Université Claude Bernard–Lyon I
CAPES de Mathématiques : épreuve 2
Année 2006–2007

Corrigé du CAPES blanc
21/12/2006

I Généralités sur les homographies

I.A Composition d'homographies

I.A.1) Pour $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ et $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$, et z dans $\mathbb{C}$ privé de quelques points, on a :

$$h_A(h_{A'}(z)) = \frac{a\frac{a'z+b'}{c'z+d'} + b}{c\frac{a'z+b'}{c'z+d'} + d} = \frac{(aa'+bc')z + ab' + bd'}{(ca'+dc')z + cb' + dd'}.$$

Pour bien faire, il faudrait dire quelque chose pour les points spéciaux, mais je ne sais pas comment le faire vite.

I.A.2) Si I est la matrice identité, h_I est Id, l'identité de $\mathbb{P}^1$. Par suite, pour $A \in G$ et A^{-1} son inverse, on a : $h_{A^{-1}} \circ h_A = \mathrm{Id} = h_A \circ h_{A^{-1}}$. Ainsi, h_A est bijective, et, en simplifiant par le déterminant, on voit que sa réciproque est l'homographie :

$$h_A^{-1} = h_{A^{-1}} : z \mapsto \frac{dz - b}{-cz + a}.$$

Ainsi, l'ensemble des homographies n'est pas vide, il est stable par produit et par passage à l'inverse, donc c'est un sous-groupe du groupe des bijection de $\mathbb{P}^1$ sur $\mathbb{P}^1$.

I.A.3) Evident. Noter que puisque tout complexe est un carré, pour tout $A \in G$, on peut écrire : $h_A = h_{\delta^{-1}A}$, où $\delta \in \mathbb{C}$ est tel que $\det \delta^{-1}A = 1$, i.e. $\delta^2 = \det(A)$, si bien que toute homographie est l'homographie associée à une matrice de déterminant 1.

I.A.4) L'hypothèse s'écrit : $h_{A^{-1}A'} = \mathrm{Id}$. Si on note $A^{-1}A' = \begin{pmatrix} \lambda & \mu \\ \nu & \pi \end{pmatrix}$, on a donc :

$$\forall z \in \mathbb{C} \setminus \{-\pi/\nu\}, \quad \lambda z + \mu = z(\nu z + \pi).$$

Comme chacun sait, un polynôme qui a une infinité de racines est le polynôme nul, d'où l'on tire : $\lambda = \pi$, $\mu = \nu = 0$. Bien sûr, $\lambda \neq 0$ car sinon, le déterminant serait nul. On en déduit que $A' = \lambda A$, comme souhaité.

I.B Homographies et birapport

I.B.1) Supposons qu'il existe une homographie $h : z \mapsto (az + b)/(cz + d)$ telle que

$$h(z_1) = \infty, \quad h(z_2) = 0, \quad h(z_3) = 1,$$

et vérifions son unicité. Les relations précédentes donnent :

$$cz_1 + d = 0, \quad az_2 + b = 0, \quad az_3 + b = cz_3 + d.$$

Vu que $z_1 \neq z_3$ et $z_3 \neq z_2$, on en tire :

$$b = -az_2, \quad d = -cz_1, \quad a = \frac{z_3 - z_1}{z_3 - z_2}\, c,$$

ce qui prouve l'unicité de h :

$$\forall z \in \mathbb{P}^1, \quad h(z) = \frac{\frac{z_3 - z_1}{z_3 - z_2}(z - z_2)}{z - z_1}.$$

Inversement, du fait que $z_2 \neq z_1$, la formule précédente définit bien une homographie (le déterminant de la matrice n'est pas nul), et on vérifie qu'elle convient.

I.B.2) On vérifie que $h(z_4) = [z_1, z_2, z_3, z_4]$.

I.B.3) On a :

$$h'g(z_1) = h'(z_1') = \infty = h(z_1),\ h'g(z_2) = h'(z_2') = 0 = h(z_2),\ h'g(z_3) = h'(z_3') = 1 = h(z_3),$$

si bien que l'unicité de l'homographie de h dans IB1) donne : $h = h' \circ g$. Mais alors :

$$[z_1', z_2', z_3', z_4'] = h'(z_4') = h' \circ g(z_4) = h(z_4) = [z_1, z_2, z_3, z_4].$$

Noter que la ligne précédente a un sens, car l'injectivité des homographies assure que les quatre points de chaque birapport écrit sont distincts.

Remarque *On peut aussi montrer cette relation par un calcul direct.*

I.C Homographies et cercles

I.C.1) Comme dans le préambule, on confond les points et leurs affixes dans le repère $(0, \overrightarrow{01}, \overrightarrow{0i})$, qu'on décrète orthonormé direct[1]. Soit a, b, c, d quatre points distincts de $\mathbb{C}$. La mesure de l'angle $(\widehat{\overrightarrow{ac}, \overrightarrow{ad}})$ est l'argument de $(d-a)/(c-a)$. De même, celle de $(\widehat{\overrightarrow{bc}, \overrightarrow{bd}})$ est l'argument de $(d-b)/(c-b)$. La différence des mesures est donc

$$(\widehat{\overrightarrow{ac}, \overrightarrow{ad}}) - (\widehat{\overrightarrow{bc}, \overrightarrow{bd}}) = \operatorname{Arg} \frac{d-a}{c-a} \times \frac{d-b}{c-b} = \operatorname{Arg} \frac{1}{[a,b,c,d]} = -\operatorname{Arg}[a,b,c,d] \mod 2\pi.$$

Comme un complexe est réel si et seulement si son argument est un multiple de π, la relation précédente exprime le théorème de l'angle inscrit sous la forme : quatre points sont cocycliques ou alignés SSI leur birapport est réel.

