**Université Pierre et Marie Curie, année 2005-2006**

Agrégation externe de Mathématiques

# Droites projectives, homographies

Ce qui suit résume les définitions et résultats essentiels concernant les droites projectives et les homographies. Dans toute la suite, on fixe un corps commutatif $K$, et les espaces vectoriels considérés seront des $K$-espaces vectoriels.

## Définitions générales

**Définition 1**. *Soit $E$ un plan vectoriel (espace vectoriel de dimension 2) sur $K$. On appelle* **droite projective associée à E** *l'ensemble des droites vectorielles de $E$, et cet ensemble est noté $\mathbb{P}(E)$. On appelle* **droite projective** *tout ensemble de la forme $\mathbb{P}(E)$ (pour un certain plan vectoriel $E$). La droite projective associée au plan $K^2$ est notée $\mathbb{P}(K^2)$ ou $\mathbb{P}^1(K)$, elle est appelée* **droite projective standard** *sur $K$.*

Soit $E$ un plan vectoriel. À tout vecteur $x \in E \setminus \{0\}$, associons la droite vectorielle $Kx$. On définit ainsi une application canonique $p : E \setminus \{0\} \longrightarrow \mathbb{P}(E)$, notée aussi $x \mapsto [x]$. Elle est surjective: si $D$ est une droite vectorielle de $E$ et $x$ est un vecteur non nul de $D$, on a $D = Kx = [x]$. La relation d'équivalence $\mathcal{R}$ sur $E \setminus \{0\}$ associée à $p$ est la relation de *colinéarité*: si $x, y \in E \setminus \{0\}$, $x\mathcal{R}y$ équivaut à $Kx = Ky$. Les classes modulo $\mathcal{R}$ sont donc les $D \setminus \{0\}$, où $D \in \mathbb{P}(E)$. Nous identifierons donc, via $p$, l'ensemble $\mathbb{P}(E)$ à l'ensemble quotient $(E \setminus \{0\})/\mathcal{R}$.

Bien que les éléments de $\mathbb{P}(E)$ soient des droites vectorielles de $E$, nous les appellerons aussi des **points** de la droite projective $\mathbb{P}(E)$.

**Définition 2**. *Soient $E, E'$ deux plans vectoriels et $u$ un isomorphisme (linéaire) de $E$ sur $E'$. On note $[u]$ la bijection de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ définie ainsi: si $D \in \mathbb{P}(E)$, i.e. si $D$ est une droite vectorielle de $E$, $[u](D)$ est la droite vectorielle $u(D)$ de $E'$. On appelle* **homographie** *de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ toute bijection de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$ de la forme $[u]$, pour un certain isomorphisme $u$ de $E$ sur $E'$.*

**Lemme 1**. *Soient $E, E'$ deux plans vectoriels et $u, v$ deux isomorphismes de $E$ sur $E'$. Pour que les homographies $[u]$ et $[v]$ soient égales, il faut et il suffit que $u$ et $v$ soient colinéaires.*

*Démonstration*. Si $v = \lambda u$, pour un certain $\lambda \in K^*$, $v(D) = \lambda(u(D)) = u(D)$ pour toute droite vectorielle $D$ de $E$, donc $[v] = [u]$. Supposons inversement que $[u] = [v]$. Pour tout $x \in E$ non nul, il existe alors un scalaire $\lambda_x \in K^*$ tel que $v(x) = \lambda_x u(x)$. Il s'agit de montrer que l'application $x \mapsto \lambda_x$ de $E \setminus \{0\}$ dans $K^*$ est constante. Soient donc $x, y \in E \setminus \{0\}$. Supposons d'abord que $x$ et $y$ soient linéairement indépendants. On a:

$$\lambda_{x+y}u(x) + \lambda_{x+y}u(y) = \lambda_{x+y}u(x+y) = v(x+y) = v(x) + v(y) = \lambda_x u(x) + \lambda_y u(y)\,.$$

Puisque $(u(x), u(y))$ est une famille libre de $E'$, on en déduit que $\lambda_x = \lambda_{x+y} = \lambda_y$. Si $x, y$ sont liés, considérons un vecteur $z \in E \setminus Kx$. Alors les familles $(x, z)$ et $(y, z)$ sont libres, donc $\lambda_x = \lambda_z = \lambda_y$, en vertu du cas déjà traité.

cqfd

Voici un théorème essentiel sur les homographies.

**Théorème 1**. *Soient $\Delta, \Delta'$ deux droites projectives et $t_1, t_2, t_3$ (resp. $t'_1, t'_2, t'_3$) trois points de $\Delta$ (resp. $\Delta'$) distincts. Il existe une* **unique** *homographie $h$ de $\Delta$ sur $\Delta'$ telle que $h(t_i) = t'_i$ pour $i = 1, 2, 3$.*

*Démonstration*. Il existe deux plans vectoriels $E, E'$ tels que $\Delta = \mathbb{P}(E)$ et $\Delta' = \mathbb{P}(E')$. Pour $i = 1, 2, 3$, le point $t_i$ de $\Delta$ est une droite vectorielle $D_i$ de $E$, de même le point $t'_i$ de $\Delta'$ est une droite vectorielle $D'_i$ de $E'$. Pour tout $i$, choisissons un vecteur non nul $x_i$ de $D_i$ (resp. $x'_i$ de $D'_i$).

Puisque $D_1 \neq D_2$, $(x_1, x_2)$ est une base de $E$. Il existe donc des scalaires $\alpha_1, \alpha_2 \in K$ uniques tels que $x_3 = \alpha_1 x_1 + \alpha_2 x_2$. En outre, $D_3$ étant distincte de $D_1$ et $D_2$, $\alpha_1$ et $\alpha_2$ sont non nuls. De même $(x'_1, x'_2)$ est une base de $E'$, et il existe $\alpha'_1, \alpha'_2 \in K^*$ tels que $x'_3 = \alpha'_1 x'_1 + \alpha'_2 x'_2$. Posons $\lambda_1 = \alpha_1^{-1}\alpha'_1$ et $\lambda_2 = \alpha_2^{-1}\alpha'_2$. Soit $u : E \to E'$ l'isomorphisme linéaire appliquant $x_1$ sur $\lambda_1 x'_1$ et $x_2$ sur $\lambda_2 x'_2$. Ainsi $u(D_i) = D'_i$ pour $i = 1, 2$. De plus:

$$u(x_3) = u(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1\lambda_1 x'_1 + \alpha_2\lambda_2 x'_2 = \alpha'_1 x'_1 + \alpha'_2 x'_2 = x'_3\,,$$

d'où $u(D_3) = D'_3$. L'homographie $[u]$ de $\Delta$ sur $\Delta'$ applique bien $t_i$ sur $t'_i$, pour $i = 1, 2, 3$.

Soit $v$ un autre isomorphisme de $E$ sur $E'$ tel que $v(D_i) = D'_i$ pour $i = 1, 2, 3$. Il existe donc $\beta_1, \beta_2, \beta_3 \in K^*$ tels que $v(x_i) = \beta_i x'_i$ pour $i = 1, 2, 3$. Alors:

$$\beta_3(\alpha'_1 x'_1 + \alpha'_2 x'_2) = \beta_3 x'_3 = v(x_3) = v(\alpha_1 x_1 + \alpha_2 x_2) = \alpha_1\beta_1 x'_1 + \alpha_2\beta_2 x'_2\,,$$

d'où $\beta_3\alpha'_1 = \alpha_1\beta_1$ et $\beta_3\alpha'_2 = \alpha_2\beta_2$. Autrement dit $\beta_1 = \lambda_1\beta_3$ et $\beta_2 = \lambda_2\beta_3$. Il en résulte que $v = \beta_3 u$ car, pour $i = 1, 2$, $v(x_i) = \beta_i x'_i = \lambda_i\beta_3 x'_i = \beta_3 u(x_i)$. Ainsi $[v] = [u]$.

cqfd

Soit $E$ un plan vectoriel. Si $u \in \mathrm{GL}(E)$, l'homographie $[u]$ est en particulier une permutation de $\mathbb{P}(E)$. Il est en outre évident que $u \mapsto [u]$ est un morphisme de $\mathrm{GL}(E)$ dans $\mathfrak{S}(\mathbb{P}(E))$, groupe des permutations de $\mathbb{P}(E)$.

**Proposition 1**. *Soit $E$ un plan vectoriel.*

1) *L'ensemble des homographies de la droite projective* $\mathbb{P}(E)$ *sur elle-même est un sous-groupe de* $\mathfrak{S}(\mathbb{P}(E))$*, on le note* $\mathrm{PGL}(E)$*. Lorsque* $E = K^2$*, le groupe* $\mathrm{PGL}(K^2)$ *est aussi noté* $\mathrm{PGL}_2(K)$*.*

2) *L'application* $u \mapsto [u]$ *est un morphisme surjectif de* $\mathrm{GL}(E)$ *sur* $\mathrm{PGL}(E)$*, dont le noyau est le groupe des homothéties* $\{\lambda \,\mathrm{id}_E \mid \lambda \in K^*\}$*.*

*Démonstration*. L'assertion 1) résulte de la définition d'une homographie et de la remarque précédant cette proposition. Pour l'assertion 2), la surjectivité résulte de la définition d'une homographie, et la description du noyau résulte du lemme 1.

cqfd

Le théorème suivant est une simple traduction du théorème 1 lorsque $E' = E$.

**Théorème 2**. *Soit* $E$ *un plan vectoriel. L'opération naturelle de* $\mathrm{PGL}(E)$*, qui est un sous-groupe de* $\mathfrak{S}(\mathbb{P}(E))$*, sur* $\mathbb{P}(E)$*, est «simplement trois fois transitive». Autrement dit, étant donnés trois points* $t_1, t_2, t_3$ *(resp.* $t'_1, t'_2, t'_3$*) de* $\mathbb{P}(E)$ *distincts, il existe une unique homographie* $h \in \mathrm{PGL}(E)$ *appliquant* $t_i$ *sur* $t'_i$ *pour* $i = 1, 2, 3$*.*

Voyons maintenant une interprétation «concrète» de la droite projective standard $\mathbb{P}^1(K)$ et du groupe $\mathrm{PGL}_2(K)$ des homographies de cette droite projective. Considérons l'ensemble $\widehat{K} = K \cup \{\infty\}$, où $\infty$ est un symbole arbitraire, n'appartenant pas à $K$.

**Lemme 2**. *Considérons l'application* $\varphi$ *de* $K^2 \setminus \{0\}$ *dans* $\widehat{K}$ *définie ainsi: soit* $(x, y) \in K^2 \setminus \{0\}$*. On pose* $\varphi((x, y)) = x/y$ *si* $y \neq 0$ *et* $\varphi((x, y)) = \infty$ *si* $y = 0$*. Alors* $\varphi$ *induit une bijection* $\Phi$ *de* $\mathbb{P}^1(K) = (K^2 \setminus \{0\})/\mathcal{R}$ *sur* $\widehat{K}$*.*

*Démonstration*. D'abord $\varphi$ est surjective: $\infty = \varphi((1, 0))$ et, pour tout $t \in K$, $t = \varphi((t, 1))$. Considérons ensuite deux couples $(x, y)$, $(x', y') \in K^2 \setminus \{0\}$. Ces deux couples ont même image par $\varphi$ si et seulement si ou bien $y = y' = 0$, ou bien $y \neq 0, y' \neq 0$ et $x/y = x'/y'$, ce qui équivaut à dire que $(x, y)$ et $(x', y')$ sont colinéaires. La relation d'équivalence associée à l'application $\varphi$ est donc $\mathcal{R}$, d'où la conclusion, par passage au quotient.

cqfd

Passons aux homographies. Tout d'abord, on identifie comme d'habitude le groupe $\mathrm{GL}(K^2)$ au groupe $\mathrm{GL}_2(K)$ des matrices carrées inversibles $2 \times 2$ à coefficients dans $K$: toute transformation linéaire $u$ de $K^2$ est identifiée à sa matrice dans la base canonique de $K^2$.

**Proposition 2**. *Soient* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ *et* $h$ *l'homographie de* $\mathbb{P}^1(K)$ *associée à* $M$*. La permutation* $\tilde{h} = \Phi \circ h \circ \Phi^{-1}$ *de* $\widehat{K}$ *s'obtient ainsi. En général, si* $z \in K$ *et si* $cz + d \neq 0$*,*

$$\tilde{h}(z) \;=\; \frac{az + b}{cz + d}\,. \tag{1}$$

*On complète cette formule par les suivantes:*

$$\tilde{h}(z) \;=\; \infty \;\text{ si }\; c \neq 0 \;\text{ et }\; z = -d/c\,,$$

$$\tilde{h}(\infty) \;=\; \begin{cases} \infty & si\ c = 0\,, \\ a/c & si\ c \neq 0\,. \end{cases} \tag{2}$$

*Démonstration*. Soient $z \in \widehat{K}$ et $(x, y) \in K^2 \setminus \{0\}$ tels que $z = \varphi((x, y))$, de sorte que $\Phi^{-1}(z)$ est la droite vectorielle $K(x, y)$. L'image $(x', y')$ de $(x, y)$ par $M$ est donnée par l'égalité:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} \;=\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Il résulte des définitions que $\tilde{h}(z) = \varphi((x', y'))$, c'est-à-dire:

$$\tilde{h}(z) \;=\; \varphi((ax + by, cx + dy))\,.$$

Supposons d'abord $z \neq \infty$, soit $y \neq 0$. Dans ce cas $z = x/y$, donc $x = zy$, d'où:

$$\tilde{h}(z) \;=\; \varphi(y(az + b, cz + d)) \;=\; \varphi((az + b, cz + d))\,.$$

Si $cz + d \neq 0$, il en résulte que $\tilde{h}(z) \in K$ est donné par la formule (1). Supposons que $cz + d = 0$. Comme $(c, d) \neq (0, 0)$, on a $c \neq 0$ et $z = -d/c$. Alors $\tilde{h}(z) = \varphi((az + b, 0)) = \infty$, comme désiré.

