



Théorie des Groupes et Géométrie

*Contrôle Continu n°2 :
Groupes et Géométrie
Une heure*



Il n'est pas nécessaire de faire l'intégralité du contrôle pour avoir la note maximale.

Questions de cours

On justifiera avec soin chaque réponse.

1. (a) *Retrouver le cardinal de $\text{PSL}_2(\mathbb{F}_3)$.*

Commençons par calculer $\#\text{GL}_2(\mathbb{F}_3)$. On a $3^2 - 1$ choix pour le premier vecteur colonne (un vecteur non nul de \mathbb{F}_3^2), et pour le deuxième il nous reste $3^2 - 3$ choix puisque l'on veut un vecteur qui ne soit pas proportionnel au premier. On a donc $\#\text{GL}_2(\mathbb{F}_3) = (3^2 - 1)(3^2 - 3) = 3(3 - 1)^2(3 + 1)$.

Calculons maintenant le cardinal de $\text{SL}_2(\mathbb{F}_3)$. Le déterminant $\det : \text{GL}_2(\mathbb{F}_3) \rightarrow \mathbb{F}_3^\times$ est un morphisme surjectif de noyau $\text{SL}_2(\mathbb{F}_3)$, donc par le premier théorème d'isomorphisme on obtient $\#\text{SL}_2(\mathbb{F}_3) \simeq \frac{\#\text{GL}_2(\mathbb{F}_3)}{\#\mathbb{F}_3^\times} = 3(3 - 1)(3 + 1)$. Finalement, par définition on obtient le cardinal de $\text{PSL}_2(\mathbb{F}_3)$ en divisant le cardinal de $\text{SL}_2(\mathbb{F}_3)$ par celui de son centre, c'est-à-dire par le nombre de $\lambda \in \mathbb{F}_3^\times$ de carré 1. Ici les deux éléments de $\mathbb{F}_3^\times = \{-1, 1\}$ sont de carré 1, donc on en déduit que

$$\#\text{PSL}_2(\mathbb{F}_3) = \frac{\#\text{SL}_2(\mathbb{F}_3)}{2} = 3(3 + 1) = 12.$$

- (b) *En faisant agir fidèlement $\text{PSL}_2(\mathbb{F}_3)$ sur un ensemble à quatre éléments, montrer que $\text{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$.*

On sait que $\text{SL}_2(\mathbb{F}_3)$ agit sur l'ensemble des droites vectorielles de \mathbb{F}_3^2 , c'est-à-dire sur $\mathbb{P}(\mathbb{F}_3^2) = \mathbb{P}^1(\mathbb{F}_3)$. On a $\#\mathbb{P}^1(\mathbb{F}_3) = 3 + 1 = 4$ (rappelons que l'on peut obtenir ce cardinal en utilisant le fait que l'action de $\text{GL}_2(\mathbb{F}_3)$ sur $\mathbb{P}^1(\mathbb{F}_3)$ est transitive, le stabilisateur d'une droite étant de la forme $\left\{ \begin{pmatrix} \lambda & * \\ 0 & * \end{pmatrix} \right\}$ donc de cardinal $(\#\mathbb{F}_3^\times)^2 \#\mathbb{F}_3 = 3(3 - 1)^2$) donc on obtient un morphisme $\text{SL}_2(\mathbb{F}_3) \rightarrow \mathfrak{S}_4$. Son noyau est le centre de $\text{SL}_2(\mathbb{F}_3)$, donc (par définition de PSL) on obtient une injection $\text{PSL}_2(\mathbb{F}_3) \hookrightarrow \mathfrak{S}_4$. D'après la question (a), le groupe $\text{PSL}_2(\mathbb{F}_3)$ s'identifie à un sous-groupe d'indice 2 de \mathfrak{S}_4 , c'est donc \mathfrak{A}_4 (en effet, ce sous-groupe est distingué car d'indice 2 et on conclut puisque la surjection canonique $\mathfrak{S}_4 \rightarrow \mathfrak{S}_4/\text{PSL}_2(\mathbb{F}_3) \simeq \mathbb{Z}/2\mathbb{Z}$ est nécessairement la signature donc est de noyau $\text{PSL}_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$).