I.C.2) Soit h une homographie et C un cercle ou une droite. On fixe trois points distincts z_1, z_2, z_3 dans C. La question précédente montre qu'un complexe z (distinct de z_1, z_2, z_3) appartient à C si, et seulement si le birapport $[z_1, z_2, z_3, z]$ est réel. On peut appeler ça une caractérisation angulaire des cercles et des droites.

Or, si on note $z_i' = h(z_i)$ (pour $i \in \{1,2,3\}$), on a vu que : $[z_1', z_2', z_3', h(z)] = [z_1, z_2, z_3, z]$. Par suite, z appartient à C si, et seulement si $h(z)$ appartient au cercle ou à la droite C' contenant z_1', z_2', z_3'.

Attention ! *Ceci prouve seulement que $h(C) \subset C'$. En effet, si on prend $z' \in C'$, rien prouve encore qu'il soit l'image d'un point de C.*

Pour conclure, on sait que h est une surjection de $\mathbb{P}^1$ sur $\mathbb{P}^1$. Par suite, tout point $z' \in C'$ est l'image d'un point z de $\mathbb{P}^1$. L'égalité des birapports montre qu'en fait, $z \in C$.

Remarque *L'énoncé était un peu négligent sur un point : pour que l'image d'une droite soit un cercle entier, il faut ajouter à cette droite le point ∞.*

I.C.3) Exemple

a. Soit z un complexe de partie réelle 1, il s'écrit : $z = 1 + it$, $t \in \mathbb{R}$. Pour montrer que $j(z)$ appartient au cercle, on calcule

$$j(z) - \frac{1}{2} = \frac{1}{1+t^2} - \frac{it}{1+t^2} - \frac{1}{2} = \frac{1}{2}\left(\frac{1-t^2}{1+t^2} + \frac{2t\,i}{1+t^2}\right) = \frac{1}{2}\left(\cos\theta + i\sin\theta\right),$$

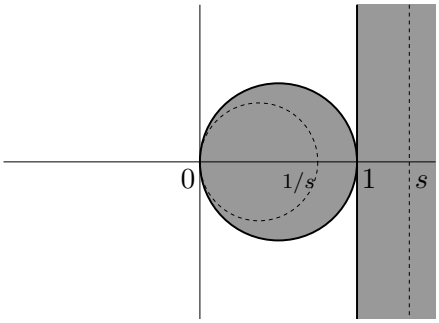
où θ est l'unique réel de $]-\pi, \pi[$ tel que $t = \tan(\theta/2)$. On en déduit d'abord que l'image de la droite $D_1 = \{\mathrm{Re} = 1\}$ est contenue dans le cercle, mais plus précisément que tout point du cercle sauf $0 = 1/2 + 1/2\exp(i\pi)$ (qui correspondrait à $\theta = \pi$ ou $t = \infty$) est l'image par j d'un point de la droite. Si on ajoute que l'image de ∞ est 0, on constate que l'image de la droite est le cercle entier.

[1] C'est encore mal dit. Help!

b. La méthode naturelle consiste à poser $z = s + it$, avec $s > 1$ et $t \in \mathbb{R}$, et à commencer par montrer que $|j(z) - 1/2| < 1/2$. C'est déplaisant.

Constatons plus habilement que P^+ est la réunion des droites $D_s = \{z \in \mathbb{C} : \operatorname{Re} z = s\}$, lorsque s parcourt $]1, +\infty[$. Fixons $s > 1$. L'image de D_s est un cercle ou une droite (privé du point 0, car $\infty \notin D_s$). Or, comme $D_s \cap D_1 = \emptyset$ et que j est injective, $j(D_s)$ ne coupe pas le cercle $j(D_1)$ qui borde Q^+. Comme toute droite passant par $j(s) = 1/s$ coupe le cercle $j(D_1)$, l'image $j(D_s)$ est un cercle contenu dans Q^+. (Plus précisément, c'est le cercle de diamètre $[0, 1/s]$.)

Le même raisonnement montre que l'image de $D_t = \{\mathrm{Re} = t\}$ ne coupe pas le disque Q^+ pour $t \leq 1$. Mais tout élément de Q^+ possède un antécédent par j dans $\mathbb{P}^1$, c'est donc que cet antécédent est dans une des droites D_s pour $s > 1$.



c. On montrerait de même que l'image de la droite $\{\operatorname{Re} z = -1\}$ est le cercle de centre $-1/2$ et de rayon $1/2$, et que celle du demi-plan $\{\operatorname{Re} z > -1\}$ est le disque ouvert Q^- bordé par ce cercle.