Supposons maintenant que $z = \infty$, i.e. $y = 0$. Alors $x \neq 0$, et il vient:

$$\tilde{h}(\infty) \;=\; \varphi(x(a, c)) \;=\; \varphi((a, c))\,.$$

On en déduit aussitôt la formule (2).

cqfd

Désormais, nous identifierons, via la bijection $\Phi$ définie dans le lemme 2, la droite projective $\mathbb{P}^1(K)$ à $\widehat{K}$. Cette identification étant faite, le groupe $\mathrm{PGL}_2(K)$ apparaît comme sous-groupe de $\mathfrak{S}(\widehat{K})$. Plus précisément, $\mathrm{PGL}_2(K)$ est formé des **transformations homographiques** de $\widehat{K}$, i.e. des transformations $[M] : z \mapsto (az + b)/(cz + d)$, où $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$, avec les trois conventions particulières concernant $\infty$ et données par la proposition 2. Rappelons que $M \mapsto [M]$ est un morphisme surjectif de $\mathrm{GL}_2(K)$ sur $\mathrm{PGL}_2(K)$, le noyau de ce morphisme étant $\{\lambda I_2 \mid \lambda \in K^*\}$. Par ailleurs, l'opération naturelle de $\mathrm{PGL}_2(K)$ sur $\widehat{K}$ est «simplement trois fois transitive», comme dans le théorème 2. Le stabilisateur de $\infty$ est simple à décrire:

**Lemme 3**. *Le stabilisateur de $\infty$ dans l'opération naturelle de $\mathrm{PGL}_2(K)$ sur $\widehat{K}$ est formé des transformations affines de la droite affine $K$, i.e. des transformations $f : z \mapsto az + b$, où $a \in K^*$ et $b \in K$, $f$ étant prolongée par $f(\infty) = \infty$.*

*Démonstration*. D'après la proposition 2, ce stabilisateur est formé des transformations $[M]$, où $M \in \mathrm{GL}_2(K)$ est du type $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, avec $a, d \in K^*$ et $b \in K$. Si $M$ est de ce type, on a $M = dN$, donc $[M] = [N]$, en posant:

$$N \;=\; \begin{pmatrix} a/d & b/d \\ 0 & 1 \end{pmatrix}.$$

Le lemme en résulte aussitôt.

cqfd

La droite projective $\widehat{K} = \mathbb{P}^1(K)$ possède trois points privilégiés, à savoir $\infty, 0, 1$ (rappelons que, dans le corps $K$, on a toujours $0 \neq 1$). Cela justifie la définition suivante:

**Définition 3**. *Soit $\Delta$ une droite projective et $a, b, c, d \in \Delta$ quatre points distincts. Il existe une unique homographie $h$ de $\Delta$ sur $\mathbb{P}^1(K)$ appliquant $a, b, c$ sur $\infty, 0, 1$ respectivement. L'image de $d$ par $h$ est appelée* **birapport** *de $a, b, c, d$ (pris dans cet ordre) et notée $[a, b; c, d]$. C'est donc un élément de $K \setminus \{0, 1\}$.*

Ce birapport $[a, b; c, d]$ peut être calculé explicitement lorsque $\Delta = \widehat{K}$:

**Proposition 3**. *Soient $a, b, c, d \in \widehat{K}$ quatre points distincts. On a en général:*

$$[a, b; c, d] \;=\; \frac{c-a}{c-b} : \frac{d-a}{d-b} \;=\; \frac{(c-a)(d-b)}{(c-b)(d-a)}. \tag{3}$$

*Plus précisément, cette formule est vraie lorsque $a, b, c, d \in K$. On la complète par les formules suivantes, qui reviennent à adopter des conventions naturelles quant au second membre de* (3)*:*

$$[\infty, b; c, d] = \frac{d-b}{c-b}\;, \quad [a, \infty; c; d] = \frac{c-a}{d-a}\;, \quad [a, b; \infty, d] = \frac{d-b}{d-a}\;, \quad [a, b; c, \infty] = \frac{c-a}{c-b}.$$

*Démonstration*. Supposons que $a, b, c, d \in K$. Pour tout $\lambda \in K^*$, l'homographie:

$$h : z \longmapsto \frac{\lambda(z-b)}{z-a}$$

applique $a$ sur $\infty$ et $b$ sur 0. Elle applique $c$ sur $\lambda(c-b)/(c-a)$. Choisissons donc $\lambda = (c-a)/(c-b)$. Alors $h$ applique $a, b, c$ sur $\infty, 0, 1$ respectivement donc, par définition, $[a, b; c, d] = h(d)$. D'où:

$$[a, b; c, d] \;=\; \frac{\lambda(d-b)}{d-a} \;=\; \frac{(c-a)(d-b)}{(c-b)(d-a)}.$$

La formule (3) est ainsi établie.

Dans le cas où l'un des points $a, b, c, d$ est égal à $\infty$, on modifie en conséquence la construction de $h$. Si $a = \infty$, on cherche $h$ sous la forme $z \mapsto \lambda(z-b), \lambda \in K^*$. On aura $h(c) = 1$ si et seulement si $\lambda = 1/(c-b)$, et alors $h(d) = (d-b)/(c-b)$, comme désiré. Si $b = \infty$, on cherche $h$ sous la forme $z \mapsto \lambda/(z-a), \lambda \in K^*$. On aura $h(c) = 1$ si et seulement si $\lambda = c-a$, et alors $h(d) = (c-a)/(d-a)$, comme désiré. Si $c = \infty$, on cherche $h$ sous la forme $z \mapsto \lambda(z-b)/(z-a), \lambda \in K^*$. On aura $h(\infty) = 1$ si et seulement si $\lambda = 1$, et alors $h(d) = (d-b)/(d-a)$, comme désiré. Enfin, si $d = \infty$, $h$ est, comme dans le cas général, donné par la formule:

$$h(z) \;=\; \frac{(c-a)(z-b)}{(c-b)(z-a)}\,.$$

Dans ce cas, par définition (cf. la proposition 2), $h(\infty) = (c-a)/(c-b)$, comme désiré.

cqfd

**Proposition 4**. *Soient $\Delta, \Delta'$ deux droites projectives et $a, b, c, d \in \Delta$ quatre points distincts.*

*1) Pour toute homographie $h$ de $\Delta$ sur $\Delta'$, on a:*

$$[h(a), h(b); h(c), h(d)] \;=\; [a, b; c, d]\,,$$

*autrement dit les homographies conservent les birapports.*

*2) Inversement, soient $a', b', c', d' \in \Delta'$ quatre points distincts. On suppose que l'on a $[a', b'; c', d'] = [a, b; c, d]$. Il existe alors une unique homographie $h$ de $\Delta$ sur $\Delta'$ appliquant $a, b, c, d$ sur $a', b', c', d'$ respectivement.*

*Démonstration*. Soit $h_1$ l'homographie de $\Delta$ sur $\widehat{K}$ appliquant $a, b, c$ sur $\infty, 0, 1$ respectivement, de sorte que $h_1(d) = [a, b; c, d]$, par définition du birapport. Alors $h_1 \circ h^{-1}$ est une homographie de $\Delta'$ sur $\widehat{K}$, appliquant $h(a), h(b), h(c)$ sur $\infty, 0, 1$ respectivement. Toujours par définition du birapport, on a:

$$[h(a), h(b); h(c), h(d)] \;=\; (h_1 \circ h^{-1})(h(d)) \;=\; h_1(d) \;=\; [a, b; c, d]\,,$$

ce qui établit l'assertion 1).

Pour 2), il existe en tous cas une unique homographie $h$ de $\Delta$ sur $\Delta'$ appliquant $a, b, c$ sur $a', b', c'$ respectivement. D'après 1), on a:

$$[a', b'; c', h(d)] \;=\; [h(a), h(b); h(c), h(d)] \;=\; [a, b; c, d] \;=\; [a', b'; c', d']\,.$$

Il en résulte que $d' = h(d)$: si $h'$ est l'homographie de $\Delta'$ sur $\widehat{K}$ appliquant $a', b', c'$ sur $\infty, 0, 1$ respectivement, on a $h'(d') = h'(h(d))$, d'où $d' = h(d)$ puisque $h'$ est une bijection de $\Delta'$ sur $\widehat{K}$.

cqfd

**Remarque.** Le birapport possède des propriétés de symétrie. Considérons, sur une droite projective $\Delta$, quatre points distincts $a, b, c, d$, et soit $\omega = [a, b; c, d]$. Alors:

$$[b, a; c, d] = [a, b; d, c] = \omega^{-1}\,,\;\; [c, d; a, b] = \omega\,,\;\; [a, c; b, d] = 1 - \omega\,.$$

Pour vérifier ces formules, compte tenu du théorème 1, on peut supposer que $\Delta = \widehat{K}$ et $a = \infty$, $b = 0$, $c = 1$, auquel cas $\omega = d$. On utilise alors les formules complémentaires de la proposition 3. Par exemple,

$$[0, \infty; 1, d] = \frac{1-0}{d-0} = d^{-1} \ , \quad [\infty, 1; 0, d] = \frac{d-1}{0-1} = 1 - d \, .$$

La conservation des birapports caractérise en fait les homographies:

**Proposition 5**. *Soient $\Delta, \Delta'$ deux droites projectives et $f$ une bijection de $\Delta$ sur $\Delta'$. Pour que $f$ soit une homographie, il faut et il suffit que $f$ conserve les birapports.*

*Démonstration*. La condition est nécessaire, vu la proposition 4. Supposons inversement que $f$ conserve les birapports. Soient $a, b, c$ trois points de $\Delta$ distincts et $a', b', c'$ leurs images respectives par $f$. Soit $h$ l'unique homographie de $\Delta$ sur $\Delta'$ appliquant $a, b, c$ sur $a', b', c'$ respectivement. Montrons que $f = h$. Pour cela, soit $x \in \Delta \setminus \{a, b, c\}$, posons $x' = h(x)$. Puisque $h$ et $f$ conservent toutes deux les birapports, on a:

$$\begin{aligned} [a', b'; c', x'] \ &= \ [h(a), h(b); h(c), h(x)] \ = \ [a, b; c, x] \\ &= \ [f(a), f(b); f(c), f(x)] \ = \ [a', b'; c', f(x)] \, . \end{aligned}$$

Comme dans la preuve précédente, il en résulte que $f(x) = x'$, i.e. $f(x) = h(x)$, ceci pour tout $x \in \Delta$, ce qui montre que $f = h$ est une homographie.

cqfd

**Remarque.** Soient $\Delta$ une droite projective et $a, b, c \in \Delta$ trois points distincts. Nous avons déjà utilisé le résultat suivant: $x \mapsto [a, b; c, x]$ est une bijection de $\Delta \setminus \{a, b, c\}$ sur $K \setminus \{0, 1\}$.

## Cas d'un corps de base fini

Supposons ici que $K$ soit un corps fini à $q$ éléments. Nous écrirons aussi $K = \mathbb{F}_q$, en désignant par $\mathbb{F}_q$ un corps à $q$ éléments fixé (un tel corps existe, et est unique à isomorphisme près). On sait que la caractéristique de $K$ est un nombre premier $p$ et que $q$ est une puissance de $p$, mais peu importe ici. Observons d'abord que la droite projective standard $\mathbb{P}^1(K)$, identifiée à $\widehat{K}$, est de cardinal $q + 1$. Il en résulte que toute droite projective $\mathbb{P}(E)$ est de cardinal $q + 1$ (considérer une homographie de $\mathbb{P}(E)$ sur $\widehat{K}$). D'après le théorème 2, le groupe $\mathrm{PGL}(E)$ opère simplement trois fois transitivement sur $\mathbb{P}(E)$, i.e. il opère simplement transitivement sur l'ensemble des triplets *injectifs* $(a, b, c)$ de points de $\mathbb{P}(E)$; il est clair que cet ensemble est de cardinal $(q+1)q(q-1) = q(q^2-1)$, d'où:

$$\mathrm{card}(\mathrm{PGL}(E)) \ = \ q(q^2 - 1) \, . \tag{4}$$

L'opération naturelle (et fidèle) de $\mathrm{PGL}(E)$ sur $\mathbb{P}(E)$ est donnée par un morphisme *injectif* de $\mathrm{PGL}(E)$ dans $\mathfrak{S}(\mathbb{P}(E))$. En numérotant les points de $\mathbb{P}(E)$, on obtient donc un morphisme injectif de $\mathrm{PGL}(E)$ dans $\mathfrak{S}_{q+1}$, i.e. $\mathrm{PGL}(E)$ est isomorphe à un sous-groupe de $\mathfrak{S}_{q+1}$. On en déduit le résultat suivant:

**Proposition 6**. *Pour les petites valeurs de $q$, on a les isomorphismes suivants:*

*1) Le groupe* $\mathrm{PGL}_2(\mathbb{F}_2)$ *est isomorphe au groupe symétrique* $\mathfrak{S}_3$.

*2) Le groupe* $\mathrm{PGL}_2(\mathbb{F}_3)$ *est isomorphe au groupe symétrique* $\mathfrak{S}_4$.

*3) Le groupe* $\mathrm{PGL}_2(\mathbb{F}_4)$ *est isomorphe au groupe alterné* $\mathfrak{A}_5$.

*4) Le groupe* $\mathrm{PGL}_2(\mathbb{F}_5)$ *est isomorphe au groupe symétrique* $\mathfrak{S}_5$.

*Démonstration*. Soit $q$ l'un des entiers $2, 3, 4, 5$. Comme il résulte de (4), $\mathrm{PGL}_2(\mathbb{F}_q)$ est isomorphe à un sous-groupe $G$ de $\mathfrak{S}_{q+1}$, d'ordre $q(q^2-1)$. Si $q = 2$ ou $q = 3$, on en déduit que $G = \mathfrak{S}_{q+1}$ (car ces deux groupes ont même ordre) , d'où les assertions 1) et 2). Si $q = 4$, $G$ est un sous-groupe de $\mathfrak{S}_5$, d'ordre 60, donc d'indice 2. On sait que $\mathfrak{A}_5$ est le seul sous-groupe d'indice 2 de $\mathfrak{S}_5$ (caractérisation du morphisme de signature), ce qui établit l'assertion 3).

Si $q = 5$, $G$ est un sous-groupe de $\mathfrak{S}_6$, d'ordre 120, donc d'indice 6. Le fait que $G$ soit isomorphe à $\mathfrak{S}_5$ est dans ce cas moins évident, cf. les compléments à la fin de ces notes.

## Cas du corps des réels et du corps des complexes: topologie

Dans ce qui suit, nous supposons que $K$ est l'un des corps $\mathbb{R}$ ou $\mathbb{C}$. Tout espace vectoriel $E$ de dimension finie sur $K$ possède alors une topologie canonique, définie par n'importe quelle norme sur $E$. En outre les parties compactes de $E$ sont exactement les parties fermées et bornées de $E$; de plus toute application linéaire d'un tel espace vectoriel de dimension finie dans un autre est continue.