2. *Soient x, y, z, t quatre points distincts d'une droite projective. Montrer que $[x, y, t, z] = [x, y, z, t]^{-1}$ (on pourra par exemple utiliser la formule explicite du birapport).*

Notre convention pour l'écriture $[x, y, z, t]$ est x va sur ∞ , y va sur 0 et z sur 1.

Première solution La formule explicite donne

$$\begin{aligned} [x, y, t, z] &= \frac{z - y}{t - y} \bigg/ \frac{z - x}{t - x} \\ &= \frac{(t - x)(z - y)}{(t - y)(z - x)} \\ &= \frac{(z - y)(t - x)}{(z - x)(t - y)} \\ &= \left(\frac{(z - x)(t - y)}{(z - y)(t - x)} \right)^{-1} \\ &= [x, y, z, t]^{-1}, \end{aligned}$$

et on vérifie que tout se passe bien quand x, y, z ou t vaut l'infini (cette vérification est en fait nécessaire seulement quand $k = \mathbb{F}_3$, en effet sinon la droite projective contient au moins un cinquième point et on peut composer le birapport par une homographie qui envoie ce cinquième point à l'infini).

Deuxième solution Soit f l'(unique) homographie qui envoie x sur ∞ , y sur 0 et z sur 1 . Alors $f(t) \neq \infty$ et l'application $g := f(t)^{-1}f$ est une homographie qui envoie x sur ∞ , y sur 0 et t sur 1 . Ainsi,

$$\begin{aligned} [x, y, t, z] &= g(z) \\ &= f(t)^{-1}f(z) \\ &= f(t)^{-1} \\ &= [x, y, z, t]^{-1}. \end{aligned}$$

Exercice 1

Soit k un corps. Une involution de $\mathbb{P}^1(k)$ est une homographie $g \neq \text{Id}_{\mathbb{P}^1(k)}$ telle que $g^2 = \text{Id}_{\mathbb{P}^1(k)}$.

1. Montrer qu'une homographie g de $\mathbb{P}^1(k)$ est une involution si et seulement s'il existe $p \neq q \in \mathbb{P}^1(k)$ tels que $g(p) = q$ et $g(q) = p$.

Tout d'abord, si g est une involution de $\mathbb{P}^1(k)$ alors puisque g n'est pas l'identité il existe p tel que $q := g(p) \neq p$. Mais $g^2 = \text{Id}$ donc $g(q) = g^2(p) = p \neq q$. Montrons maintenant la réciproque ; soit g une homographie de $\mathbb{P}^1(k)$ telle qu'il existe $p \neq q$ avec $g(p) = q$ et $g(q) = p$. En particulier, on a $g \neq \text{Id}_{\mathbb{P}^1(k)}$.

Première solution, version algèbre linéaire Les deux points distincts p et q de $\mathbb{P}^1(k)$ correspondent à deux droites distinctes de k^2 . Par hypothèse, l'élément de $\text{GL}(k^2)$ associé à g permute ces deux droites, donc sa matrice dans une base adaptée est de la forme $M := \begin{pmatrix} 0 & \beta \\ \alpha & 0 \end{pmatrix}$ (on remarque que deux vecteurs non nuls distincts et non colinéaires de k^2 forment une base). Mais alors $M^2 = \alpha\beta I_2$ donc $g^2 = \text{Id}_{\mathbb{P}^1(k)}$ donc g est une involution.

Deuxième solution, version projectif Si $g(r) = r$ pour tout $r \in \mathbb{P}^1(k) \setminus \{p, q\}$ alors c'est gagné (on a bien $g^2 = \text{Id}_{\mathbb{P}^1(k)} \neq g$). Supposons maintenant qu'il existe $r \in \mathbb{P}^1(k) \setminus \{p, q\}$ tel que $g(r) \neq r$ et montrons que $g^2(r) = r$. Remarquons que l'on a nécessairement $g(r) \notin \{p, q\}$ (si $g(r) \in \{p, q\}$ alors on obtient $r \in \{p, q\}$ en appliquant g^{-1}). Soit maintenant f l'homographie de $\mathbb{P}^1(k)$ qui envoie p sur ∞ , q sur 0 et r sur 1 . Les points $p, q, r, g(r)$ sont des points de la droite projective $\mathbb{P}^1(k)$ deux à deux distincts donc on peut considérer le birapport $[p, q, r, g(r)]$. Par définition, ce birapport est égal à $f(g(r))$, et en composant par l'homographie g on obtient (les homographies conservent le birapport)