II Le groupe $\Gamma(2) = \langle u, v \rangle$: un groupe libre

On note $\Gamma(2)$ le groupe engendré par u et v dans le groupe des homographies. On note aussi

$$P^- = \{z \in \mathbb{C},\ \operatorname{Re} z < -1\}, \quad P^+ = \{z \in \mathbb{C},\ \operatorname{Re} z > 1\}, \quad P_0 = \{z \in \mathbb{C},\ -1 < \operatorname{Re} z < 1\},$$

$$Q^- = \left\{z \in \mathbb{C},\ \left|z + \frac{1}{2}\right| < \frac{1}{2}\right\}, \quad Q^+ = \left\{z \in \mathbb{C},\ \left|z - \frac{1}{2}\right| < \frac{1}{2}\right\}, \quad Q_0 = \mathbb{C} \setminus \overline{Q^+ \cup Q^-}.$$

II.A Le groupe $\Gamma(2)$

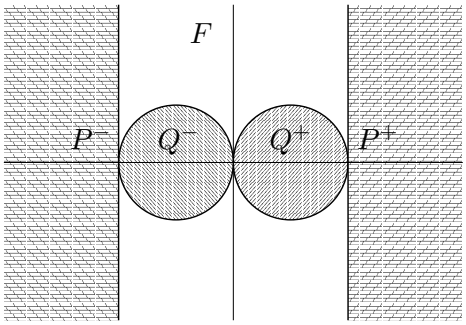
II.A.1) En prenant $n = 1$, $k_1 = 1$, on constate que Γ' contient u et v ; en particulier, il n'est pas vide. Si $w = w_1^{k_1} \cdots w_n^{k_n}$ et $w' = {w'_1}^{k'_1} \cdots {w'_{n'}}^{k'_{n'}}$ sont deux éléments de Γ', alors $w^{-1}w' = w_n^{-k_n} \cdots w_1^{-k_1} {w'_1}^{k'_1} \cdots {w'_{n'}}^{k'_{n'}}$ appartient à Γ. Ceci finit de prouver que Γ' est un sous-groupe de $\Gamma(2)$ contenant u et v.
Puisqu'un sous-groupe contient tous les produits et les inverses de ses éléménts, le sous-groupe engendré par u et v contient Γ'. C'est fini.
II.A.2) On montre le résultat par récurrence $n+|k_1|+\cdots+|k_n|$. Appelons réduite une écriture $w_1^{k_1} \cdots w_n^{k_n}$ telle que pour tout $1 \leq i \leq n$, $k_i \neq 0$ et pour tout $1 \leq i \leq n-1$, $w_i \neq w_{i+1}$. Pour $N \in \mathbb{N}^*$, on note H_N l'assertion suivante : tout élément de $\Gamma(2) \setminus \{\mathrm{Id}\}$, de la forme $w_1^{k_1} \cdots w_n^{k_n}$ avec $n + |k_1| + \cdots + |k_n| = N$, possède une écriture réduite.
L'assertion H_1 est vide : si $n + |k_1| + \cdots + |k_n| = 1$, alors nécessairement $n = 1$ et $k_1 = 0$, si bien que l'élément noté $w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n}$ est Id.
Pour $N = 2$, on a nécessairement $n = 1$ et $k_1 = \pm 1$, et la décomposition est réduite : il n'y a rien à démontrer
Supposons que pour un certain $N \geq 2$, H_2,..., H_{N-1} soient vraies et soit $g = w_1^{k_1} \cdots w_n^{k_n}$ avec $n + |k_1| + \cdots + |k_n| = N$. Si la décomposition n'est pas réduite, on est dans l'un des deux cas suivants :

- si l'un des k_i est nul, on peut supprimer le w_i correspondant et obtenir une décomposition du même type avec $n-1$ à la place de n, et $N-1$ à la place de N ;
- si, pour un certain i, on a $w_i = w_{i+1}$, on remplace $w_i^{k_i} w_{i+1}^{k_{i+1}}$ par $w_i^{k_i+k_{i+1}}$, ce qui donne une décomposition du même type avec $N' = n-1+|k_1|+\cdots+|k_i+k_{i+1}|+\cdots+|k_n|$ à la place de N ; notons qu'alors, $n-1<n$ et $|k_i+k_{i+1}| \leq |k_i|+|k_{i+1}|$, si bien que $N'<N$.

Dans chaque cas, l'hypothèse de récurrence fournit une décomposition réduite. On conclut.

II.B Action de u et v sur certains disques

II.B.1) Voici un joli dessin :



II.B.2) Pour z tel que $\mathrm{Re}\, z > -1$, on a : $\mathrm{Re}\, z + 2 > 1$. Ainsi : $u(P_0) \subset P^+$ et $u(P^+) \subset P^+$. Une récurrence immédiate montre que pour tout $k \in \mathbb{N}^*$, on a : $u^k(P_0) \subset P^+$. De même, $u^{-1}(P_0) \subset P^-$ et $u^{-1}(P^-) \subset P^-$, ce qui permet de montrer que pour $k \in \mathbb{N}^*$, $u^{-k}(P_0) \subset P^-$.

II.B.3) Puisque $j = h_J$, où $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, il suffit de calculer :

$$JUJ^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = V.$$

II.B.4) Effet de la conjugaison par j sur les disques

Idée *Le principe est simple mais* très *souvent utile : quand on conjugue une transformation u par une transformation j, i.e. quand on calcule juj^{-1}, on obtient une transformation de même "nature géométrique" que u, dont les "éléments caractéristiques" sont les images par j des éléments correspondants de u.*
Dans notre cas très précis, la propriété que $u^k(P_0) \subset P^\pm$ va automatiquement se traduire en : $v^k(j(P_0)) \subset j(P^\pm)$. Il n'y a plus qu'à reconnaître $j(P_0)$ et $j(P^\pm)$.

