au plus $b + 2c < n$ réflexions de $\mathcal{E}_O$, d'où, puisque $t_{\overrightarrow{v}}$ est produit de deux réflexions, une décomposition de f en produits d'au plus $b + 2c + 2 \leq n + 1$ réflexions.

Voici une autre preuve, plus géométrique, de cet énoncé. Soient $\Phi \subset Fix(f)$ un ensemble de points fixes de f, et P un point de $\mathcal{E}$ non fixé par f. Montrons qu'il existe une réflexion $\tau_{\mathcal{H}}$ telle que l'isométrie $g_1 = \tau_{\mathcal{H}} \circ f$ admette P et les points de Φ parmi ses points fixes. Puisque $f(P) = P'$ n'est pas égal à P, il existe un unique hyperplan $\mathcal{H}$ orthogonal à (PP') et passant par le milieu M du segment $[PP']$. Alors, $\tau_{\mathcal{H}}(P') = P$, donc $P \in Fix(g_1)$. Par ailleurs, tout point Q de Φ vérifie $d(Q, P) = d(f(Q)f(P)) = d(Q, P')$, donc $(QM) \perp (PP')$, et $Q \in \mathcal{H}$ est fixé par $\tau_{\mathcal{H}}$, donc par $\tau_{\mathcal{H}} \circ f = g_1$.

Soit alors $\{P_0, ..., P_n\}$ un repère affine de $\mathcal{E}$. En itérant le procédé supra p fois, avec $p \leq n + 1$, on construit p hyperplans $\mathcal{H}_i$ tels que l'isométrie $g = \tau_{\mathcal{H}_p} \circ ... \circ \tau_{\mathcal{H}_1} \circ f$ admette $P_0, ..., P_n$ parmi ses points fixes. Comme une application affine est entièrement déterminée par ses valeurs sur un repère affine, c'est que $g = id_{\mathcal{E}}$, et $f = \tau_{\mathcal{H}_p} \circ ... \circ \tau_{\mathcal{H}_1}$.

Signalons pour conclure que sans être des isométries, les projections orthogonales et les similitudes (c'est-à-dire les composées d'isométries par des homothéties) jouent un rôle important en géométrie euclidienne. Le cercle des 9 points en fournit une illustration classique: voir http://pagesperso-orange.fr/debart/geoplan/feuerbach.html , d'où est extraite la figure ci-dessous.