$$[p, q, r, g(r)] = [q, p, g(r), g^2(r)].$$

En raisonnant comme dans la deuxième solution de la question 2 des questions de cours, on voit que l'homographie $\frac{f(g(r))}{f}$ envoie q sur ∞ , p sur 0 et $g(r)$ sur 1 (remarquons que $f(g(r)) \neq \infty$ puisque $g(r) \neq p$). Ainsi, on a

$$[q, p, g(r), g^2(r)] = \frac{f(g(r))}{f(g^2(r))}.$$

Finalement, on obtient

$$f(g(r)) = [p, q, r, g(r)] = [q, p, g(r), g^2(r)] = \frac{f(g(r))}{f(g^2(r))},$$

donc en simplifiant on obtient $f(g^2(r)) = 1$ donc $g^2(r) = r$ par injectivité de f . On conclut.

2. Soient p_1, p_2, p_3 (respectivement q_1, q_2, q_3) trois points distincts de $\mathbb{P}^1(k)$ avec $(p_1, p_2, p_3) \neq (q_1, q_2, q_3)$. Soit f l'unique homographie de $\mathbb{P}^1(k)$ qui envoie chaque p_i sur q_i pour tout $i \in \{1, 2, 3\}$. Montrer que f est une involution si et seulement si

$$[p_1, p_2, p_3, q_i] = [q_1, q_2, q_3, p_i],$$

pour tout $i \in \{1, 2, 3\}$.

La condition nécessaire est claire puisque les homographies conservent le birapport. Montrons la condition suffisante. On a :

$$[p_1, p_2, p_3, q_i] = [f(p_1), f(p_2), f(p_3), f(q_i)] = [q_1, q_2, q_3, f(q_i)] = [q_1, q_2, q_3, p_i]$$

La première égalité est par invariance du birapport par homographie. La seconde utilise simplement la définition de f . La troisième est l'hypothèse sur les p_i, q_i . On obtient donc que $f(q_i) = p_i$ pour tout i . Finalement, puisque $(p_1, p_2, p_3) \neq (q_1, q_2, q_3)$, il existe un i tel que $p_i \neq q_i$ et on conclut par la question 1 que f est un involution.

On suppose maintenant que k est de caractéristique différente de 2. Soit g une involution de $\mathbb{P}^1(k)$ possédant un point fixe.

3. Montrer que g possède exactement deux points fixes. On note a, b ces points fixes.

On peut remarquer que puisque $g \neq \text{Id}_{\mathbb{P}^1(k)}$, on sait que g possède au plus deux points fixes (sinon g coïnciderait avec $\text{Id}_{\mathbb{P}^1(k)}$ sur trois points distincts donc serait l'identité). Soit f un élément de $\text{GL}(k^2)$ associé à g . Puisque g est une involution de $\mathbb{P}^1(k)$, on a $f^2 = \lambda \text{Id}_{\text{GL}(k^2)}$ avec $\lambda \in k^\times$. Puisque g possède un point fixe, l'automorphisme f possède un vecteur propre et donc une valeur propre μ dans k^\times . Remarquons que μ est une racine carrée de λ , l'autre racine carrée étant $-\mu$. De plus, on a $-\mu \neq \mu$ car $\mu \neq 0$ et k est de caractéristique différente de 2. Maintenant, puisque f est annulé par $X^2 - \lambda = (X - \mu)(X + \mu)$ qui est donc scindé à racines simples sur k , on sait que f est diagonalisable. L'automorphisme f n'est pas une homothétie puisque $g \neq \text{Id}_{\mathbb{P}^1(k)}$, donc les deux valeurs propres de f sont distinctes et sont μ et $-\mu$. Ainsi f possède exactement deux droites propres, c'est-à-dire g possède exactement deux points fixes.