Comme P_0 est l'intérieur du complémentaire de $P^+ \cup P^-$ et que j est un homéomorphisme de $\mathbb{P}^1$ qui envoie $P^+ \cup P^-$ sur $Q^+ \cup Q^-$, on a : $j(P_0) = Q_0$.
On en déduit que pour $k > 0$, on a : $v^k(Q_0) = ju^k j^{-1} j(P_0) = ju^k(P_0) \subset j(P^+) = Q^+$. On en tire : $v^k(Q_0) \subset Q^+$ et de même : $v^{-k}(Q_0) \subset Q^-$.
II.B.5) Soit $k \in \mathbb{N}^*$ et $\eta \in \{+,-\}$. Comme $Q^\eta \subset P_0$, on a : $u^k(Q^\eta) \subset u^k(P_0) \subset P^+$. Comme $P^\eta \subset Q_0$, on a : $v^k(P^\eta) \subset v^k(Q_0) \subset Q^+$.
De même, on montrerait : $u^{-k}(Q^\eta) \subset P^-$ et $v^{-k}(P^\eta) \subset Q^-$.

II.C Liberté de $\Gamma(2)$

II.C.1) L'idée, c'est qu'en appliquant des u et des v à un élément de F, on ne revient jamais dans F.

a. Si $w_n = u$, on a : $w_n^{k_n}(F) \subset u^{k_n}(P_0) \subset P^\varepsilon$, où ε est le signe de k_n. On en déduit que $w_{n-1}^{k_{n-1}} w_n^{k_n}(F) \subset v^{k_{n-1}}(Q_0) \subset Q^{\varepsilon'}$, où ε' est le signe de k_{n-1}. Par une récurrence descendante triviale, dont le pas est prouvé en IIB5), on voit que $g(F)$ est contenu dans un des disques $P^\pm$ ou $Q^\pm$, selon la parité de n.

b. Par définition de F, l'intersection de F et de $P^+ \cup P^- \cup Q^+ \cup Q^-$ est vide. Or, si on choisit $z \in F$ quelconque, son image $g(z)$ appartient à $P^+ \cup P^- \cup Q^+ \cup Q^-$: par suite, $g(z) \neq z$ et $g \neq \mathrm{Id}$.

II.C.2) Supposons que les deux décompositions ne coïncident pas. Soit i l'indice minimal tel que $w_i \neq w'_i$ ou $k_i \neq k'_i$. Quitte à simplifier par $w_1^{k_1} \cdots w_{i-1}^{k_{i-1}} = {w'_1}^{k'_1} \cdots {w'_{i-1}}^{k'_{i-1}}$ et à renuméroter, on peut supposer que $i = 1$. Mais alors, considérons $\mathrm{Id} = w_n^{-k_n} \cdots w_1^{-k_1} {w'_1}^{k'_1} \cdots {w'_{n'}}^{k'_{n'}}$. Deux cas :

- soit $w_1 \neq w'_1$, et alors $w_n^{-k_n} \cdots w_1^{-k_1} {w'}_1^{k'_1} \cdots {w'_{n'}}^{k'_{n'}}$ est une décomposition réduite ;
- soit $w_1 = w'_1$ et $k_1 \neq k'_1$, et alors $w_n^{-k_n} \cdots w_2^{-k_2} w_1^{-k_1+k'_1} {w'_2}^{k'_2} \cdots {w'_{n'}}^{k'_{n'}}$ est réduite.

Dans les deux cas, la question précédente contredit le fait que l'élément désigné est l'identité. Par suite, les décompositions coïncident.

Remarque *On dit que* $\Gamma(2)$ *est isomorphe au groupe libre sur deux lettres.*

II.D Domaine fondamental

II.D.1) On note $g : Z \mapsto (aZ+b)/(cZ+d)$. Vu que $\Gamma(2)$ est engendré par $u = h_U$ et $v = h_V$, où U et V ont pour déterminant 1, g est l'homographie associée à une matrice qui est un produit de puissances de U et de V : cette matrice a donc pour déterminant 1, si bien qu'on peut supposer que $ad - bc = 1$. Notons $z = x + iy$, avec $x \in \mathbb{R}$ et $y \in \mathbb{R}_+^*$. On a alors :

$$\mathrm{Im}\, g(z) = \mathrm{Im}\, \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \mathrm{Im}\, \frac{(ax+b+iay)(cx+d-icy)}{|cz+d|^2} = \frac{(ad-bc)y}{|cz+d|^2} = \frac{\mathrm{Im}\, z}{|cz+d|^2}.$$

II.D.2) Rappelons que ε et z sont fixés. Soit g comme avant. De $|cz+d| \geq |c\,\mathrm{Im}(z)|$, on tire :

$$|c| > \frac{1}{\sqrt{\varepsilon\,\mathrm{Im}\, z}} \quad \Longrightarrow \quad \mathrm{Im}\, g(z) \leq \frac{\mathrm{Im}\, z}{|c|^2\,\mathrm{Im}(z)^2} = \frac{1}{|c|^2\,\mathrm{Im}\, z} < \varepsilon.$$

De plus, $|cz+d| \geq |d| - |cz|$, donc :

$$|c| \leq \frac{1}{\varepsilon\,\mathrm{Im}\, z} \text{ et } |d| > \frac{|z|}{\sqrt{\varepsilon\,\mathrm{Im}\, z}} + \sqrt{\frac{\mathrm{Im}\, z}{\varepsilon}} \quad \Longrightarrow \quad \mathrm{Im}\, g(z) \leq \frac{\mathrm{Im}\, z}{(|d|-|cz|)^2} \leq \frac{\mathrm{Im}\, z}{\left(|d| - \frac{|z|}{\sqrt{\varepsilon\,\mathrm{Im}\, z}}\right)^2} < \varepsilon.$$

Ainsi, à part pour un nombre fini de couples (c,d), on a : $\mathrm{Im}\, g(z) < \varepsilon$.