En premier lieu, rappelons ce qu'est une **topologie quotient**. Soient $X$ un espace topologique, $\mathcal{R}$ une relation d'équivalence et $X/\mathcal{R}$ l'ensemble quotient correspondant. Désignons par $\pi : X \to X/\mathcal{R}$ la projection (ou application canonique), elle associe à chaque $x \in X$ sa classe modulo $\mathcal{R}$. La topologie quotient sur $X/\mathcal{R}$ est la topologie pour laquelle les ouverts sont les parties $\Omega$ de $X/\mathcal{R}$ telles que $\pi^{-1}(\Omega)$ soit un ouvert de $X$. On obtient bien ainsi une topologie sur $X/\mathcal{R}$. En outre d'une part les fermés de $X/\mathcal{R}$ sont les parties $F$ telles que $\pi^{-1}(F)$ soit un fermé de $X$, et d'autre part $\pi$ est évidemment continue. Le lemme suivant est utile:

**Lemme 4**. *Soient $Z$ un espace topologique et $f : X/\mathcal{R} \to Z$ une application. Pour que $f$ soit continue, il faut et il suffit que $f \circ \pi : X \to Z$ soit continue.*

*Démonstration*. Si $f$ est continue, $f \circ \pi$ l'est aussi, comme composée d'applications continues. Supposons que $f \circ \pi$ soit continue. Pour montrer que $f$ est continue, il suffit de voir que, pour tout ouvert $W$ de $Z$, $f^{-1}(W)$ est un ouvert de $X/\mathcal{R}$; par définition de la topologie quotient, cela signifie que $\pi^{-1}(f^{-1}(W))$ est un ouvert de $X$. C'est bien le cas, car $f \circ \pi$ est continue, et donc $(f \circ \pi)^{-1}(W) = \pi^{-1}(f^{-1}(W))$ est un ouvert de $X$.

cqfd

**Définition 4**. *Soit $E$ un plan vectoriel sur $K$. On a identifié la droite projective $\mathbb{P}(E)$ au quotient de $E\setminus\{0\}$ par la relation d'équivalence $\mathcal{R}$ de colinéarité. On munit désormais $\mathbb{P}(E)$ de la topologie quotient de $(E \setminus \{0\})/\mathcal{R}$.*

**Proposition 7**. *Toute homographie d'une droite projective (sur $K$) sur une autre est un homéomorphisme.*

*Démonstration*. Soient donc $E, E'$ deux plans vectoriels et $h$ une homographie de $\mathbb{P}(E)$ sur $\mathbb{P}(E')$. Par définition, il existe un isomorphisme $u$ de $E$ sur $E'$ tel que $h = [u]$ soit induite par $u$. Autrement dit, pour tout $x \in E \setminus \{0\}$, $h([x]) = [u(x)]$. En notant $\pi : E \setminus \{0\} \to \mathbb{P}(E)$ et $\pi' : E' \setminus \{0\} \to \mathbb{P}(E')$ les projections, cela signifie que le carré suivant est commutatif, i.e. $\pi' \circ u = h \circ \pi$:

$$\begin{array}{ccc} E \setminus \{0\} & \xrightarrow[\approx]{u} & E' \setminus \{0\} \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi'} \\ \mathbb{P}(E) & \xrightarrow[h]{\approx} & \mathbb{P}(E')\,. \end{array}$$

Or $u$ et $\pi'$ sont continues, donc $h \circ \pi$ est continue. Le lemme 4 montre ainsi que $h$ est continue. Il en est de même pour l'homographie réciproque $h^{-1}$, donc $h$ est un homéomorphisme.

cqfd

Compte tenu de cette proposition, il nous reste à étudier la topologie de la droite projective standard $\mathbb{P}^1(K)$. Cette droite projective ayant été identifiée à $\widehat{K}$, il nous faut décrire la topologie obtenue sur $\widehat{K}$ (c'est la topologie quotient sur $(K^2 \setminus \{0\})/\mathcal{R}$). Voici ce que l'on obtient:

**Proposition 8**. *Les ouverts de $\widehat{K}$ sont les suivants:*

- *les ouverts de $K$;*
- *les parties de la forme $(K \setminus A)\cup\{\infty\}$, où $A$ est un compact de $K$.*

*En particulier la topologie sur $K$ induite par celle de $\widehat{K}$ est la topologie usuelle de $K$, et en outre $K$ est un ouvert de $\widehat{K}$.*

*Démonstration*. Soit $\pi : K^2 \setminus \{0\} \to \widehat{K}$ la projection. Rappelons que, si $(x, y) \in K^2$ n'est pas nul, $\pi((x, y))$, que nous noterons simplement $\pi(x, y)$, vaut $\infty$ si $y = 0$ et $x/y$ si $y \neq 0$. Considérons une partie $U$ de $K$. Pour que $U$ soit un ouvert de $\widehat{K}$, il faut et il suffit que $\pi^{-1}(U)$ soit un ouvert de $K^2 \setminus \{0\}$, i.e. de $K^2$ (définition de la topologie quotient). Il est clair que l'on a:

$$\pi^{-1}(U) \;=\; \{(\lambda u, \lambda) \mid (u, \lambda) \in U \times K^*\}\,.$$

L'application $(t, \lambda) \mapsto (\lambda t, \lambda)$ est un homéomorphisme de $K \times K^*$ sur lui-même, appliquant $U \times K^*$ sur $\pi^{-1}(U)$. Ainsi $\pi^{-1}(U)$ est un ouvert de $K^2$ si et seulement si $U \times K^*$ est un ouvert

de $K \times K^*$, ce qui revient évidemment à dire que $U$ est un ouvert de $K$. En conclusion, une partie $U$ de $K$ est ouverte dans $\widehat{K}$ si et seulement si elle est ouverte dans $K$. Cela démontre déjà la dernière assertion de l'énoncé.

Soit maintenant $\Omega$ une partie de $\widehat{K}$ contenant $\infty$; on peut l'écrire sous la forme suivante: $\Omega = \{\infty\} \cup (K \setminus A)$, où $A$ est une partie de $K$. Alors:

$$\pi^{-1}(\Omega) \;=\; \{(\lambda u, \lambda) \mid (u, \lambda) \in (K \setminus A) \times K^*\} \cup (K^* \times \{0\})\,.$$

Supposons d'abord $\Omega$ ouverte. Alors, vu ce qui précède, $K \setminus A = \Omega \cap K$ est un ouvert de $K$, i.e. $A$ est fermé dans $K$. Par ailleurs $\pi^{-1}(\Omega)$ est un voisinage de $(1, 0)$. Il existe donc un réel $r \in ]0, 1[$ tel que tout couple $(t, \mu) \in K^2$ vérifiant $|1 - t| < r$ et $|\mu| < r$ appartienne à $\pi^{-1}(\Omega)$. En particulier, si $\mu \in K$ et $0 < |\mu| < r$, le couple $(1, \mu)$ appartient à $\pi^{-1}(\Omega)$, i.e. $1/\mu \in K \setminus A$. Ainsi $A$ est contenu dans le disque fermé de $K$, de centre 0 et de rayon $1/r$, donc $A$ est compact.

Supposons inversement que $A$ soit compact. Il existe $r \in ]0, 1[$ tel que $A$ soit contenu dans le disque fermé de $K$, de centre 0 et de rayon $1/r$. Pour conclure, étant donné $\alpha \in K^*$, il suffit de montrer que $\pi^{-1}(\Omega)$ est un voisinage de $(\alpha, 0)$. Montrons donc que $\pi^{-1}(\Omega)$ contient tout couple $(\beta, \lambda) \in K^2$ vérifiant les inégalités $|\beta - \alpha| < |\alpha|/2$ et $|\lambda| < r|\alpha|/2$. C'est clair si $\lambda = 0$. Sinon, on a $|\lambda^{-1}| > 2/(r|\alpha|)$ et $|\beta| > |\alpha|/2$, d'où $|\lambda^{-1}\beta| > 1/r$, ce qui montre que $u = \lambda^{-1}\beta \in K \setminus A$ et ainsi $(\beta, \lambda) = (\lambda u, \lambda) \in \pi^{-1}(\Omega)$, comme désiré.

cqfd

Pour déterminer plus précisément l'espace topologique $\widehat{K}$, à homéomorphisme près, étudions une situation plus générale. Considérons un entier $n \geq 1$. Munissons l'espace $\mathbb{R}^{n+1}$ (et aussi $\mathbb{R}^n$) de sa norme euclidienne standard, et identifions $\mathbb{R}^{n+1}$ à $\mathbb{R}^n \times \mathbb{R}$. Notons $S^n$ la sphère-unité de $\mathbb{R}^{n+1}$:

$$S^n \;=\; \left\{(x, t) \in \mathbb{R}^n \times \mathbb{R} \;\middle|\; \|x\|^2 + t^2 = 1\right\}.$$

Notons par ailleurs $N$ le pôle nord de $S^n$: $N = (0, 1) \in \mathbb{R}^n \times \mathbb{R}$. Considérons enfin l'ensemble $\widehat{\mathbb{R}^n} = \mathbb{R}^n \cup \{\infty\}$ (où $\infty$ est un symbole n'appartenant pas à $\mathbb{R}^n$).

Notons $s$ l'application de $S^n$ dans $\widehat{\mathbb{R}^n}$ définie comme suit:

$$s(N) = \infty \;\text{ et, si } M = (x, t) \in S^n \setminus \{N\}, \quad s(M) = \frac{1}{1 - t}\, x\,. \tag{5}$$

Si $M = (x, t) \in S^n \setminus \{N\}$, i.e. si $t < 1$, la droite affine $NM$ coupe l'hyperplan $\mathbb{R}^n \times \{0\}$ (identifié à $\mathbb{R}^n$) de $\mathbb{R}^{n+1}$ en $s(M)$, car

$$\overrightarrow{Ns(M)} \;=\; \left(\frac{1}{1 - t}\, x, -1\right) \;=\; \frac{1}{1 - t}\,(x, t - 1) \;=\; \frac{1}{1 - t}\,\overrightarrow{NM}\,.$$

L'application $s$ est appelée **projection stéréographique** de pôle $N$.

**Proposition 9**. *L'application $s$ est une bijection de $S^n$ sur $\widehat{\mathbb{R}^n}$.*

*Démonstration*. Il suffit de montrer que la restriction de $s$ à $S^n \setminus \{N\}$ est une bijection de $S^n \setminus \{N\}$ sur $\mathbb{R}^n$. Soit $\rho : \mathbb{R}^n \to \mathbb{R}^{n+1}$ l'application définie par:

$$\rho(y) \;=\; \left( \frac{2}{\|y\|^2+1}\, y, \frac{\|y\|^2-1}{\|y\|^2+1} \right) . \tag{6}$$

Soit $y \in \mathbb{R}^n$. Si l'on écrit $\rho(y) = (x,t)$, on a $t < 1$, et

$$\|x\|^2 + t^2 \;=\; \frac{4\|y\|^2 + (\|y\|^2-1)^2}{(\|y\|^2+1)^2} \;=\; 1\,.$$

Ainsi $\rho(y) \in S^n \setminus \{N\}$. En outre, $1 - t = 2/(\|y\|^2+1)$, d'où:

$$s(\rho(y)) \;=\; s(x,t) \;=\; \frac{\|y\|^2+1}{2}\, x \;=\; y\,.$$

Le composé $s \circ \rho$ est donc l'identité de $\mathbb{R}^n$.

Soit ensuite $(x,t) \in S^n \setminus \{N\}$, et soit $y = s(x,t)$. Alors:

$$\|y\|^2 \;=\; \frac{\|x\|^2}{(1-t)^2} \;=\; \frac{1-t^2}{(1-t)^2} \;=\; \frac{1+t}{1-t}\,.$$

On en déduit:

$$\|y\|^2 - 1 \;=\; \frac{2t}{1-t}\,, \quad \|y\|^2 + 1 \;=\; \frac{2}{1-t}\,, \quad \frac{\|y\|^2-1}{\|y\|^2+1} \;=\; t\,,$$

et par suite $\rho(y) = ((1-t)y, t) = (x,t)$. Le composé $\rho \circ s$ est donc l'identité de $S^n \setminus \{N\}$. La proposition est ainsi démontrée. En outre la bijection réciproque de $s$ est $\rho$, prologée par $\rho(\infty) = N$.

cqfd

Munissons maintenant $\widehat{\mathbb{R}^n}$ de la topologie dont les ouverts sont:

- d'une part les ouverts de $\mathbb{R}^n$;
- d'autre part les $(\mathbb{R}^n \setminus A) \cup \{\infty\}$, où $A$ est un compact de $\mathbb{R}^n$.

La topologie usuelle de $\mathbb{R}^n$ coïncide donc avec la topologie induite par celle de $\widehat{\mathbb{R}^n}$, et en outre $\mathbb{R}^n$ est un ouvert de $\widehat{\mathbb{R}^n}$.

**Lemme 5**. *L'espace topologique $\widehat{\mathbb{R}^n}$ est séparé.*

*Démonstration*. D'abord $\mathbb{R}^n$ est séparé, donc deux points de $\mathbb{R}^n$ distincts peuvent être séparés par deux ouverts de $\mathbb{R}^n$, qui sont aussi ouverts dans $\widehat{\mathbb{R}^n}$. Ensuite, si $a \in \mathbb{R}^n$, soient $B$ la boule ouverte de centre $a$ et de rayon 1 et $\bar{B}$ son adhérence. Alors $(\mathbb{R}^n \setminus \bar{B}) \cup \{\infty\}$ et $B$ sont deux ouverts de $\widehat{\mathbb{R}^n}$ disjoints, contenant $\infty$ et $a$ respectivement.

cqfd

**Proposition 10**. *La projection stéréographique $s$ est un homéomorphisme de la sphère $S^n$ sur $\widehat{\mathbb{R}^n}$. En particulier $\widehat{\mathbb{R}^n}$ est compact et connexe par arcs.*

*Démonstration*. On sait que $S^n$ est compacte et connexe par arcs. La dernière assertion de l'énoncé résultera donc du fait que $s$ soit un homéomorphisme. La proposition 9 montre que $s$ est bijective. De plus $S^n$ est compacte et $\widehat{\mathbb{R}^n}$ est séparé, vu le lemme précédent. Il suffit donc de montrer que $s$ est continue. La restriction de $s$ à $S^n \setminus \{N\}$ est une application continue de $S^n \setminus \{N\}$ dans $\mathbb{R}^n$, comme le montre la dernière formule (5).

Il reste à voir que $s$ est continue au point $N$. Soit $\Omega$ un ouvert de $\widehat{\mathbb{R}^n}$ contenant $\infty$, montrons que $s^{-1}(\Omega)$ est un voisinage de $N$ dans $S^n$. Nous pouvons nous restreindre au cas où $\Omega = (\mathbb{R}^n \setminus \bar{B}) \cup \{\infty\}$, $\bar{B}$ étant une boule fermée de centre 0 et de rayon $r > 1$ de $\mathbb{R}^n$. Dans ce cas, $s^{-1}(\Omega)$ est formé de $N$ et des points $(x,t) \in S^n \setminus \{N\}$ tels que $\|s(x,t)\| > r$, c'est-à-dire $\|x\|^2 > r^2(1-t)^2$, ce qui équivaut à $1 - t^2 > r^2(1-t)^2$, ou encore à $1 + t > r^2(1-t)$. Ainsi

$$s^{-1}(\Omega) \;=\; \left\{(x,t) \in S^n \mid t > \frac{r^2-1}{r^2+1}\right\},$$

ce qui montre que $s^{-1}(\Omega)$ est un ouvert de $S^n$.

cqfd

Cette proposition permet de décrire la topologie des droites projectives sur $\mathbb{R}$ ou $\mathbb{C}$:

**Proposition 11**.

*1) Toute droite projective réelle est homéomorphe au cercle-unité $S^1$.*

*2) Toute droite projective complexe est homéomorphe à la sphère-unité $S^2$ de $\mathbb{R}^3$.*

*Démonstration*. Soit $K$ l'un des corps $\mathbb{R}$ ou $\mathbb{C}$. Comme $\mathbb{R}$-espace vectoriel, $K = \mathbb{R}^n$, où $n$ vaut 1 ou 2, suivant les cas. La topologie sur $\widehat{K}$ décrite dans la proposition 8 n'est autre que la topologie de $\widehat{\mathbb{R}^n}$ décrite ci-dessus. La proposition 10 montre donc que la droite projective standard $\mathbb{P}^1(K) = \widehat{K}$ est homéomorphe à $S^n$. Il en est alors de même pour toute droite projective sur $K$, en vertu de la proposition 7.

cqfd

**Remarque.** La topologie sur $\widehat{\mathbb{R}^n}$ décrite ci-dessus se généralise comme suit. Soit $X$ un espace topologique localement compact: $X$ est séparé, et tout point de $X$ possède un voisinage compact. Sur $\widehat{X} = X \cup \{\infty\}$, on considère la topologie dont les ouverts sont:

- les ouverts de $X$;
- les $(X \setminus A) \cup \{\infty\}$, où $A$ est un compact de $X$.