4. Montrer que pour tout point $m \in \mathbb{P}^1(k) \setminus \{a, b\}$ on a $[a, b, m, g(m)] = -1$.

Par la question précédente, on sait que $g(m) \neq m$. De plus, puisque $g^2 = \text{Id}_{\mathbb{P}^1(k)}$ on a également $g(m) \notin \{a, b\}$ donc les quatre points $a, b, m, g(m)$ sont bien distincts. Puisque g conserve le birapport, on a d'une part

$$[a, b, m, g(m)] = [a, b, g(m), m].$$

D'autre part, par le 2 des questions de cours on a

$$[a, b, m, g(m)] = [a, b, g(m), m]^{-1}.$$

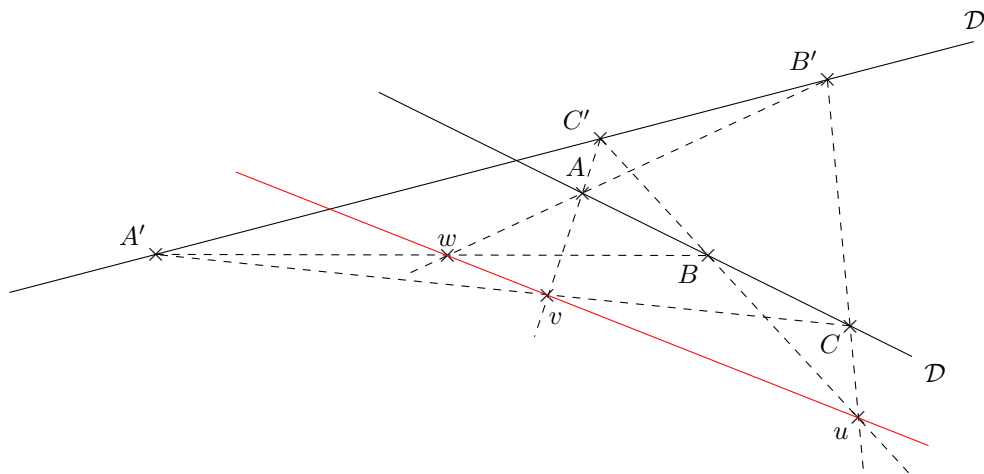
Ainsi, on obtient

$$[a, b, m, g(m)] = [a, b, m, g(m)]^{-1},$$

donc $[a, b, m, g(m)] = \pm 1$. Or, puisque $g(m) \neq m$ on a $[a, b, m, g(m)] \neq 1$ (par définition du birapport), d'où le résultat.

Exercice 2

Soient $\mathcal{D}, \mathcal{D}'$ deux droites d'un plan projectif. Soient A, B, C trois points de \mathcal{D} et A', B', C' trois points de \mathcal{D}' . On note $u = (BC') \cap (B'C)$, $v = (CA') \cap (C'A)$ et $w = (AB') \cap (A'B)$. Le but de l'exercice est de montrer que les points u, v, w sont alignés à l'aide de perspectives.



1. Rappeler le nom de cet énoncé.

C'est un sens du théorème de Pappus (on a en fait équivalence).

On note $p_1 : (BC') \rightarrow \mathcal{D}'$ la perspective de centre C de (BC') vers \mathcal{D}' . On note $p_2 : \mathcal{D}' \rightarrow (A'B)$ la perspective de centre A de \mathcal{D}' vers $(A'B)$. On note $f = p_2 \circ p_1$.

2. On note $M = (BC') \cap (A'C)$ et $N = (AC') \cap (A'B)$. Calculer $f(B)$, $f(M)$, $f(C')$ et $f(u)$.

Calculons d'abord les images par p_1 , que l'on représente sur la Figure 1. Soit O le point d'intersection de \mathcal{D} et \mathcal{D}' (rappelons que deux droites projectives se coupent toujours). Par définition, on a $p_1(B) \in \mathcal{D}' \cap (CB)$ donc $p_1(B) = O$ puisque $(BC) = \mathcal{D}$. De même, on trouve

$$\begin{aligned} p_1(M) &= A', \\ p_1(C') &= C', \\ p_1(u) &= B'. \end{aligned}$$