Il n'est pas nécessaire de faire des majorations si précises. On peut aussi dire ce qui suit.
Deuxième version : Puisque pour tout (c,d), on a : $|cz+d| \geq |cz|$ et que $\lim_{|c|\to+\infty} |cz| = +\infty$, il existe $C \in \mathbb{N}$ tel que pour tout c, $|c| > C$ entraîne $\mathrm{Im}\, g(z) = \mathrm{Im}(z)/|cz+d|^2 < \varepsilon$. Si $|c| \leq C$ et $|d|$ assez grand (tel que $|d| > C|z|$), on a : $\mathrm{Im}\, g(z) \leq \mathrm{Im}(z)/(|d|-|cz|)^2 \leq \mathrm{Im}(z)/(|d|-C|z|)^2$. Or, cette quantité tend vers 0 lorsque $|d|$ tend vers l'infini, si bien que pour $D \in \mathbb{N}$ convenable et tout (c,d) tel que $|c| \leq C$ et $|d| \geq D$, on a : $\mathrm{Im}\, g(z) < \varepsilon$. Ainsi, dès que $|c| > C$ ou que $|d| > D$, ce qui est vrai pour tous les couples (c,d) sauf un nombre fini, on a : $\mathrm{Im}\, g(z) < \varepsilon$.
II.D.3) Fixons par exemple $\varepsilon = \mathrm{Im}\, z$. L'ensemble $\mathcal{I}_z \cap [\varepsilon, +\infty[$ étant fini, il possède un élément maximal, qui est aussi un élément maximal de $\mathcal{I}_z$.
II.D.4) Soit $z' \in \mathcal{O}_z$ de partie imaginaire maximale. Il existe un unique $k \in \mathbb{Z}$ tel que $-1 \leq \mathrm{Im}\, z' - 2k < 1$, à savoir, la partie entière de $(\mathrm{Im}\, z + 1)/2$. Alors, $u^{-k}(z')$ a la même partie imaginaire que z', et une partie réelle dans l'intervalle $[-1,1]$.

II.D.5) Comme $z'' \in Q^+$, on a : $|2z''+1| < 1$. Par suite :

$$\operatorname{Im} v(z'') = \operatorname{Im} \frac{z''}{2z''+1} = \operatorname{Im} \frac{2|z''|^2 + z''}{|2z''+1|^2} = \frac{\operatorname{Im} z''}{|2z''+1|^2} > \operatorname{Im} z''.$$

On montrerait de même que si $z'' \in Q^-$, alors $\operatorname{Im} v^{-1}(z'') > \operatorname{Im} z''$.
II.D.6) Soit $z'' = g(z')$. D'après la question précédente, la maximalité de $\operatorname{Im} z''$ dans $\mathcal{O}_z$ exclut que z'' appartienne à Q^+ et à Q^-. Par suite, $z'' = g(z') \in \overline{F}$.
II.D.7) Avec les notations précédentes, il existe $h \in \Gamma(2)$ tel que $z' = h(z)$. Mais alors, on a : $z = h^{-1} \circ g^{-1}(z'')$, avec $h^{-1} \circ g^{-1} \in \Gamma(2)$ et $z'' \in \overline{F}$.

Remarque *Avec quelques calculs supplémentaires, on peut montrer que si $z \in \overline{F}$ et $g \in \Gamma(2)$ sont tels que $g(z) \in \overline{F}$, alors $g = \mathrm{Id}$, ou alors z appartient au bord de F et g est $u^{\pm 1}$ ou $v^{\pm 1}$.*

III Le groupe $\tilde{\Gamma} = \operatorname{Ker}(PSL_2(\mathbb{Z}) \to PSL_2(\mathbb{Z}/2\mathbb{Z}))$

III.A Le groupe $\tilde{\Gamma}$, un groupe presque libre

III.A.1) Bien sûr, $\tilde{\Gamma}$ n'est pas vide, puisqu'il contient U et V. Vérifions que c'est un sous-groupe de $GL_2(\mathbb{C})$. Par multiplicativité du déterminant, le produit de deux éléments de $\tilde{\Gamma}$ a pour déterminant 1. Le produit de deux éléments quelconques de $\tilde{\Gamma}$ est, avec des notations évidentes :

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}.$$

On a alors : $aa'+bc' \equiv cb'+dd' \equiv 1$ [2], $ab'+bd' \equiv ca'+dc' \equiv 0$ [2], ce qui prouve que $\tilde{\Gamma}$ est stable par produit.
Enfin, comme les éléments de $\tilde{\Gamma}$ ont pour déterminant 1, on a :

$$\forall A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \tilde{\Gamma}, \quad A^{-1} = \frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \in \tilde{\Gamma}.$$

Idée *On veut montrer que U et V engendrent $\tilde{\Gamma}$. Pour cela, on se rappelle que U et V sont des matrices "élémentaires", et que multiplier une matrice à gauche par U ou V, c'est faire des combinaisons linéaires des lignes. A l'aide d'opérations élémentaires bien choisies, on fait baisser la quantité $\delta(A)$, jusqu'à arriver à une matrice triangulaire supérieure.*

III.A.2) *Il faut supposer que $|a| \neq |c|$, sans quoi le résultat est faux !*
Si $0 < |c| < |a|$, on a : $-|a| < |a| - 2|c| < |a|$, d'où : $\Big||a| - 2|c|\Big| < |a| = \max(|a|, |c|)$. Comme l'assertion à démontrer est symétrique en a et c, il n'y a rien à ajouter.
III.A.3) *Il faut supposer que $\delta(A) > 1$, sans quoi le résultat est faux !* Puisque a est impair, il n'est pas nul, d'où : $\delta(A) \geq 1$. Si $\delta(A) = 1$, pas moyen de faire baisser $\delta(A)$!
On commence par calculer WA pour $W \in \{U^{\pm 1}, V^{\pm 1}\}$:

$$U^{\pm 1}A = \begin{pmatrix} a \pm 2c & b \pm 2d \\ c & d \end{pmatrix}, \quad V^{\pm 1}A = \begin{pmatrix} a & b \\ c \pm 2a & d \pm 2b \end{pmatrix}.$$