Ainsi $X$ est un ouvert de $\widehat{X}$, et la topologie de $X$ induite par celle de $\widehat{X}$ coïncide avec la topologie donnée de $X$. On démontre que $\widehat{X}$ est un espace compact, c'est ce qu'on appelle le compactifié d'Alexandroff de l'espace localement compact $X$. On a compactifié (rendu compact)

$X$ en lui ajoutant un point. Ainsi le compactifié d'Alexandroff de $\mathbb{R}$ est homéomorphe à $S^1$. On ne confondra pas avec un autre compactifié de $\mathbb{R}$, à savoir la droite achevée $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ qui, munie de sa topologie naturelle, est homéomorphe au segment $[0, 1]$.

### Droite projective complexe et géométrie euclidienne plane

Notons ici $X$ le plan affine euclidien orienté $\mathbb{R}^2$ standard. On identifie $X$ à la droite affine complexe $\mathbb{C}$, en identifiant chaque point $A \in X$ avec son affixe $a \in \mathbb{C}$. En posant $\widehat{X} = X \cup \{\infty\}$, on identifie ainsi $\widehat{X}$ à $\widehat{\mathbb{C}}$. Par convention, l'affixe de $\infty \in \widehat{X}$ est $\infty \in \widehat{\mathbb{C}}$. Dans ce cadre, le but de ce qui suit est d'étudier les permutations (transformations) de $\widehat{X}$ correspondant aux homographies de $\widehat{\mathbb{C}}$.

Rappelons d'abord comment se traduisent certaines transformations géométriques simples de $X$ en termes d'affixes.

1) Translations.

Considérons une translation $M \mapsto M + \vec{u}$, où $\vec{u} = (a, b)$ est un vecteur de $\mathbb{R}^2$. En termes d'affixes, cette translation s'écrit: $z \mapsto z + \lambda$, où $\lambda = a + ib \in \mathbb{C}$.

2) Homothéties.

Considérons une homothétie de $X$, de centre $A$ et de rapport $k \in \mathbb{R}^*$. En termes d'affixes, cette homothétie se traduit ainsi: $z \mapsto a + k(z - a)$, où $a$ est l'affixe de $A$.

3) Rotations.

Considérons une rotation de $X$, de centre $A$ et d'angle $\theta \in \mathbb{R}$. En termes d'affixes, cette rotation se traduit ainsi: $z \mapsto a + e^{i\theta}(z - a)$, où $a$ est l'affixe de $A$.

4) Déplacements.

Un déplacement de $X$ est une isométrie affine de $X$ qui est directe, i.e. dont la partie linéaire est de déterminant 1. On sait que les déplacements de $X$ sont d'une part les translations et d'autre part les rotations. En termes d'affixes, ce sont donc les transformations du type $z \mapsto az + b$, où $a, b \in \mathbb{C}$ sont fixés et $|a| = 1$; il s'agit d'une translation si $a = 1$ et d'une rotation (non triviale) si $a \neq 1$.

5) Similitudes planes directes.

Par définition, une similitude plane directe de $X$ est la composée d'un déplacement et d'une homothétie. En termes d'affixes, on obtient toutes les transformations du type $z \mapsto az + b$, où $a \in \mathbb{C}^*$ et $b \in \mathbb{C}$ sont fixés et quelconques.

**Conclusion.** Notons $\mathrm{Sim}^+(X)$ le groupe des similitudes planes directes de $X$. C'est un sous-groupe de $\mathfrak{S}(X)$, nous le considèrerons en fait comme sous-groupe de $\mathfrak{S}(\widehat{X})$, en prolongeant toute similitude plane directe $f$ par $f(\infty) = \infty$. Ce qui précède montre que, si l'on identifie $\widehat{X}$ à $\widehat{\mathbb{C}}$, le groupe $\mathrm{Sim}^+(X)$ est identifié au groupe des transformations affines $z \mapsto az + b$ de la droite affine complexe $\mathbb{C}$. Compte tenu du lemme 3, on a donc:

$$\mathrm{Sim}^+(X) \;=\; \mathrm{PGL}_2(\mathbb{C})_\infty \;\subset\; \mathfrak{S}(\widehat{\mathbb{C}})\,. \tag{7}$$

Il nous faut maintenant voir à quelles transformations de $\widehat{X}$ correspondent les homographies de $\widehat{\mathbb{C}}$, ne fixant pas nécessairement $\infty$. Pour cela, on doit faire intervenir les droites (affines réelles) et les cercles de $X$. Rappelons d'abord ce que sont, en termes d'affixes, les équations de cercles ou droites de $X$:

**Proposition 12**. *Considérons les équations de la forme suivante:*

$$\alpha z\bar{z} + \beta z + \bar{\beta}\bar{z} + \gamma \;=\; 0\,, \tag{8}$$

*où $\alpha, \gamma \in \mathbb{R}$ et $\beta \in \mathbb{C}$ sont donnés et vérifient la condition suivante:*

$$\alpha\gamma \;<\; |\beta|^2\,. \tag{9}$$

1) *Si $\alpha = 0$, l'équation (8) est l'équation d'une droite (affine réelle) de $X$, et l'on obtient ainsi toutes les droites de $X$.*

2) *Si $\alpha \neq 0$, l'équation (8) est l'équation d'un cercle de $X$, et l'on obtient ainsi tous les cercles de $X$.*

*Démonstration*. Pour un point $M$ de $X$, notons $(x, y)$ ses coordonnées cartésiennes, de sorte que l'affixe de $M$ est $z = x + iy$. Soit d'abord $D$ une droite de $X$, définie par une équation:

$$ux + vy + w \;=\; 0\,, \tag{10}$$

où $u, v, w \in \mathbb{R}$ sont donnés et $(u, v) \neq (0, 0)$. Puisque $z = x + iy$ et $\bar{z} = x - iy$, l'équation (10) s'écrit: $u(z + \bar{z})/2 + v(z - \bar{z})/(2i) + w = 0$, ce qui équivaut à:

$$(u - iv)z + (u + iv)\bar{z} + 2w \;=\; 0\,.$$

En posant $\alpha = 0$, $\beta = u - iv$ et $\gamma = 2w$, on obtient bien l'équation (8), et (9) est vérifiée, car $\beta \neq 0$, donc $|\beta|^2 > 0$. Inversement, si $(\alpha, \beta, \gamma)$ vérifie (9) et si $\alpha = 0$, autrement dit si $\beta \in \mathbb{C}^*$, l'équation (8) n'est autre que (10), en posant $u = \mathrm{Re}\ \beta$, $v = -\,\mathrm{Im}\ \beta$ et $w = \gamma/2$. D'où l'assertion 1).

Soit ensuite $C(A, r)$ le cercle de centre $A \in X$ et de rayon $r > 0$. Notant $a$ l'affixe de $A$, l'équation de ce cercle, en termes d'affixes, est: $|z - a|^2 = r^2$, c'est-à-dire:

$$z\bar{z} - \bar{a}z - a\bar{z} + |a|^2 - r^2 \;=\; 0\,. \tag{11}$$

En posant $\alpha = 1$, $\beta = -\bar{a}$ et $\gamma = |a|^2 - r^2$, on retrouve l'équation (8); de plus (9) est vérifiée, car $|\beta|^2 - \alpha\gamma = |a|^2 - (|a|^2 - r^2) = r^2 > 0$.

Inversement, supposons que $(\alpha; \beta, \gamma) \in \mathbb{R} \times \mathbb{C} \times \mathbb{R}$ vérifie (9) et $\alpha \neq 0$. En divisant par $\alpha$ et en posant $a = -\bar{\beta}/\alpha$, l'équation (8) s'écrit:

$$z\bar{z} - \bar{a}z - a\bar{z} + \frac{\gamma}{\alpha} \;=\; 0\,.$$

De plus, compte tenu de la condition (9), on a:

$$|a|^2 - \frac{\gamma}{\alpha} \;=\; \frac{|\beta|^2 - \alpha\gamma}{\alpha^2} \;>\; 0\,.$$

Ainsi, en posant $r = \left(\sqrt{|\beta|^2 - \alpha\gamma}\right)/\alpha$, l'équation (8) n'est autre que (11), i.e. c'est l'équation du cercle $C(A, r)$, où $A \in X$ est le point d'affixe $a$. D'où l'assertion 2).

cqfd

Donnons maintenant une définition:

**Définition 5**. *On appelle* **pseudo-cercle** *toute partie $S$ de $\widehat{X}$ de l'une des deux formes suivantes:*

1) *$S = C(A, r)$, cercle de centre $A \in X$ et de rayon $r > 0$. On note $\mathcal{C}$ l'ensemble des cercles de $X$.*

2) *$S = \widehat{D} = D \cup \{\infty\}$, où $D$ est une droite (affine, réelle) de $X$. On note $\mathcal{D}$ l'ensemble de ces parties $\widehat{D}$ de $\widehat{X}$.*

*Enfin on note $\Pi$ l'ensemble des pseudo-cercles de $\widehat{X}$, c'est-à-dire la réunion disjointe de $\mathcal{C}$ et $\mathcal{D}$.*

**Proposition 13**. *Toute homographie de $\widehat{\mathbb{C}}$ laisse stable $\Pi$. En d'autres termes, dans l'opération naturelle du groupe $\mathrm{PGL}_2(\mathbb{C})$ sur l'ensemble des parties de $\widehat{\mathbb{C}} = \widehat{X}$, $\Pi$ est une partie stable.*

*Démonstration*. Notons $G$ le sous-groupe de $\mathfrak{S}(\widehat{\mathbb{C}})$ formé des permutations $\tau$ telles que $\tau(\Pi) = \Pi$. Il s'agit de démontrer l'inclusion $\mathrm{PGL}_2(\mathbb{C}) \subset G$. Comme $\mathrm{PGL}_2(\mathbb{C})$ est un sous-groupe de $\mathfrak{S}(\widehat{\mathbb{C}})$, il suffit de montrer que, pour toute homographie $h'$ de $\widehat{\mathbb{C}}$, on a $h'(\Pi) \subset \Pi$. C'est vrai si $h'$ est une translation ou une rotation, i.e. un déplacement, car on a alors séparément $h'(\mathcal{C}) \subset \mathcal{C}$ et $h'(\mathcal{D}) \subset \mathcal{D}$. La conclusion est la même si $h'$ est une homothétie donc, par composition, si $h'$ est une similitude plane directe. D'où l'inclusion:

$$\mathrm{Sim}^+(X) \;=\; \mathrm{PGL}_2(\mathbb{C})_\infty \;\subset\; G\,.$$

Supposons maintenant que $h'(\infty) = a \in \mathbb{C}$. Notons $h$ l'homographie $z \mapsto 1/z$ et $\tau$ la translation $z \mapsto z - a$. En posant $h'' = h \circ \tau \circ h'$, on a $h''(\infty) = h(0) = \infty$, donc $h'' \in G$, d'après ce qui précède; de même $\tau \in G$. Il suffit donc maintenant de prouver l'inclusion $h(\Pi) \subset \Pi$. Soit donc $S$ un pseudo-cercle de $\widehat{X}$, distinguons plusieurs cas.

1) Supposons d'abord que $S = \widehat{D}$, où $D$ est une droite de $X$ passant par l'origine 0. Ainsi $D$ a une équation de la forme $\beta z + \bar{\beta}\bar{z} = 0$, où $\beta \in \mathbb{C}^*$. Pour un point $M \in D$ distinct de 0, d'affixe $z \neq 0$, l'affixe $Z$ de $h(M)$ est $1/z$. En divisant l'égalité $\beta z + \bar{\beta}\bar{z} = 0$ par $|z|^2$, on obtient: $\bar{\beta}Z + \beta\bar{Z} = 0$. Il en résulte que $h(\widehat{D}) = \widehat{D'}$, où $D'$ est la symétrique de $D$ par rapport à l'axe des abscisses.

2) Supposons ensuite que $S = C(A, r)$ soit un cercle de centre $A$ et de rayon $r$, ne passant pas par 0: $r \neq |a|$, en notant $a$ l'affixe de $A$. Soit $M$ un point de $S$, d'affixe $z$, de sorte que $z$ vérifie l'égalité (11). Le point $h(M)$ appartient à $X$, il a pour affixe $Z = 1/z$. En divisant l'égalité (11) par $|z|^2$, on obtient l'égalité:

$$1 - aZ - \bar{a}\bar{Z} + (|a|^2 - r^2)Z\bar{Z} \;=\; 0\,.$$

D'après la proposition 12, c'est là l'équation d'un cercle $S'$ de $X$, ne passant pas par l'origine, et ainsi $h(S) = S' \in \mathcal{C} \subset \Pi$.

3) Supposons que $S = C(A, r)$ soit un cercle de centre $A$ et de rayon $r$, passant par 0: $r = |a|$, en notant $a$ l'affixe de $A$. Soit $M$ un point de $S$, d'affixe $z$, de sorte que $z$ vérifie l'égalité (11). Si $M = 0$, $h(M) = \infty$. Si $M \neq 0$, on a $z \neq 0$, le point $h(M)$ appartient à $X$, il a pour affixe $Z = 1/z$. En divisant l'égalité (11) par $|z|^2$, on obtient ici l'égalité:

$$1 - aZ - \bar{a}\bar{Z} \;=\; 0\,.$$

D'après la proposition 12, c'est là l'équation d'une droite $D'$ de $X$, ne passant pas par l'origine, et ainsi $h(S) = \widehat{D'} \in \mathcal{D} \subset \Pi$.

4) Supposons enfin que $S = \widehat{D}$, où $D$ est une droite de $X$ ne passant pas par l'origine 0. Ainsi $D$ a une équation de la forme $\beta z + \bar{\beta}\bar{z} + \gamma = 0$, où $\beta \in \mathbb{C}^*$ et $\gamma \in \mathbb{R}^*$. Pour un point $M \in D$, d'affixe $z \neq 0$, l'affixe $Z$ de $h(M)$ est $1/z$. En divisant l'égalité $\beta z + \bar{\beta}\bar{z} + \gamma = 0$ par $|z|^2$, on obtient:

$$\bar{\beta}Z + \beta\bar{Z} + \gamma Z\bar{Z} \;=\; 0\,.$$

D'après la proposition 12, c'est là l'équation d'un cercle $C'$ de $X$, passant par l'origine. Lorsque $M$ décrit $D$, on obtient ainsi tous les points de $C'$, sauf l'origine. Mais $h(\infty) = 0$, et donc $h(S) = C' \in \mathcal{C} \subset \Pi$.

cqfd

Le résultat suivant est évident:

**Proposition 14**. *Soient $A, B, C$ trois points de $\widehat{X}$ distincts. Il existe un unique pseudo-cercle passant par ces trois points.*

*Démonstration*. Supposons d'abord que $A, B, C \in X$. Deux cas sont possibles. Si $A, B, C$ sont alignés, aucun cercle ne passe par $A, B, C$, et il existe une seule droite de $X$ passant par $A, B, C$, à savoir la droite $AB$! Si $A, B, C$ ne sont pas alignés, il n'existe aucune droite de $X$ passant par ces trois points (!); de plus $ABC$ est un vrai triangle de $X$, et l'on sait qu'il existe un unique cercle passant par $A, B, C$, à savoir le cercle circonscrit à ce triangle.