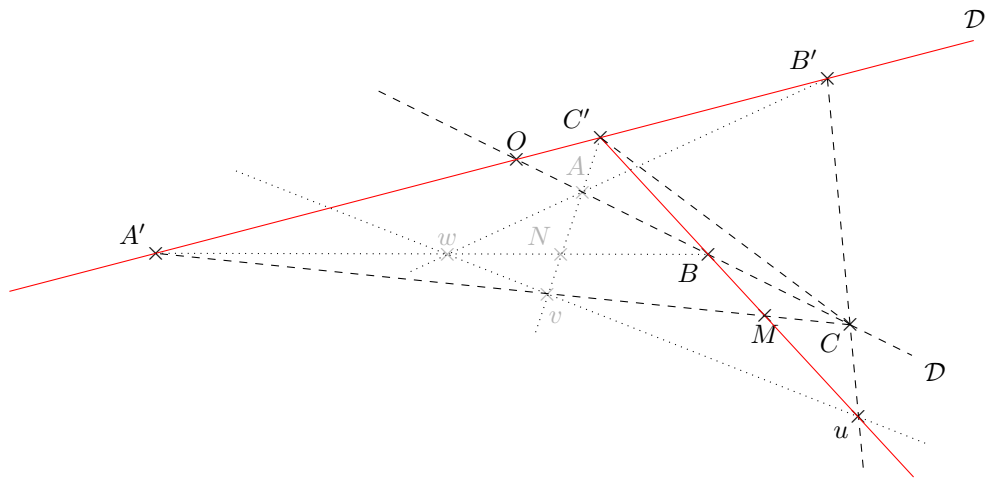


FIGURE 1 – Perspective p_1 de centre C de (BC') vers D'

Calculons maintenant les images par p_2 , des points O, A', C' et B' d'après ce qui précède, que l'on représente sur la Figure 2. On a $p_2(O) = (A'B) \cap (AO)$ donc $p_2(O) = B$ puisque $(AO) = D \ni B$. De même, on montre que

$$\begin{aligned} p_2(A') &= A', \\ p_2(C') &= N, \\ p_2(B') &= w. \end{aligned}$$

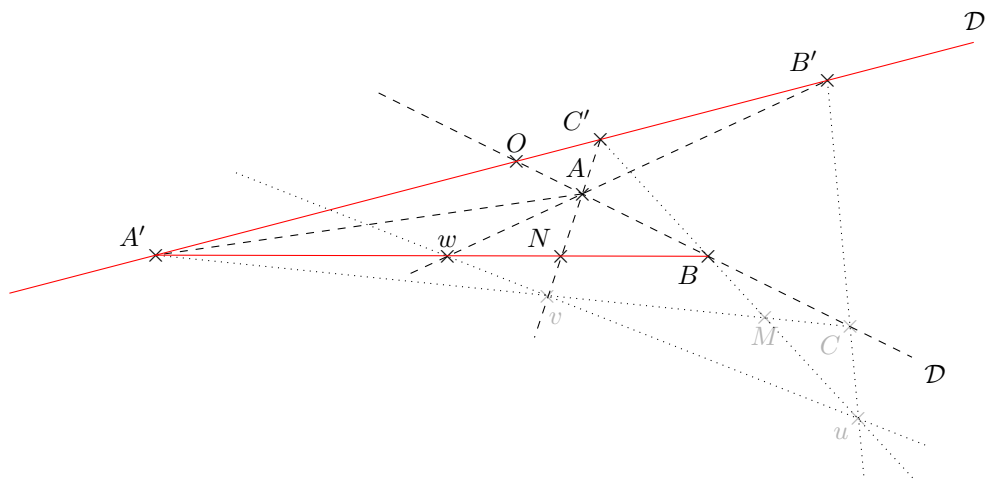


FIGURE 2 – Perspective p_2 de centre A de D' vers $(A'B)$

Finalement, on a donc

$$\begin{aligned} f(M) &= p_2(p_1(M)) = p_2(A') = A', \\ f(C') &= p_2(p_1(C')) = p_2(C') = N, \\ f(u) &= p_2(p_1(u)) = p_2(B') = w. \end{aligned}$$

On note $q : (BC') \rightarrow (A'B)$ la perspective de centre v de (BC') vers $(A'B)$.

3. Calculer $q(B)$, $q(M)$ et $q(C')$.

On calcule comme dans la question précédente, pour trouver (cf. Figure 3)

$$q(B) = B, \quad q(M) = A', \quad q(C') = N.$$

4. En déduire $q(u)$.

Les homographies f et q coïncident sur les points alignés distincts B, M et C' donc sont égales sur cette droite. Cette droite contient u donc $q(u) = f(u) = w$.