On a déjà dit que a n'est pas nul. Si c est nul, alors $ad = 1$ donc $\delta(A) = |a| = 1$.
Supposons désormais $\delta(A) \geq 2$. Alors, a et c ne sont pas nuls, et de plus : $|a| \neq |c|$, puisque les parités de a et c sont différentes. D'après la question précédente, $|a| - 2|c|$ ou $|c| - 2|a|$ a une valeur absolue strictement plus petite que $\max(|a|, |c|)$.

- Supposons que $|c| < |a|$, de sorte que $\Big||a| - 2|c|\Big| < \max(|a|, |c|)$; si a et c sont de même signe, $\delta(U^{-1}A) < \delta(A)$; sinon, $\delta(UA) < \delta(A)$;
- De même, supposons que $|a| < |c|$, de sorte que $\Big||c| - 2|a|\Big| < \max(|a|, |c|)$; si a et c sont de même signe, $\delta(V^{-1}A) < \delta(A)$; sinon, $\delta(VA) < \delta(A)$.

III.A.4) *Il faut supposer que* $A \neq \mathrm{Id}$*, sinon le résultat est faux.*
Supposons $\delta(A) = 1$. Comme c est pair et $|c| \leq \delta(A)$, on a : $c = 0$. Par suite, $a = \pm 1$. Comme $ad = 1$, il vient : $d = a = \pm 1$, et bien sûr, b est pair. Mais alors, on a : $A = aV^{b/2}$, qui est de la forme voulue.
Soit $n \in \mathbb{N}^*$, supposons que toute matrice $A' \in \tilde{\Gamma}$ telle que $\delta(A') \leq n$ puisse s'écrire sous la forme voulue. Soit alors $A \in \tilde{\Gamma}$ avec $\delta(A) = n + 1$. D'après la question précédente, il existe $W \in \{U^{\pm 1}, V^{\pm 1}\}$ tel que $\delta(WA) < \delta(A)$. On applique l'hypothèse de récurrence à $A' = WA$, ce qui donne une décomposition de $A = W^{-1}A'$ comme dans II.A.2). On applique alors le même raisonnement qu'en II.A.3) pour trouver une décomposition réduite, i.e. satisfaisant de plus : $W_i \neq W_{i+1}$ et $k_i \neq 0$.

Remarque *On en déduit que* $\Gamma(2)$ *est formé des homographies définies par les matrices de* $\tilde{\Gamma}$*. Plus précisément,* $\Gamma(2)$ *est isomorphe au quotient de* $\tilde{\Gamma}$ *par* $\{\pm \mathrm{Id}\}$*.*

III.A.5) Soit $\varepsilon, \varepsilon' \in \{-1, 1\}$, $r, r' \in \mathbb{N}^*$, $(W_1, \ldots, W_r) \in \{U, V\}^r$, $(W'_1, \ldots, W'_{r'}) \in \{U, V\}^{r'}$, $(k_1, \ldots, k_r) \in \mathbb{Z}^{*r}$ et $(k'_1, \ldots, k'_{r'}) \in \mathbb{Z}^{*r'}$ tels que

$$A = \varepsilon\, W_1^{k_1} W_2^{k_2} \cdots W_r^{k_r} = \varepsilon'\, {W'_1}^{k'_1} \cdots {W'_{r'}}^{k'_{r'}}$$

et pour tout i, i', $W_i \neq W_{i+1}$, $W'_{i'} \neq W'_{i'+1}$.
Considérons l'homographie h_A. Si on note $w_i \in \{u, v\}$ l'homographie associée à $W_i \in \{U, V\}$, et de même pour $w'_{i'}$, on a avec I.A.1) :

$$w_1^{k_1} w_2^{k_2} \cdots w_r^{k_r} = {w'_1}^{k'_1} \cdots {w'_{r'}}^{k'_{r'}} \in \Gamma(2).$$

D'après II.C.2), on a : $r = r'$ et, pour tout i, $w_i = w'_i$ et $k_i = k'_i$. D'où, pour tout i, $W_i = W'_i$. Reste à voir que $\varepsilon = \varepsilon'$, ce qui est évident après simplification par les produits de W_i dans l'expression de A.

III.B Complétions d'une colonne

III.B.1) Pour $m, n \in \mathbb{Z}$ avec $m \wedge n = 1$, le "théorème de Bezout" assure qu'il existe $p, q \in \mathbb{Z}$ tel que $mq - np = 1$.
III.B.2) Supposons de plus que m est impair et n est pair et soit $(p, q) \in \mathbb{Z}^2$ tel que $mq - np = 1$. Notons que comme n est pair, q est nécessairement impair, sans quoi $mq - np$ est pair. Si p est pair, on a gagné. Si p est impair, on pose $p' = p + m$ et $q' = q + n$: alors p' est pair, q' est toujours impair, et $mq' - np' = mq - np = 1$. La matrice dont les lignes sont $(m\ p')$ et $(n\ q')$ convient.
III.B.3) Puisque A et A' sont dans $\tilde{\Gamma}$, leur déterminant est 1, d'où, par différence : $m(q' - q) = n(p' - p)$. Comme m et n sont premiers entre eux, le lemme de Gauss donne : $m | (p' - p)$. Il existe donc $j \in \mathbb{Z}$ tel que $p' - p = jm$, d'où l'on tire en remplaçant : $q' - q = jn$. Or, comme p et p' sont tous deux pairs et que m est impair, j est pair. On écrit $j = 2k$, puis on constate que les relations $p' = p + 2km$ et $q' = q + 2km$ signifient exactement que $A' = AU^k$.
Inversement (l'énoncé est un peu vague sur le sens de la réciproque), un calcul direct montre que pour tout $k \in \mathbb{Z}$, A et AU^k ont la même première colonne.