Supposons maintenant (par exemple) que $C = \infty$. Aucun cercle de $X$ ne passe par $\infty$; la seule droite $D$ de $X$ telle que $A, B, C \in \widehat{D}$, soit $A, B \in D$, est la droite $AB$. D'où la conclusion.

On peut raisonner autrement. Notons $a, b, c \in \widehat{\mathbb{C}}$ les affixes respectives de $A, B, C$ (éventuellement $\infty$). Soit $h$ l'unique homographie de $\widehat{\mathbb{C}}$ qui applique $a, b, c$ sur $\infty, 0, 1$ respectivement (cf. la définition 3, ou le théorème 1). Il existe évidemment un seul $S \in \Pi$ passant par $\infty, 0, 1$, à savoir $S = \widehat{D}$, où $D$ est l'axe des abscisses. Compte tenu de la proposition précédente, $h^{-1}(S)$ est l'unique pseudo-cercle passant par $A, B, C$.

cqfd

Voici une application géométrique importante de la notion de birapport.

**Théorème 3**. *Soient $A, B, C, D \in \widehat{X}$ quatre points distincts et $a, b, c, d \in \widehat{\mathbb{C}}$ leurs affixes respectives. Pour que $A, B, C, D$ appartiennent à un même pseudo-cercle, il faut et il suffit que le birapport $[a, b; c, d]$ soit* **réel**. *En particulier, si ces quatre points appartiennent à $X$, ils sont cocycliques ou alignés si et seulement si $[a, b; c, d]$ est réel.*

*Démonstration*. Posons $\omega = [a, b; c, d] \in \mathbb{C} \setminus \{0, 1\}$. Soit $h$ l'unique homographie de $\widehat{\mathbb{C}}$ appliquant $a, b, c$ sur $\infty, 0, 1$ respectivement. Par définition, $\omega = h(d)$. D'après la proposition 13, $A, B, C, D \in \widehat{X}$ appartiennent à un même pseudo-cercle, i.e. $a, b, c, d \in \widehat{\mathbb{C}}$ appartiennent à un même élément de $\Pi$, si et seulement si c'est le cas pour $h(a), h(b), h(c), h(d)$, c'est-à-dire pour $\infty, 0, 1, \omega$. Comme on l'a vu, le seul pseudo-cercle passant par $\infty, 0, 1$ est $\widehat{D}$, où $D$ est l'axe des abscisses. Ainsi $A, B, C, D$ appartiennent à un même pseudo-cercle si et seulement si $\omega \in D$, ce qui revient à dire que $\omega$ est réel. D'où la première assertion du théorème. La seconde assertion en est une conséquence immédiate.

cqfd

**Remarque.** Soient $A, B, C, D \in X$ quatre points distincts, notons $a, b, c, d$ leurs affixes respectives. Notons par exemple $(\overrightarrow{CB}, \overrightarrow{CA}) \in \mathbb{R}$ une mesure (définie modulo $2\pi$) de l'angle orienté des vecteurs $\overrightarrow{CB}$ et $\overrightarrow{CA}$. On sait que

$$\arg\left(\frac{c-a}{c-b}\right) \;=\; (\overrightarrow{CB}, \overrightarrow{CA}) \bmod 2\pi\,,$$

en notant $\arg(z)$ un argument (défini modulo $2\pi$) d'un nombre complexe $z \neq 0$. De même

$$\arg\left(\frac{d-a}{d-b}\right) \;=\; (\overrightarrow{DB}, \overrightarrow{DA}) \bmod 2\pi\,.$$

Compte tenu de l'expression explicite du birapport (formule (3)), il vient:

$$\arg([a, b; c, d]) \;=\; (\overrightarrow{CB}, \overrightarrow{CA}) - (\overrightarrow{DB}, \overrightarrow{DA}) \bmod 2\pi\,.$$

Or $[a, b; c, d]$ est réel si et seulement si son argument est nul modulo $\pi$, i.e. si:

$$(\overrightarrow{CB}, \overrightarrow{CA}) \;=\; (\overrightarrow{DB}, \overrightarrow{DA}) \bmod \pi\,.$$

Notons maintenant $(CA, CB)$ une mesure (définie modulo $\pi$) de l'angle orienté des *droites* $CA$ et $CB$. Ce qui précède montre que l'égalité

$$(CA, CB) \;=\; (DA, DB) \bmod \pi \tag{12}$$

est une condition nécessaire et suffisante pour que les quatre points $A, B, C, D$ soient cocycliques ou alignés (**théorème de l' arc capable**).

Voir dans les compléments des applications du théorème 3.

## Groupe circulaire

On garde les notations précédentes, notamment $X$ est le plan affine euclidien $\mathbb{R}^2$ standard, et $\widehat{X} = X \cup \{\infty\}$ est identifié à la droite projective complexe standard $\widehat{\mathbb{C}}$. Notons $\sigma$ la symétrie orthogonale par rapport à l'axe des abscisses, prolongée par $\sigma(\infty) = \infty$. En termes d'affixes, $\sigma$ se traduit par la conjugaison $z \mapsto \bar{z}$.

**Proposition 15**.

*1) Comme élément de* $\mathfrak{S}(\widehat{\mathbb{C}})$, $\sigma$ *normalise* $\mathrm{PGL}_2(\mathbb{C})$. *Plus précisément, si* $h$ *est l'homographie* $z \mapsto \dfrac{az+b}{cz+d}$ , *sa conjuguée* $\sigma \circ h \circ \sigma^{-1}$ *est l'homographie* $z \mapsto \dfrac{\bar{a}z+\bar{b}}{\bar{c}z+\bar{d}}$.

*2) La réunion de* $\mathrm{PGL}_2(\mathbb{C})$ *et de* $\mathrm{PGL}_2(\mathbb{C})\,\sigma$ *est un sous-groupe* $\Gamma$ *de* $\mathfrak{S}(\widehat{\mathbb{C}})$.

*Démonstration*. Soient donc $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$ et $h = [M]$ l'homographie correspondante. Notons $\bar{h}$ l'homographie correspondant à $\overline{M}$, conjuguée de $M$. Pour l'assertion 1), il s'agit de vérifier que $\sigma \circ h = \bar{h} \circ \sigma$, i.e. de vérifier, pour tout $z \in \widehat{\mathbb{C}}$, l'égalité suivante:

$$\overline{\left(\frac{az+b}{cz+d}\right)} \;=\; \frac{\bar{a}\bar{z}+\bar{b}}{\bar{c}\bar{z}+\bar{d}}.$$

C'est évident, en tenant compte des cas particuliers donnés dans la proposition 2.

L'assertion 2) résulte alors du fait suivant: soient $(G, \times)$ un groupe, $\sigma$ un élément d'ordre 2 de $G$ et $H$ un sous-groupe de $G$. Si $\sigma$ normalise $H$, i.e. si $\sigma H \sigma^{-1} = H$, la réunion $H \cup H\sigma$ est un sous-groupe de $G$. C'est là une conséquence évidente de l'égalité $\sigma H = H\sigma$.

cqfd

**Définition 6**. *Le sous-groupe* $\Gamma$ *de* $\mathfrak{S}(\widehat{\mathbb{C}})$ *défini dans la proposition précédente est appelé* **groupe circulaire**. *Les éléments de* $\mathrm{PGL}_2(\mathbb{C})\,\sigma$, *i.e. les transformations de* $\widehat{\mathbb{C}}$ *de la forme* $z \mapsto \dfrac{a\bar{z}+b}{c\bar{z}+d}$ , *où* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{C})$, *sont appelées* **antihomographies** *de* $\widehat{\mathbb{C}}$.

**Théorème 4**. *Le groupe circulaire est formé des permutations de* $\widehat{X} = \widehat{\mathbb{C}}$ *laissant stable l'ensemble* $\Pi$ *des pseudo-cercles de* $\widehat{X}$.

*Démonstration*. Notons $\Gamma'$ le sous-groupe de $\mathfrak{S}(\widehat{\mathbb{C}})$ formé des permutations $f$ telles que $f(\Pi) = \Pi$. D'après la proposition 13, $\mathrm{PGL}_2(\mathbb{C})$ est un sous-groupe de $\Gamma'$. Il est clair que $\sigma \in \Gamma'$, car $\sigma$ laisse stables $\mathcal{D}$ et $\mathcal{C}$. Ainsi $\Gamma \subset \Gamma'$.

Soit donc $f \in \Gamma'$. Il existe une unique homographie $h$ de $\widehat{\mathbb{C}}$ appliquant $f(\infty), f(0), f(1)$ sur $\infty, 0, 1$ respectivement. Quitte à remplacer $f$ par $h \circ f$, on peut donc supposer que $f$ laisse fixes les points $\infty, 0, 1$. Nous allons montrer que $f$ est égal soit à l'identité soit à $\sigma$, en procédant en plusieurs étapes. Commençons par des remarques évidentes:

1. si $D$ est une droite de $X$, $f(D)$ est une droite de $X$: en effet, $f$ fixe $\infty$, et les pseudo-cercles contenant $\infty$ sont les $\widehat{D}$, $D$ droite de $X$;

2. si $D, D'$ sont deux droites parallèles, les droites $f(D), f(D')$ sont parallèles (parce que $f$ est bijective);

3. si $C$ est un cercle de $X$, $f(C)$ est aussi un cercle: en effet $C \in \Pi$, donc $f(C) \in \Pi$, et l'on applique 1;

4. si une droite $D$ et un cercle $C$ sont tangents, i.e. ont un seul point d'intersection, $f(D)$ et $f(C)$ sont tangents, idem pour deux cercles tangents.

Étape 1.

Soit $C$ un cercle. Deux points distincts $A, B \in C$ sont diamétralement opposés sur $C$ si et seulement si les tangentes à $C$ en $A$ et $B$ sont parallèles. D'après les propriétés 1 à 4, il en résulte que, si $A, B$ sont deux points diamétralement opposés de $C$, $f(A)$ et $f(B)$ sont deux points diamétralement opposés du cercle $f(C)$.

Soit maintenant $\Omega$ le centre de $C$. Toute droite $D$ passant par $\Omega$ coupe $C$ en deux points diamétralement opposés de $C$, et cette propriété caractérise le point $\Omega$. On en déduit que $f(\Omega)$ est le centre du cercle $f(C)$, ce qui n'était pas évident a priori.

Étape 2.

Montrons que $f$ conserve les milieux. Soient donc $A, B \in X$ deux points distincts et $M$ leur milieu. Soit $C$ le cercle de centre $M$ passant par $A$; il passe par $B$, et $A, B$ sont diamétralement opposés sur $C$. D'après l'étape 1, $f(A), f(B)$ sont diamétralement opposés sur le cercle $f(C)$. Le milieu de $f(A)f(B)$ est donc le centre de $f(C)$, à savoir $f(M)$.

Soient $A, B \in X$ deux points distincts et $A'$ le symétrique de $A$ par rapport à $B$. C'est le seul point $M \neq A$ tel que $B$ soit milieu de $AM$. Vu ce qui précède, $f(A')$ est donc le symétrique de $f(A)$ par rapport à $f(B)$.

Étape 3.

Montrons que $f$ conserve l'orthogonalité des droites. Soient donc $D, D'$ deux droites orthogonales, se coupant en un point $\Omega$. Soit $A' \in D'$, $A' \neq \Omega$. Soit $C'$ un cercle de centre $A'$ et de rayon $r > A'\Omega$. Il coupe $D$ en deux points distincts $A, B$ de milieu $\Omega$. Alors $f(C')$ est un cercle de centre $f(A')$, coupant $f(D)$ en $f(A), f(B)$, et $f(\Omega)$ est le milieu de $f(A)f(B)$. Puisque les distances $f(A')f(A)$ et $f(A')f(B)$ sont égales, $f(A')$ appartient à la médiatrice $\Delta$ de $f(A)f(B)$, laquelle médiatrice passe par $f(\Omega)$ et est orthogonale à $f(D) = f(A)f(B)$. Ainsi $\Delta = f(D')$, donc $f(D')$ est orthogonale à $f(D)$.

Soient $0, I, J, J' \in X$ les points d'affixes respectives $0, 1, i, -i$. Puisque $f(0) = 0$ et $f(I) = I$, la droite $OI$ (axe des $x$) est stable par $f$, donc l'axe des $y$, c'est-à-dire $OJ$, l'est aussi (vu ce qui précède). De plus le cercle $C$ de centre 0 et de rayon 1 est stable par $f$, et il coupe $OJ$ en $J, J'$. Il en résulte que $\{J, J'\}$ est stable par $f$. Quitte à remplacer $f$ par $f \circ \sigma$, on peut supposer que $f(J) = J$. Le but est alors de montrer que $f$ est l'identité.

Étape 4.

Notons $\Phi$ l'ensemble des points de $X$ fixés par $f$. On peut aussi considérer $\Phi$ comme ensemble des points fixes de $f$ dans $\mathbb{C}$. Pour simplifier, pour tout $z \in \mathbb{C}$, notons $M(z) \in X$ le point d'affixe $z$. Observons que, pour tout $n \in \mathbb{Z}$, $M(n+1)$ est le symétrique de $M(n-1)$ par rapport à $M(n)$. Comme $\Phi$ contient $0, I$, on en déduit, d'après l'étape 2, que $\Phi$ contient $\mathbb{Z}$ (on montre par récurrence sur $n \in \mathbb{N}$ que $n \in \Phi$ et $-n \in \Phi$).

Montrons que $\Phi$ contient l'ensemble $T$ des nombres dyadiques. Pour cela prouvons, par récurrence sur l'entier $m \geq 0$, que, pour tout $u \in \mathbb{Z}$, $u/2^m \in \Phi$. C'est vrai pour $m = 0$ puisque $\mathbb{Z} \subset \Phi$. Supposons que cela soit vrai pour un certain entier $m \geq 0$, et soit $u \in \mathbb{Z}$. Si $u$ est pair, on écrit $u = 2v$, et alors $u/2^{m+1} = v/2^m \in \Phi$ vu l'hypothèse de récurrence. Si $u$ est impair, on écrit $u = 2v + 1$, et l'on remarque que $M(u/2^{m+1})$ est le milieu du segment joignant $M(v/2^m)$

et $M((v+1)/2^m)$; ces deux points étant fixés par $f$ vu l'hypothèse de récurrence, $M(u/2^{m+1})$ l'est aussi, d'après l'étape 2. Puisque $i \in \Phi$, on voit de même que, pour tout $t \in T$, $ti \in \Phi$.

Soient $x, y \in \mathbb{R}$ tels que $x$ et $iy$ appartiennent à $\Phi$. Alors $z = x + iy \in \Phi$. En effet, $f$ laisse stable l'axe des $x$ et fixe $M(x)$, donc $f$ laisse stable la droite verticale d'abscisse $x$. Pour la même raison $f$ laisse stable la droite horizontale d'ordonnée $y$. Ces deux droites se coupant en $M(z)$, $f$ laisse fixe $M(z)$, i.e. $z \in \Phi$. Ainsi $\Phi$ contient tout point dont les coordonnées sont dans $T$.

Étape 5.