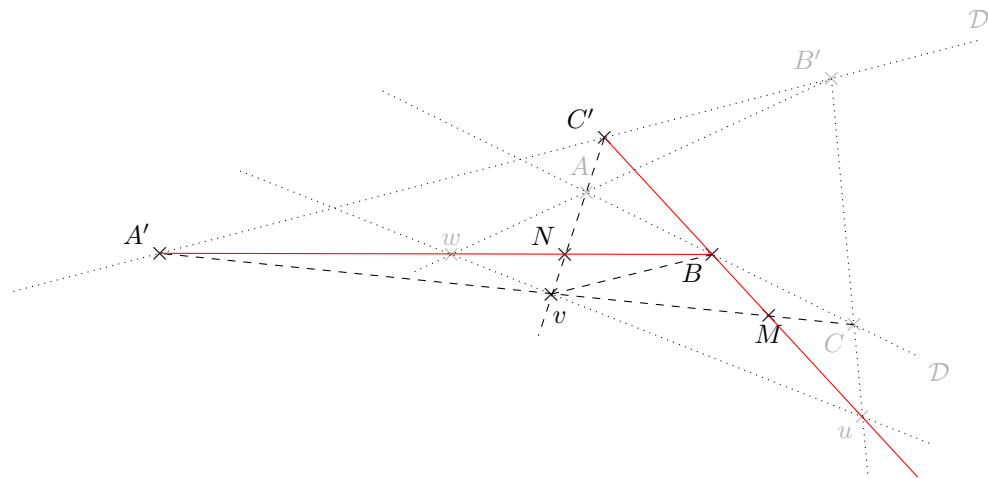


FIGURE 3 – Perspective q de centre v de (BC') vers $(A'B)$

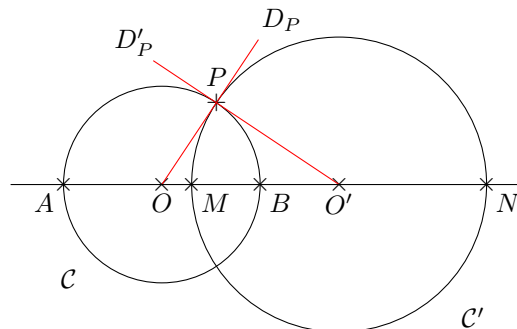
5. *Conclure.*

Puisque $q(u) = w$, par définition de q on sait que v, u et w sont alignés.

Exercice 3

Soient \mathcal{C} et \mathcal{C}' deux cercles du plan euclidien \mathbb{R}^2 de centres O et O' . On dit que \mathcal{C} et \mathcal{C}' sont orthogonaux lorsque $\mathcal{C} \cap \mathcal{C}' = \{P, Q\}$ et que les tangentes D_P et D'_P à \mathcal{C} et \mathcal{C}' en P sont orthogonales.

On suppose que la droite (OO') rencontre \mathcal{C} en A, B et \mathcal{C}' en M, N .



1. Montrer que les cercles \mathcal{C} et \mathcal{C}' sont orthogonaux si et seulement si $[A, B, M, N] = -1$.

Première solution, version géométrie euclidienne classique Trouvons d'abord une condition d'orthogonalité. Quitte à changer de repère en utilisant un automorphisme affine du plan, qui est une homographie donc conserve le birapport, on peut supposer que $O = (0, 0)$ est l'origine et $O' = (x_0, 0)$ avec $x_0 \neq 0$ (car $O' \neq O$, sinon bon courage pour la tangence). Soit r (respectivement r') le rayon de \mathcal{C} (resp. \mathcal{C}'). Les points P, Q sont déterminés par

$$\begin{cases} x^2 + y^2 = r^2, \\ (x - x_0)^2 + y^2 = r'^2, \end{cases}$$

donc en soustrayant on obtient $x = \frac{r^2 - r'^2 + x_0^2}{2x_0}$. On a donc $x_P = x_Q$ avec

$$x_P = \frac{r^2 - r'^2 + x_0^2}{2x_0}, \quad (1)$$

et $y_P = -y_Q = \sqrt{r^2 - x_P^2}$. La tangente à \mathcal{C} (resp. \mathcal{C}') en P a pour vecteur normal \overrightarrow{OP} (resp. $\overrightarrow{O'P}$),

on obtient donc

$$\begin{aligned}
\mathcal{C} \perp \mathcal{C}' &\iff \overrightarrow{OP} \cdot \overrightarrow{OP'} = 0 \\
&\iff \begin{pmatrix} x_P \\ y_P \end{pmatrix} \cdot \begin{pmatrix} x_P - x_0 \\ y_P \end{pmatrix} = 0 \\
&\iff x_P(x_P - x_0) + y_P^2 = 0 \\
&\iff x_P^2 + y_P^2 - x_P x_0 = 0 \\
&\iff x_P x_0 = r^2.
\end{aligned}$$