III.C Une bijection

L'énoncé ne précise pas que pour $\varepsilon = \pm 1$*,* $\Phi(\varepsilon \mathrm{Id}) = \varepsilon \mathrm{Id}$.
On montre par récurrence sur $\ell(A) = |k_1| + \cdots + |k_r|$ que

$$A = \varepsilon\, W_1^{k_1} W_2^{k_2} \cdots W_r^{k_r} = \begin{pmatrix} m & p \\ n & q \end{pmatrix} \implies \Phi(A) = \begin{pmatrix} m & -p \\ -n & q \end{pmatrix}.$$

C'est évident pour $\ell(A) = 1$ par calcul immédiat des inverses de U et V. Pour montrer le pas de récurrence, on calcule :

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} m & p \\ n & q \end{pmatrix} = \begin{pmatrix} m+2n & p+2q \\ n & q \end{pmatrix}, \quad \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} m & -p \\ -n & q \end{pmatrix} = \begin{pmatrix} m+2n & -p-2q \\ -n & q \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} m & p \\ n & q \end{pmatrix} = \begin{pmatrix} m & p \\ n+2m & q+2p \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}\begin{pmatrix} m & -p \\ -n & q \end{pmatrix} = \begin{pmatrix} m & -p \\ -n-2m & q+2p \end{pmatrix}.$$

On en déduit que si, pour $\ell(A) = N$

IV Enumération des triplets pythagoriciens

IV.A Réduction aux TP primitifs

IV.A.1) Soit (x, y, z) un TP et d le pgcd de x, y et z. Ecrivons $x = dx'$, $y = dy'$ et $z = dz'$. Comme l'équation $x^2 + y^2 = z^2$ est homogène de degré 2, (x', y', z') est un TP, et il est primitif par construction.

IV.A.2) Soit (x, y, z) un TP primitif. En écrivant $z^2 = x^2 + y^2$ (resp. $y^2 = z^2 - x^2$, resp. $x^2 = z^2 - y^2$), on voit que si un nombre divise x et y (resp. z et x, resp. z et y), alors il divise z (resp. y, resp. x), donc il divise le pgcd de (x, y, z), qui vaut 1. Ainsi, x, y et z sont premiers entre eux deux à deux.

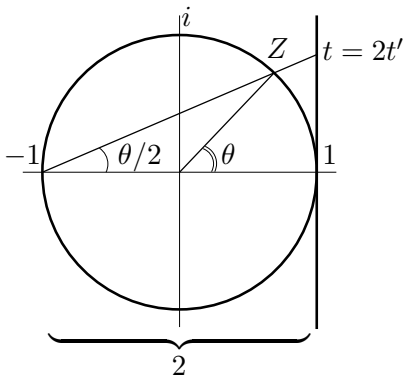
En particulier, x et y ne sont pas tous les deux pairs. Mais en supposant qu'ils sont tous les deux impairs, disons $x = 2k + 1$ et $y = 2\ell + 1$, on voit d'abord que z est pair, puis, en écrivant $z = 2m$, en remplaçant et en divisant par 2, il vient :

$$4k^2 + 4k + 4\ell^2 + 4\ell + 2 = 4m^2 + 4m, \quad \text{d'où :} \quad 2(k^2 + k + \ell^2 + \ell - m^2 - m) + 1 = 0,$$

ce qui est impossible. Ainsi, x et y sont de parités différentes et z et impair.

IV.B Paramétrage des TP primitifs

IV.B.1) Voici un dessin.



IV.B.2) Par construction, on a : $Z \neq -1$. Soit $\theta \in]-\pi, \pi[$ tel que $Z = \exp(i\theta)$. Par le théorème de l'angle inscrit, l'argument de $(1 + it) - (-1)$ est $\theta/2$, d'où :

$$\tan\frac{\theta}{2} = \frac{t}{2}.$$

En notant $t' = t/2$, il vient :

$$Z = \cos\theta + i\sin\theta = \frac{1 - t'^2}{1 + t'^2} + \frac{2t'}{1 + t'^2}\, i.$$

Eh oui, encore une coquille dans l'énoncé. Repassez dans 2 ans, il sera plus propre !