Soient $P, Q, R \in X$ trois points distincts alignés. Observons que $R$ appartient à $]P, Q[$ si et seulement si toute doite passant par $R$ coupe le cercle $C$ de diamètre $AB$. Il en résulte que, si $R \in ]P, Q[$, alors $f(R) \in ]f(P), f(Q)[$.

Soit $x \in \mathbb{R}$. Il existe deux suites $(t_n)_{n\geq 0}$ et $(t'_n)_{n\geq 0}$ de $T$ telles que la première soit strictement croissante, la deuxième strictement décroissante, et telles que

$$\bigcap_{n\geq 0} \,]\, t_n, t'_n \,[ \;=\; \{x\}\,.$$

D'après l'étape 4, $f(t_n) = t_n$ et $f(t'_n) = t'_n$ pour tout $n \in \mathbb{N}$. On en déduit donc que $f(x) = x$. Ainsi $\mathbb{R} \subset \Phi$. Le même raisonnement, appliqué à l'axe des ordonnées, montre que $i\,\mathbb{R} \subset \Phi$. La fin de l'étape 4 montre alors que $\Phi = \mathbb{C}$, autrement dit $f$ est l'identité.

cqfd

Le résultat suivant montre que les pseudo-cercles de $\widehat{X}$ correspondent simplement, via la projection stéréographique, aux cercles ordinaires tracés sur la sphère $S^2$.

**Proposition 16**. *Soit $s : S^2 \longrightarrow \widehat{X}$ la projection stéréographique. Les pseudo-cercles de $\widehat{X}$ sont exactement les images par $s$ des cercles tracés sur $S^2$.*

*Démonstration*. Rappelons qu'un cercle tracé sur $S^2$ est l'intersection avec $S^2$ d'un plan affine $P$ de $\mathbb{R}^3$ tel que la distance de 0 à $P$ soit $< 1$. Considérons un tel plan $P$, donné par l'équation:

$$\alpha x + \beta y + \gamma z + \delta \;=\; 0\,, \tag{13}$$

où $\alpha, \beta, \gamma, \delta \in \mathbb{R}$ et $(\alpha, \beta, \gamma) \neq (0, 0, 0)$. Il est classique que la distance $d(0, P)$ de 0 à $P$ est donné par la formule suivante:

$$d(0, P)^2 \;=\; \frac{\delta^2}{\alpha^2 + \beta^2 + \gamma^2}\,.$$

Compte tenu de l'hypothèse, on a donc:

$$\delta^2 \;<\; \alpha^2 + \beta^2 + \gamma^2\,. \tag{14}$$

Il s'agit d'identifier l'image $S$ du cercle $C = P \cap S^2$ par $s$. Distinguons deux cas, suivant que $P$ passe ou ne passe pas par le pôle nord $N$. Notons qu'un point $R \in X$ de coordonnées $(x, y)$ appartient à $S$ si et seulement si $s^{-1}(R) \in P$. Compte tenu de la formule (6) donnant la réciproque de $s$, cela revient à dire que $x, y$ vérifient l'égalité:

$$2\alpha x + 2\beta y + \gamma(x^2 + y^2 - 1) + \delta(x^2 + y^2 + 1) \;=\; 0\,. \tag{15}$$

Cas 1: P passe par $N$.

On a donc $\gamma+\delta=0$. Tout d'abord $S$ contient $\infty$. Soit $D=S\setminus\{\infty\}$. D'après (15), $D$ a pour équation: $\alpha x+\beta y+\delta=0$. Par hypothèse, $\alpha^2+\beta^2>0$, i.e. $(\alpha,\beta)\neq(0,0)$. Ainsi $D$ est une droite de $X$. En faisant varier $(\alpha,\beta,\delta)\in\mathbb{R}^3$ de sorte que $(\alpha,\beta)\neq(0,0)$ (et en posant $\gamma=-\delta$), on obtient ainsi toutes les droites de $X$.

Cas 2: P ne passe pas par $N$.

On a donc $\gamma+\delta\neq 0$, et l'on peut supposer que $\gamma+\delta=1$, quitte à diviser l'équation (13) par $\gamma+\delta$. L'équation (15) s'écrit alors:

$$x^2+y^2+2\alpha x+2\beta y+(\alpha^2+\beta^2) \;=\; \alpha^2+\beta^2-(\delta-\gamma)\,.$$

Puisque $\gamma+\delta=1$, la condition (14) s'écrit $\delta-\gamma<\alpha^2+\beta^2$, ou encore $2\delta<\alpha^2+\beta^2+1$. Il en résulte que $S$ est le cercle de centre $A$ et de rayon $r$, où $A$ a pour coordonnées $-\alpha,-\beta$, et où $r>0$ est donné par l'égalité

$$r^2 \;=\; \alpha^2+\beta^2-(\delta-\gamma) \;=\; \alpha^2+\beta^2-(2\delta-1)\,.$$

Inversement, le point $A\in X$ de coordonnées $-\alpha,-\beta$ étant fixé, faisons varier $\delta$ dans l'intervalle $]-\infty,(\alpha^2+\beta^2+1)/2[$. Pour tout $\delta$ dans cet intervalle, posons $\gamma=1-\delta$ et $r=(\alpha^2+\beta^2-(2\delta-1))^{1/2}$. Alors $r$ décrit $]0,+\infty[$. Il en résulte que l'on obtient, en prenant les images par $s$, tous les cercles de $X$ de centre $A$, d'où la proposition.

cqfd

La définition et le théorème suivant justifient la terminologie de «groupe circulaire».

**Définition 7**. *On appelle* **groupe circulaire** *de $S^2$ le sous-groupe de $\mathfrak{S}(S^2)$ formé des permutations de $S^2$ laissant stable l'ensemble des cercles tracés sur $S^2$. Ce groupe est noté* $\mathrm{Circ}(S^2)$.

Le théorème suivant est une simple conséquence de la proposition précédente et du théorème 4.

**Théorème 5**. *Le groupe* $\mathrm{Circ}(S^2)$ *est formé des composés $s^{-1}\circ h\circ s$, où $h$ décrit le groupe circulaire $\Gamma\subset\mathfrak{S}(\widehat{\mathbb{C}})$, i.e. $h$ est soit une homographie soit une antihomographie de $\widehat{\mathbb{C}}$.*

**Remarque.** Considérons le groupe $\mathrm{SO}(\mathbb{R}^3)$ des rotations de $\mathbb{R}^3$. Il laisse stable $S^2$, et il opère évidemment fidèlement sur $S^2$. De plus, l'image par une rotation de $\mathbb{R}^3$ d'un cercle tracé sur $S^2$ est encore un cercle tracé sur $S^2$. On obtient ainsi un morphisme injectif de $\mathrm{SO}(\mathbb{R}^3)$ dans $\mathrm{Circ}(S^2)$ d'où, par composition avec $s$ et $s^{-1}$, un morphisme injectif $\varphi:\mathrm{SO}(\mathbb{R}^3)\to\Gamma$. En fait l'image de $\varphi$ est contenue dans $\mathrm{PGL}_2(\mathbb{C})$, et ainsi $\mathrm{SO}(\mathbb{R}^3)$ se plonge naturellement dans $\mathrm{PGL}_2(\mathbb{C})$. Pour le voir, on peut raisonner comme suit.

- Les éléments d'ordre 2 de $\mathrm{SO}(\mathbb{R}^3)$ sont les demi-tours (symétries orthogonales par rapport aux droites de $\mathbb{R}^3$ passant par l'origine). Ces demi-tours forment une classe de conjugaison de $\mathrm{SO}(\mathbb{R}^3)$, qui engendre $\mathrm{SO}(\mathbb{R}^3)$. Par ailleurs $\mathrm{PGL}_2(\mathbb{C})$ est un sous-groupe distingué de $\Gamma$ (il est d'indice 2). Pour conclure, il suffit donc d'expliciter l'image par $\varphi$ du demi-tour d'axe $Oz$, et de montrer que cette image est une homographie.

- Soit donc $r$ le demi-tour d'axe O$z$, défini par $(x, y, z) \mapsto (-x, -y, z)$. Les formules (5) et (6) montrent que $s^{-1} \circ r \circ s$ est la symétrie par rapport à l'origine de $X$, i.e. se traduit par l'homographie $z \mapsto -z$ de $\widehat{\mathbb{C}}$. Ainsi $\varphi(r) \in \mathrm{PGL}_2(\mathbb{C})$, d'où la conclusion.

## Point de vue analytique

Soit $U$ un ouvert connexe de $\mathbb{C}$. Considérons une application $f : U \to \widehat{\mathbb{C}}$. On sait que $f$ est une **fonction méromorphe** sur $U$ si, pour tout point $a \in U$, il existe un réel $r > 0$ et une série de Laurent

$$\sum_{-\infty}^{+\infty} a_n (z-a)^n \qquad (*)$$

vérifiant les conditions suivantes:

1. l'ensemble des indices $n < 0$ tels que $a_n \neq 0$ est fini, et il est non vide si et seulement si $f(a) = \infty$;
2. pour tout $z \in \mathbb{C}$ tel que $0 < |z - a| < r$, on a $z \in U$, la série $(*)$ converge et a pour somme $f(z)$, en particulier $f(z) \neq \infty$.

Si $a_n = 0$ pour tout $n < 0$, $f$ est *holomorphe* en $a$. Sinon, soit $m$ le plus grand entier $> 0$ tel que $a_{-m} \neq 0$. On dit alors que $a$ est pôle d'ordre $m$ de $f$. L'ensemble des pôles de $f$, c'est-à-dire $f^{-1}(\infty)$, est une partie *discrète* de $U$. Avec cette définition, on voit immédiatement que $f : U \to \widehat{\mathbb{C}}$ est continue ($\widehat{\mathbb{C}}$ étant muni de la topologie définie précédemment). Par ailleurs l'ensemble $\mathcal{M}(U)$ des fonctions méromorphes sur $U$ est de manière naturelle un corps, que l'on peut identifier, bien que ce ne soit pas évident, au corps des fractions de l'anneau des fonctions holomorphes de $U$ dans $\mathbb{C}$. Comme exemples de fonctions méromorphes sur $\mathbb{C}$, il y a les fractions rationnelles $z \mapsto P(z)/Q(z)$, où $P, Q \in \mathbb{C}[X]$ sont premiers entre eux et $Q \neq 0$, les pôles de cette fonction étant les racines de $Q$.

Soit maintenant $f$ une application de $\widehat{\mathbb{C}}$ dans $\widehat{\mathbb{C}}$. Nous dirons que $f$ est une fonction méromorphe sur $\widehat{\mathbb{C}}$ si

1. la restriction de $f$ à $\mathbb{C}$ est méromorphe;
2. l'application $z \mapsto f(1/z)$ de $\mathbb{C}$ dans $\widehat{\mathbb{C}}$ est méromorphe.

Ici $z \mapsto 1/z$ est une homographie de $\widehat{\mathbb{C}}$, donc une permutation de $\widehat{\mathbb{C}}$, échangeant $\infty$ et 0.

Par exemple, soit $f : z \mapsto P(z)/Q(z)$ une fraction rationnelle, $P$ et $Q$ étant comme ci-dessus. A priori $f$ est une fonction méromorphe sur $\mathbb{C}$. Prolongeant la en définissant $f(\infty)$ comme suit. Si $P = 0$, on pose $f(\infty) = 0$. Si $P \neq 0$, écrivons:

$$P \;=\; a_m X^m + \cdots + a_0 \quad , \quad Q \;=\; b_n X^n + \cdots + b_0 \,,$$

où $m, n \in \mathbb{N}$, $a_0, \ldots, a_m, b_0, \ldots, b_n \in \mathbb{C}$ et $a_m \neq 0$, $b_n \neq 0$. On pose:

$$f(\infty) \;=\; \begin{cases} \infty & \text{si } m > n \,, \\ 0 & \text{si } m < n \,, \\ a_m/b_n & \text{si } m = n \,. \end{cases}$$

Montrons que $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ est méromorphe. Cela revient à dire que la fonction $g : z \mapsto f(1/z)$ est méromorphe sur $\mathbb{C}$. C'est clair si $P = 0$. Sinon, considérons les polynômes suivants:

$$P_1 \;=\; a_0X^m + \cdots + a_m \;=\; X^mP(1/X)\;,\quad Q_1 \;=\; b_0X^n + \cdots + b_n \;=\; X^nQ(1/X)\,.$$

Si $z \in \mathbb{C}^*$ et si $1/z$ n'est pas racine de $Q$, i.e. si $Q_1(z) \neq 0$, il vient:

$$g(z) \;=\; \frac{a_mz^{-m} + \cdots + a_0}{b_nz^{-n} + \cdots + b_0} \;=\; z^{n-m}\,\frac{P_1(z)}{Q_1(z)} \;=\; F(z)$$

où $F$ est la fraction rationnelle $X^{n-m}P_1/Q_1$. Si $z \in \mathbb{C}^*$ est racine de $Q_1$, i.e. si $Q(1/z) = 0$, $g(z) = f(1/z) = \infty$ par définition. Enfin la définition de $f(\infty)$ montre que $g(0) = f(\infty) = F(\infty)$. Ainsi $g : \mathbb{C} \to \widehat{\mathbb{C}}$ n'est autre que la fraction rationnelle $F$, elle est donc méromorphe.

En conclusion, toute fraction rationnelle définit une fonction méromorphe sur $\widehat{\mathbb{C}}$. La réciproque est vraie, comme le montre le théorème suivant. Noter que par contre, sur $\mathbb{C}$, il y a des fonctions méromorphes qui ne sont pas des fractions rationnelles, par exemple l'exponentielle!

**Théorème 6**.

1. *Les fonctions méromorphes de $\widehat{\mathbb{C}}$ dans $\widehat{\mathbb{C}}$ sont exactement les fractions rationnelles.*

2. *Les fonctions méromorphes bijectives de $\widehat{\mathbb{C}}$ sur $\widehat{\mathbb{C}}$ sont exactement les homographies de $\widehat{\mathbb{C}}$.*

*Démonstration*. Soit d'abord $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ une fonction méromorphe. Posons $S = f^{-1}(\infty)$. Puisque $f$ est méromorphe sur $\mathbb{C}$, $S \cap \mathbb{C}$ est une partie discrète de $\mathbb{C}$. Puisque $z \mapsto f(1/z)$ est méromorphe sur $\mathbb{C}$, l'ensemble des $z \in \mathbb{C}$ tels que $1/z \in S$ est aussi une partie discrète de $\mathbb{C}$. Vu la définition de la topologie de $\widehat{\mathbb{C}}$, il en résulte que $S$ est une partie discrète de $\widehat{\mathbb{C}}$. Comme $\widehat{\mathbb{C}}$ est compact, $S$ est finie.

Soient $\alpha_1, \ldots, \alpha_r$ les pôles de $f$ dans $\mathbb{C}$ et $m_1, \ldots, m_r$ leurs ordres respectifs. Considérons le polynôme suivant (égal à 1 si $r = 0$):

$$P \;=\; (X - \alpha_1)^{m_1} \cdots (X - \alpha_r)^{m_r}\,.$$

La fonction $Pf$ est encore méromorphe sur $\widehat{\mathbb{C}}$, mais elle est holomorphe sur $\mathbb{C}$, elle est donc la somme d'une série entière $\sum_{n\geq 0} a_nz^n$, de rayon de convergence infini. Pour tout $z \in \mathbb{C}^*$, on a donc:

$$(Pf)(1/z) \;=\; \sum_{n=0}^{+\infty} a_nz^{-n}\,.$$

Mais $z \mapsto (Pf)(1/z)$ est méromorphe sur $\mathbb{C}$, donc l'ensemble des $n \in \mathbb{N}$ tels que $a_n \neq 0$ est fini, autrement dit $Pf$ est un polynôme. Il en résulte que $f$ est une fraction rationnelle, ce qui prouve l'assertion 1.