Ainsi, en utilisant (1) on obtient

$$\mathcal{C} \perp \mathcal{C}' \iff x_0^2 = r^2 + r'^2. \quad (2)$$

Considérons maintenant $A(-r, 0)$, $B(r, 0)$, $M(x_0 - r', 0)$ et $N(x_0 + r', 0)$. En notant t l'abscisse de $T \in \{A, B, M, N\}$ on a

$$\begin{aligned}
[A, B, M, N] &= \frac{n-b}{m-b} \Big/ \frac{n-a}{m-a} \\
&= \frac{(n-b)(m-a)}{(m-b)(n-a)} \\
&= \frac{(x_0 + r' - r)(x_0 - r' + r)}{(x_0 - r' - r)(x_0 + r' + r)} \\
&= \frac{x_0^2 - (r - r')^2}{x_0^2 - (r + r')^2}
\end{aligned}$$

Ainsi, par (2) on obtient finalement

$$\begin{aligned}
[A, B, M, N] = -1 &\iff \frac{x_0^2 - (r - r')^2}{x_0^2 - (r + r')^2} = -1 \\
&\iff x_0^2 - (r - r')^2 = -x_0^2 + (r + r')^2 \\
&\iff 2x_0^2 = 2r^2 + 2r'^2 \\
&\iff x_0^2 = r^2 + r'^2 \\
&\iff \mathcal{C} \perp \mathcal{C}'.
\end{aligned}$$

Deuxième solution, version géométrie projective de la droite complexe On envoie le point N à l'infini, ou de façon équivalente, on applique une homographie g de la droite projective complexe telle que $g(N) = \infty$. On se rappelle que les homographies de la droite projective complexe préserve l'ensemble des droites et des cercles. Ainsi,

- (a) $g(\mathcal{C})$ est un cercle puisque \mathcal{C} ne contient pas N .
- (b) $g(\mathcal{C}')$ est une droite puisque \mathcal{C}' contient le point N .
- (c) $g((OO'))$ est une droite puisque $(OO') = (AB) = (MN)$ donc contient le point N .

Attention : $g(O)$ n'a pas de raison d'être le centre du cercle $g(\mathcal{C})$. Penser à $g(O')$ qui n'est pas le centre de la droite $g(\mathcal{C}')$...

Une droite \mathcal{D} et un cercle \mathcal{C} sont dits *orthogonaux* si les tangentes au cercle \mathcal{C} aux points d'intersections $\mathcal{C} \cap \mathcal{D}$ sont orthogonales à la droite \mathcal{D} , autrement dit si et seulement si \mathcal{D} passe par le centre du cercle \mathcal{C} .

Il est important de se rappeler qu'une homographie de la droite projective complexe est une application holomorphe $\mathbb{C} \setminus \{N\} \rightarrow \mathbb{C}$. Par conséquent, elle conserve les angles entre les courbes par conséquent :

$$g(\mathcal{C}') \perp g((OO')), \quad g(\mathcal{C}) \perp g((OO')) \quad \text{et} \quad g(\mathcal{C}') \perp g(\mathcal{C}) \iff \mathcal{C}' \perp \mathcal{C}$$

puisque $(OO') \perp \mathcal{C}, \mathcal{C}'$. En particulier, la droite $g((OO'))$ passe par le centre de $g(\mathcal{C})$ donc $[g(A)g(B)]$ est un diamètre de $g(\mathcal{C})$ et la droite $g(\mathcal{C}') \perp g((OO'))$. On en déduit les équivalences suivantes :

$$\begin{aligned}
\mathcal{C}' \perp \mathcal{C} &\iff g(\mathcal{C}') \perp g(\mathcal{C}) \\
&\iff g(M) \text{ est le milieu du segment } [g(A)g(B)] \\
&\iff [g(A), g(B), g(M), \infty] = -1 \\
&\iff [g(A), g(B), g(M), g(N)] = -1 \\
&\iff [A, B, M, N] = -1
\end{aligned}$$