Soit maintenant $F$ une fraction rationnelle non nulle: $F = P/Q$, où $P, Q \in \mathbb{C}[X]$ sont non nuls, premiers entre eux, de degrés $m, n$ respectivement. Il s'agit de voir que $F : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ est bijective si et seulement si $F$ est une homographie, i.e. si $\max(m, n) = 1$. La suffisance est évidente: les homographies sont des permutations de $\widehat{\mathbb{C}}$. Pour la nécessité, raisonnons par contraposition, en supposant $p = \max(m, n) \geq 2$. Le polynôme $PQ' - QP'$ n'est pas nul, il

existe donc un $t \in \mathbb{C}^*$ tel que $P - tQ$ soit de degré $p$ et que, d'autre part, pour toute racine $z$ de $PQ' - QP'$, on ait $P(z) - tQ(z) \neq 0$. Choisissons un tel $t$. Toute racine $z$ de $P - tQ$ est alors simple: sinon on aurait $P(z) - tQ(z) = 0$ et $P'(z) - tQ'(z) = 0$, d'où $P(z)Q'(z) - Q(z)P'(z) = 0$, contredisant le choix de $t$. Ainsi le polynôme $P - tQ$ a $p$ racines distinctes, qui ne sont pas racines de $Q$, et donc $F^{-1}(t)$ est de cardinal $\geq p$. Il en résulte que $F$ n'est pas injective.

cqfd

## Compléments

Commençons par donner une application du théorème 3.

**Proposition 17 (théorème des six birapports)**. *Soient $A, B, C, D, E, F, G, H$ huit points de $\widehat{X}$ distincts. Considérons les conditions suivantes:*

- *les points $B, C, F, G$ appartiennent à un même pseudo-cercle;*
- *les points $C, D, G, H$ appartiennent à un même pseudo-cercle;*
- *les points $A, D, E, H$ appartiennent à un même pseudo-cercle;*
- *les points $A, B, E, F$ appartiennent à un même pseudo-cercle;*
- *les points $E, F, G, H$ appartiennent à un même pseudo-cercle;*
- *les points $A, B, C, D$ appartiennent à un même pseudo-cercle.*

*Si cinq de ces conditions sont satisfaites, la sixième l'est aussi.*

*Démonstration*. Notons $a, b, \ldots, h$ les affixes de ces points. Le nom du théorème vient du calcul ci-dessous du produit de six birapports, à l'aide de la proposition 3:

$$[a,c;b,d]\,[a,f;e,b]\,[a,h;d,e]\,[c,f;b,g]\,[c,h;g,d]\,[f,h;e,g] \;=$$

$$\frac{\overbrace{(b-a)}^{1}\;\overbrace{(d-c)}^{2}}{\underbrace{(b-c)}_{7}\;\underbrace{(d-a)}_{5}} \times \frac{\overbrace{(e-a)}^{3}\;\overbrace{(b-f)}^{4}}{\underbrace{(e-f)}_{11}\;\underbrace{(b-a)}_{1}} \times \frac{\overbrace{(d-a)}^{5}\;\overbrace{(e-h)}^{6}}{\underbrace{(d-h)}_{10}\;\underbrace{(e-a)}_{3}}$$

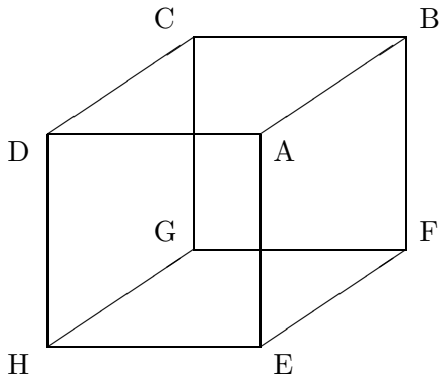
$$\times \frac{\overbrace{(b-c)}^{7}\;\overbrace{(g-f)}^{8}}{\underbrace{(b-f)}_{4}\;\underbrace{(g-c)}_{9}} \times \frac{\overbrace{(g-c)}^{9}\;\overbrace{(d-h)}^{10}}{\underbrace{(g-h)}_{12}\;\underbrace{(d-c)}_{2}} \times \frac{\overbrace{(e-f)}^{11}\;\overbrace{(g-h)}^{12}}{\underbrace{(e-h)}_{6}\;\underbrace{(g-f)}_{8}} \;=\; 1\,.$$

La démonstration du fait que le produit de ces six birapports soit égal à 1 est peu subtile: chacune des douze parenthèses notées ci-dessus $1, \ldots, 12$ apparaît deux fois, une fois au numérateur et une fois au dénominateur!

Parmi les six birapports dont on a fait le produit, cinq sont réels: cela traduit les hypothèses faites, en vertu du théorème 3. Le dernier de ces birapports est donc lui aussi réel, d'où la conclusion, toujours en vertu du théorème 3.

cqfd

Donnons une représentation «graphique» ou mnémotechnique de ce théorème. Représentons les huit points donnés par les sommets d'un cube, comme dans la figure ci-dessous.

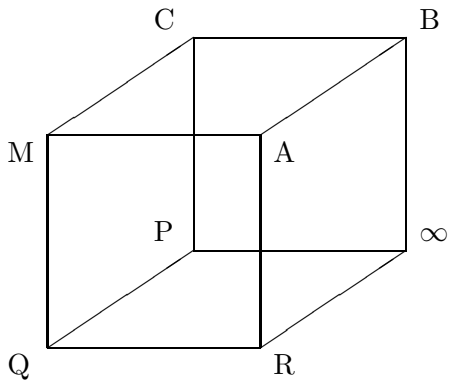



Les six birapports correspondent aux faces du cube. Partons de la face $ABCD$. Chaque arête du cube doit intervenir deux fois mais les petites diagonales, telles que $AC$, ne doivent pas intervenir. Commençons par le birapport $[a, c; b, d]$. La différence $b - a$ est au numérateur, elle doit donc figurer au dénominateur du birapport correspondant à la face $ABFE$; compte tenu des propriétés de symétrie du birapport (remarque page 7), ce birapport ne peut être que $[a, f; e, b]$. En continuant ainsi pour les autres arêtes, on aboutit aux six birapports considérés.

Donnons quelques applications du théorème des six birapports.

**Application 1**: droite de Simson.

Soient $ABC$ un triangle de $X$ et $\Gamma$ son cercle circonscrit. Soient $M$ un point de $X$ et $P, Q, R$ ses projections sur les côtés $BC, CA, AB$ respectivement. Pour simplifier, supposons les points $A, B, C, M, P, Q, R$ distincts (le lecteur examinera les cas particuliers restants). Alors $M$ appartient à $\Gamma$ si et seulement si $P, Q, R$ sont alignés (si $M \in \Gamma$, la droite $PQ$ est appelée droite de Simson de $M$ par rapport à $ABC$). Considérons le cube suivant:



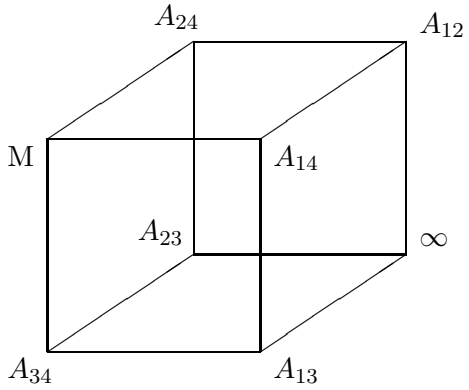
- La face droite donne un birapport réel, car $R$ appartient à $AB$;
- la face arrière donne un birapport réel, car $P$ appartient à $BC$;
- la face avant donne un birapport réel, en vertu du théorème de l'arc capable. En effet, les angles de droites $(QA, QM)$ et $(RA, RM)$ sont droits;
- pour la même raison, la face gauche donne un birapport réel.

Ainsi, d'après le théorème des six birapports, les points $M, A, B, C$ sont cocycliques si et seulement si $P, Q, R$ sont alignés, d'où le résultat.

**Application 2**: point de Miquel.

Soient $D_1, D_2, D_3, D_4$ quatre droites de $X$ «en position générale», i.e. deux à deux non parallèles et trois à trois non concourantes. Elles déterminent quatre triangles $T_i$, $i = 1, 2, 3, 4$, en notant par exemple $T_1$ le triangle formé par les droites $D_2, D_3, D_4$. Pour tout $i$, notons $C_i$ le cercle circonscrit au triangle $T_i$. Alors les cercles $C_1, C_2, C_3, C_4$ ont un point commun $M$, appelé point de Miquel de $\{D_1, D_2, D_3, D_4\}$.

Si $i < j$, notons $A_{ij}$ le point d'intersection de $D_i$ et $D_j$. Les cercles $C_1$ et $C_2$ se coupent en $A_{34}$. Ils ne sont pas tangents: s'ils l'étaient, l'unique homothétie de centre $A_{34}$ appliquant $C_1$ sur $C_2$ appliquerait $A_{24}$ sur $A_{14}$ et $A_{23}$ sur $A_{13}$, donc appliquerait la droite $A_{24}A_{23} = D_2$ sur la droite $A_{14}A_{13} = D_1$. Alors $D_1, D_2$ seraient parallèles, ce qui est faux. Notons donc $M$ le second point d'intersection de $C_1$ et $C_2$. Par symétrie, il suffit de montrer que $M \in C_3$. Considérons pour cela le cube suivant:




- La face droite donne un birapport réel: elle correspond à la droite $D_1$;
- la face du bas donne un birapport réel: elle correspond à la droite $D_3$;
- la face arrière donne un birapport réel: elle correspond à la droite $D_2$;
- la face avant donne un birapport réel: elle correspond au cercle $C_2$;
- la face gauche donne un birapport réel: elle correspond au cercle $C_1$.

D'après le théorème des six birapports, les quatre points de la face du haut sont cocycliques ou alignés, i.e. $M \in C_3$, comme désiré.

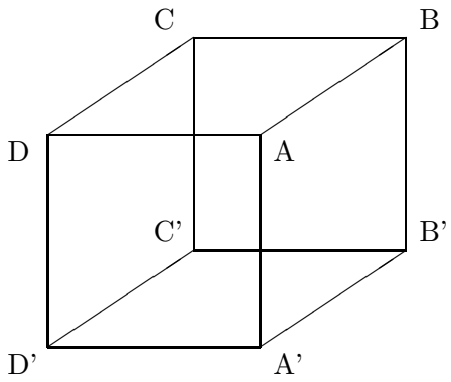
On peut montrer (cf. le livre de géométrie de Berger) que $M$ est le foyer de l'unique parabole tangente aux droites $D_1, D_2, D_3, D_4$.

**Application 3**: théorème des six cercles de Miquel.

Soient $C_1, C_2, C_3, C_4$ quatre cercles de $X$. On écrit:

$$C_1 \cap C_2 = \{A, A'\}\ ,\quad C_2 \cap C_3 = \{B, B'\}\ ,\quad C_3 \cap C_4 = \{C, C'\}\ ,\quad C_4 \cap C_1 = \{D, D'\}\,,$$

en supposant pour simplifier que les huit points $A, A', B, B', C, C', D, D'$ sont distincts. Alors $A, B, C, D$ sont cocycliques ou alignés si et seulement si $A', B', C', D'$ sont cocycliques ou alignés. La démonstration est ici immédiate, nous la laissons au lecteur; il suffit de considérer le cube:




Revenons au cas des droites projectives sur un corps $K$ quelconque. Étant donné une droite projective $\mathbb{P}(E)$ sur $K$, $E$ étant un plan vectoriel, il est naturel de chercher à classifier les homographies, i.e. à décrire les classes de conjugaison de $\mathrm{PGL}(E)$. Tout d'abord, si $u \in \mathrm{GL}(E)$ et si $h = [u]$ est l'homographie correspondante, posons:

$$\omega(h) \;=\; \frac{\mathrm{tr}\,(u)^2}{\det(u)}\cdot$$

Le second membre de cette formule ne dépend bien que de $h$, et pas du choix de $u$, à cause du lemme 1: si l'on remplace $u$ par $\lambda u$, où $\lambda \in K^*$, $\mathrm{tr}\,(u)^2$ et $\det(u)$ sont multipliés par $\lambda^2$. Il est clair que, si $h, h' \in \mathrm{PGL}(E)$ sont conjuguées, on a $\omega(h) = \omega(h')$. La réciproque est presque vraie:

**Proposition 18**. *Soient $E$ un plan vectoriel et $h, h'$ deux homographies de $\mathbb{P}(E)$ distinctes de l'identité. Soient $u, u' \in \mathrm{GL}(E)$ tels que $h = [u]$ et $h' = [u']$.*

1. *Si $\omega(h) \neq 0$ et $\omega(h') \neq 0$, $h$ et $h'$ sont conjuguées si et seulement si $\omega(h) = \omega(h')$.*

2. *Supposons que* $\omega(h) = \omega(h') = 0$. *Pour que* $h, h'$ *soient conjuguées, il faut et il suffit que* $\det(u)$ *et* $\det(u')$ *diffèrent multiplicativement d'un carré de* $K$.

*Démonstration*. Posons $t = \operatorname{tr}(u)$ et $d = \det(u)$. Puisque $h$ n'est pas l'identité, $u$ n'est pas une homothétie, i.e. son polynôme minimal est de degré $> 1$. Ce polynôme est donc égal au polynôme caractéristique de $u$ (Cayley-Hamilton), à savoir $P = X^2 - tX + d$. On sait de plus que la matrice de $u$ dans une base de $E$ convenable est $\begin{pmatrix} 0 & -d \\ 1 & t \end{pmatrix}$: il suffit de considérer une base $(x, u(x))$, où $x \in E$ n'est pas vecteur propre de $u$. De même la matrice de $u'$ dans une base de $E$ convenable est $\begin{pmatrix} 0 & -d' \\ 1 & t' \end{pmatrix}$, où $t' = \operatorname{tr}(u')$ et $d' = \det(u')$. Si $\lambda \in K^*$, la matrice de $\lambda\, u$ dans une base convenable est $\begin{pmatrix} 0 & -d\lambda^2 \\ 1 & t\lambda \end{pmatrix}$. Par ailleurs, $h$ et $h'$ sont conjuguées si et seulement s'il existe $\lambda \in K^*$ tel que $u'$ et $\lambda\, u$ soient semblables, ce qui revient à dire que $t' = t\lambda$ et $d' = d\lambda^2$.

Supposons d'abord $t, t' \neq 0$, et posons $\lambda = t'/t$. Vu ce qui précède, $h$ et $h'$ sont conjuguées si et seulement si $d' = d\lambda^2$, soit $t^2/d = t'^2/d'$, i.e. $\omega(h) = \omega(h')$. D'où l'assertion 1.

Si $t = t' = 0$, vu ce qui précède, $h$ et $h'$ sont conjuguées si et seulement s'il existe $\lambda \in K^*$ tel que $d' = d\lambda^2$, d'où l'assertion 2.

cqfd

Dans le cas où $K = \mathbb{C}$, la classification des homographies est facile:

**Proposition 19**. *Il y a deux types d'homographies de* $\widehat{\mathbb{C}}$ *autres que l'identité:*

1. *les homographies ayant un unique point fixe, ce sont les conjuguées de* $z \mapsto z + 1$*;*
2. *les homographies ayant exactement deux points fixes. Une telle homographie est conjuguée de* $z \mapsto \lambda\, z$*, pour un certain* $\lambda \in \mathbb{C} \setminus \{0, 1\}$*. De plus, étant donnés* $\lambda, \lambda' \in \mathbb{C} \setminus \{0, 1\}$*, les homographies* $z \mapsto \lambda\, z$ *et* $z \mapsto \lambda' z$ *sont conjuguées si et seulement si* $\lambda' = \lambda$ *ou* $\lambda' = 1/\lambda$.

*En particulier, il y a une seule classe de conjugaison d'homographies «* involutives*», i.e. d'ordre* 2*. Plus précisément, si* $x, y \in \widehat{\mathbb{C}}$ *sont distincts, il y a une unique homographie* $s_{x,y}$ *d'ordre* 2 *ayant pour points fixes* $x, y$ *et, lorsque* $\{x, y\}$ *varie, les* $s_{x,y}$ *décrivent la classe en question.*

*Démonstration*. Soit $h$ une homographie distincte de l'identité. D'abord $h$ a au moins un point fixe. En effet, soit $u \in \mathrm{GL}(\mathbb{C}^2)$ tel que $h = [u]$. Les points fixes de $h$ sont les droites propres de $u$, d'où la conclusion puisque $\mathbb{C}$ est algébriquement clos. Par ailleurs, d'après le théorème 2, $h$ possède au plus deux points fixes.

Supposons d'abord que $h$ possède un seul point fixe. Puisque $\mathrm{PGL}_2(\mathbb{C})$ opère transitivement sur $\widehat{\mathbb{C}}$ on peut supposer, sans changer la classe de conjugaison de $h$, que ce point fixe est $\infty$. Dans ce cas $h$ est une translation $z \mapsto z + \lambda$, où $\lambda \in \mathbb{C}^*$. En outre $\omega(h) = 2$, donc la proposition précédente montre que $h$ est conjuguée de $z \mapsto z + 1$.

Supposons que $h$ ait deux points fixes. Puisque $\mathrm{PGL}_2(\mathbb{C})$ opère deux fois transitivement sur $\widehat{\mathbb{C}}$ on peut supposer, sans changer la classe de conjugaison de $h$, que ces points fixes sont $\infty$ et 0. Dans ce cas $h$ est de la forme $z \mapsto \lambda\, z$, où $\lambda \in \mathbb{C} \setminus \{0, 1\}$, i.e. est définie par la matrice

$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$. Alors $\omega(h) = (\lambda+1)^2/\lambda$. Si $\lambda, \lambda' \in \mathbb{C} \setminus \{0, -1, 1\}$, la proposition 18 montre que $z \mapsto \lambda z$ et $z \mapsto \lambda' z$ sont conjuguées si et seulement si $(\lambda+1)^2/\lambda = (\lambda'+1)^2/\lambda'$, ce qui équivaut à $(\lambda' - \lambda)(\lambda\lambda' - 1) = 0$, i.e. à $\lambda' = \lambda$ ou $\lambda' = 1/\lambda$. Dans le cas où $\lambda = -1$, $h$ est l'involution $z \mapsto -z$, c'est le seul cas où $h$ soit une involution. La dernière assertion de l'énoncé est alors clair, puisque l'opération de $\mathrm{PGL}_2(\mathbb{C})$ sur $\widehat{\mathbb{C}}$ est deux fois transitive.

cqfd

**Remarque.** Si $a \in X$, l'involution $s_{\infty,a}$ est la symétrie de centre $a$. En revanche, si $a, b \in X$ sont distincts, l'interprétation de $s_{a,b}$ n'est pas aussi simple. Si $m = (a+b)/2$, on vérifie que $s_{a,b}$ échange $\infty$ et $m$ et que, pour tout $z \in \mathbb{C} \setminus \{m\}$, on a:

$$s_{a,b}(z) \;=\; \frac{mz - ab}{z - m}\,.$$

Si $a, b \in \widehat{\mathbb{C}}$ sont distincts mais quelconques, et si $z \in \widehat{\mathbb{C}} \setminus \{a, b\}$, on vérifie aussi que $s_{a,b}(z) \in \widehat{\mathbb{C}}$ est caractérisé par l'égalité $[a, b; z, s_{a,b}(z)] = -1$.

Passons aux antihomographies. Celles qui sont involutives correspondent aux symétries axiales ou aux *inversions* de $X$. Rappelons la définition de ces inversions.

**Définition 8**. *Soient $A$ un point de $X$ et $k \in \mathbb{R}^*$. On appelle* **inversion** *de pôle $A$ et de puissance $k$ la permutation $i_{A,k}$ de $\widehat{X}$ échangeant $\infty$ et $A$ et telle que, pour tout point $M \in X \setminus \{A\}$, le point $M' = i_{A,k}(M)$ soit le seul point de la droite $AM$ vérifiant l'égalité:*

$$\overline{AM}.\overline{AM'} \;=\; k\,.$$

la traduction en termes d'affixes est claire. Soit $a$ l'affixe de $A$. Alors

$$\overrightarrow{AM'} \;=\; \left(\frac{k}{AM^2}\right)\overrightarrow{AM}\;,\quad i_{A,k}(z) \;=\; a + \frac{k}{\bar{z} - \bar{a}}\,.$$

On en déduit que

1. si $k < 0$, $i_{A,k}$ ne possède aucun point fixe;
2. si $k > 0$, l'ensemble des points fixes de $i_{A,k}$ est le cercle $C$ de centre $A$ et de rayon $\sqrt{k}$; on dit alors que $i_{A,k}$ est l'inversion de cercle $C$;
3. dans tous les cas, $i_{A,k}$ est une antihomographie involutive de $\widehat{X}$.

**Proposition 20**. *Pour tout pseudo-cercle $S$, il existe une unique antihomographie $i_S$ dont l'ensemble des points fixes soit $S$. De plus, il y a dans $\Gamma$ deux classes de conjugaison d'homographies involutives, ce sont:*

1. *la classe formée de toutes les inversions de puissance $< 0$;*
2. *la classe formée des $i_S$, où $S$ décrit $\Pi$.*

*Démonstration*. Pour la première assertion, il suffit, puisque l'opération de $\Gamma$ sur $\widehat{X}$ est deux fois transitive, de traiter le cas où $S = \widehat{D}$, $D$ étant l'axe des abscisses. Dans ce cas, la symétrie $\sigma$ par rapport à $D$ répond à la question. Inversement, si $f$ est une antihomographie fixant tous les points de $\widehat{D}$, $f \circ \sigma$ est une homographie fixant ces mêmes points, c'est donc l'identité, d'où $f = \sigma$.

Soit maintenant $f$ une antihomographie involutive de $\widehat{X}$. Supposons d'abord que $f(\infty) = \infty$. Alors $f \circ \sigma$ est une similitude plane directe $z \mapsto az+b$, où $a \in \mathbb{C}^*,\ b \in \mathbb{C}$, donc $f$ s'écrit $z \mapsto a\bar{z}+b$. Puisque $f$ est involutive, $z = a\overline{(a\bar{z}+b)} + b$ pour tout $z \in \mathbb{C}$, i.e. $a\bar{b} + b = 0$ et $|a| = 1$. Si $b \neq 0$, l'ensemble des points fixes de $f$ dans $X$ a pour équation $z - a\bar{z} - b = 0$, soit $\bar{b}z - a\bar{b}\bar{z} - |b|^2 = 0$, ou encore $\bar{b}z + b\bar{z} - |b|^2 = 0$. C'est l'équation d'une droite $D$ (ne passant pas par 0), et donc $f$ est la symétrie par rapport à $D$. Si $b = 0$, $f$ est donnée par $z \mapsto a\bar{z}$, c'est la composée de $\sigma$ et d'une rotation de centre 0, c'est encore la symétrie par rapport à une droite (passant par 0).

Supposons ensuite que $f(\infty) = c \in X$. Soit $i'$ une inversion de pôle $c$ et de puissance $k \in \mathbb{R}^*$. Alors $f \circ i'$ est une similitude plane directe fixant $c$, elle est de la forme $z \mapsto c + \lambda(z - c)$, où $\lambda \in \mathbb{C}^*$. Un calcul immédiat montre que $f$ s'écrit: $z \mapsto c + \frac{\lambda k}{\bar{z} - \bar{c}}$ pour $z \in \mathbb{C} \setminus \{c\}$, et $f$ échange $\infty$ et $c$. Le fait que $f$ soit involutive se traduit par la condition $\lambda \in \mathbb{R}^*$, et ainsi $f$ est une inversion de pôle $c$.

Pour conclure, il reste à vérifier deux choses. La première est que, si $S$ décrit $\Pi$, les $i_S$ décrivent une classe de conjugaison de $\Gamma$. Cela résulte de la première assertion de l'énoncé, de la proposition 14 et du théorème 2 (qui montrent que $\mathrm{PGL}_2(\mathbb{C})$ opère transitivement sur $\Pi$). La deuxième chose à vérifier est que les inversions de puissance $< 0$ forment une classe de conjugaison de $\Gamma$. D'abord, si $\gamma \in \Gamma$ et si $i'$ est une inversion de puissance $< 0$, $\gamma \circ i' \circ \gamma^{-1}$ est une antihomographie involutive sans points fixes, ce qui précède montre que c'est une inversion de puissance $< 0$. Ensuite, soit $i'$ une inversion, de pôle $A$ et de puissance $k < 0$. Si $t$ est une translation de vecteur $\vec{u}$, on vérifie que $t \circ i' \circ t^{-1}$ est l'inversion de pôle $A + \vec{u}$ et de puissance $k$. D'autre part, si $h$ est une homothétie de centre $A$ et de rapport $r > 0$, on vérifie que $h \circ i' \circ h^{-1}$ est l'inversion de pôle $A$ et de puissance $kr^2$. Il en résulte que toutes les inversions de puissance $< 0$ sont conjuguées de $i'$, ce qui achève la preuve de la proposition.

cqfd

**Remarque.** Soit $S$ un pseudo-cercle. Si $S$ est un cercle, $i_S$ est l'inversion de cercle $C$. Si $S = \widehat{D}$, où $D$ est une droite de $X$, $i_S$ est la symétrie orthogonale par rapport à $D$. Tout cela résulte de la première assertion de la proposition précédente.

Terminons ces compléments en reprenant le cas d'une doite projective sur $\mathbb{F}_5$, cf. la proposition 6. Comme nous l'avons vu dans la preuve de la proposition 6, $\mathrm{PGL}_2(\mathbb{F}_5)$ est isomorphe à un sous-groupe $G$ de $\mathfrak{S}_6$ possédant les deux propriétés suivantes:

1. Le groupe $G$ est d'ordre 120.
2. L'opération naturelle de $G$ sur $\{1, \ldots, 6\}$ est simplement trois fois transitive, en particulier transitive. Bien sûr, cette propriété 2 implique 1.

Soit $E$ l'ensemble des classes à gauche de $\mathfrak{S}_6$ modulo $G$. Il est de cardinal 6, et $\mathfrak{S}_6$ opère transitivement, par translations à gauche, sur $E$. Cette opération est définie par un morphisme $\psi : \mathfrak{S}_6 \to \mathfrak{S}(E)$. Le noyau de $\psi$ est un sous-groupe distingué de $\mathfrak{S}_6$, on sait qu'il est égal à $\{1\}, \mathfrak{A}_6$ ou $\mathfrak{S}_6$. D'un autre côté, par définition, l'opération naturelle de l'image de $\psi$ sur $E$ est transitive, donc l'ordre de cette image est multiple de 6. Il en résulte que $\psi$ est injectif, c'est donc un isomorphisme: $\mathfrak{S}_6$ et $\mathfrak{S}(E)$ ont même ordre.

Notons $C_1, \ldots, C_6$ les classes à gauche de $\mathfrak{S}_6$ modulo $G$, avec $C_1 = H$. L'isomorphisme $\psi$ correspond à un automorphisme $\omega$ de $\mathfrak{S}_6$. Plus précisément, pour toute permutation $s \in \mathfrak{S}_6$ et tout indice $i \in [1, 6]$, on a:

$$s\,C_i \;=\; \psi(s)(C_i) \;=\; C_{\omega(s)(i)}\,. \tag{16}$$

**Proposition 21**.

1. *L'automorphisme $\omega$ de $\mathfrak{S}_6$ n'est pas intérieur.*
2. *En revanche, si $n \geq 1$ est un entier distinct de 6, tout automorphisme du groupe $\mathfrak{S}_n$ est intérieur.*

*Démonstration*. L'assertion 2 est assez classique, mais elle n'a rien à voir avec les droites projectives, nous la signalons seulement pour mettre en relief 1. Nous nous contenterons donc de prouver l'assertion 1. Raisonnons par l'absurde, en supposant que $\omega$ est un automorphisme intérieur de $\mathfrak{S}_6$: il existe un élément $t$ de $\mathfrak{S}_6$ tel que $\omega(u) = t \circ u \circ t^{-1}$ pour tout $u \in \mathfrak{S}_6$. Pour tous $s \in \mathfrak{S}_6$ et $i \in [1, 6]$, on a donc:

$$s\,C_i \;=\; C_{(tst^{-1})(i)}\,.$$

Dans cette égalité, prenons $i = 1$ et $s \in G$. Alors $sC_1 = G$, donc $(tst)^{-1}(1) = 1$. Autrement dit, posant $j = t^{-1}(1)$, on a $s(j) = j$. C'est vrai pour tout $s \in G$, et donc $G$ est contenu dans $(\mathfrak{S}_6)_j$, stabilisateur de $j$ dans $\mathfrak{S}_6$. C'est absurde, puisque $G$ opère transitivement sur $\{1, \ldots, 6\}$.

cqfd

**Remarque.** Gardons les notations précédentes. Pour montrer que $\mathrm{PGL}_2(\mathbb{F}_5)$ est isomorphe à $\mathfrak{S}_5$ (cf. la proposition 6), reprenons les égalités (16). Si $i = 1$ et $s \in G$, on a $C_1 = sC_1 = \psi(s)(C_1)$, ainsi $\psi(s)(C_1) = C_1$. Le groupe $\psi(G)$ est donc inclus dans le stabilisateur de $C_1$ dans $\mathfrak{S}(E)$. Comme $E$ est de cardinal 6, ledit stabilisateur est isomorphe à $\mathfrak{S}_5$. De plus, $\psi$ définit un isomorphisme de $G$ sur $\psi(G)$. En conclusion, $G$ est isomorphe à un sous-groupe de $\mathfrak{S}_5$; mais $G$ est d'ordre 120, donc $G$ est isomorphe à $\mathfrak{S}_5$, comme annoncé.

En fait, on peut montrer plus généralement que, si $n \geq 2$ est un entier, tout sous-groupe d'indice $n$ de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$.