IV.B.3) La coquille ne prête pas trop à conséquence, car t est rationnel SSI t' est rationnel. Il est clair que si t (ou t') est rationnel, alors $\operatorname{Re} Z$ et $\operatorname{Im} Z$ sont rationnels. Inversement, supposons que $\operatorname{Re} Z$ et $\operatorname{Im} Z$ sont rationnels. Alors, constatant que $\operatorname{Re} Z \neq -1$, on a :

$$\operatorname{Re} Z = \frac{1-t'^2}{1+t'^2} \iff t'^2 = \frac{\operatorname{Re} Z - 1}{-\operatorname{Re} Z - 1}.$$

On en tire que t'^2 est rationnel. Mais alors, on a : $t' = (1+t'^2)\operatorname{Im} Z/2$, donc t' est rationnel.
IV.B.4) Soit (x,y,z) un TP primitif. Si x ou y est nul, on peut prendre $m=1$ et $n=0$ ou $m=0$ et $n=1$, ce qui marche au signe de z près. Supposons désormais $xy \neq 0$, d'où $z \neq 0$.
Quitte à permuter x et y, on peut supposer que x est impair et y est pair. Alors, $Z = x/z + iy/z$ est un point du cercle unité, autre que ± 1. La droite passant par -1 et Z coupe la droite $\{\mathrm{Re} = 1\}$ en un point noté $1+it$, avec $t \in \mathbb{R}$. Evidemment, le point Z est l'autre intersection de la droite contenant -1 et $1+it$ et du cercle, donc on peut appliquer ce qui précède. En notant $t' = t/2$, on voit que t' est rationnel. On l'écrit sous la forme n/m, où $m, n \in \mathbb{Z}^*$ et $m \wedge n = 1$. En chassant les dénominateurs dans l'expression de x/z, on trouve :

$$(*) \qquad (m^2+n^2)\,x = (m^2-n^2)\,z \quad \text{et} \quad (m^2+n^2)\,y = 2mn\,z.$$

Puisque z divise $x(m^2+n^2)$ et est premier avec x, le lemme de Gauss donne l'existence de $d \in \mathbb{Z}$ tel que $m^2+n^2 = dz$. En reportant et en simplifiant par z, on trouve : $m^2 - n^2 = dx$. Si d admet un diviseur premier p, on a donc : $p|(m^2+n^2)$ et $p|(m^2-n^2)$, d'où : $p|2m^2$ et $p|2n^2$. Comme m et n sont premiers entre eux, le lemme de Gauss montre que $p=2$.
On veut montrer que c'est impossible. Pour cela, il suffit de montrer que m et n sont de parités différentes (car alors, $m^2 \pm n^2$ sera impair). Comme $m \wedge n = 1$, m et n ne sont pas tous deux pairs. Supposons-les tous deux impairs. Alors m^2+n^2 est pair, si bien que $(m^2+n^2)y$ est divisible par 4. Comme m, n et z sont impairs, $2mnz$ n'est pas divisible par 4, d'où une contradiction.
Ainsi, d n'a pas de diviseur premier, et donc, à permutation de x et y près, on a :

$$x = \pm(m^2-n^2), \quad y = \pm 2mn, \quad z = \pm(m^2+n^2),$$

où m et n sont premiers entre eux et de parités différentes.

IV.C Enumération des TP primitifs positifs

IV.C.1) La surjectivité de f a été prouvée à la question précédente.
IV.C.2) Soit $A \in \tilde{\Gamma}$. Alors, on a, en ignorant ce qui se passe sur la deuxième colonne :

$$A = \begin{pmatrix} m & * \\ n & * \end{pmatrix} \quad \Longrightarrow \quad \Phi(A) = \begin{pmatrix} m & * \\ -n & * \end{pmatrix}, \quad -A = \begin{pmatrix} -m & * \\ -n & * \end{pmatrix}, \quad -\Phi(A) = \begin{pmatrix} -m & * \\ n & * \end{pmatrix}.$$

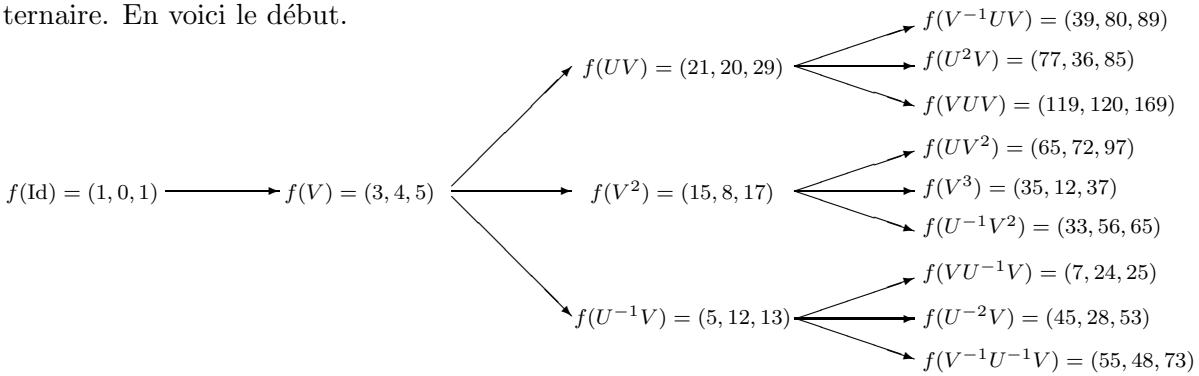
De plus, la multiplication à droite par U^k (pour $k \in \mathbb{Z}$) ne change pas la première colonne d'une matrice. D'où pour $\varepsilon \in \{-1,1\}$ et $k \in \mathbb{Z}$, $f(\varepsilon A U^k) = f(\varepsilon \Phi(A) U^k) = f(A)$.
Inversement, supposons que A et A' ont la même image (x,y,z) par f. Notons ${}^t(m\ n)$ la première colonne de A, ${}^t(m'\ n')$ celle de A'. En posant $Z = x/z + iy/z$, on voit comme ci-dessus que

$$\frac{n^2}{m^2} = \frac{z-x}{z+x} = \frac{n'^2}{m'^2}.$$

Or, d'après le lemme de Gauss, $m^2 \wedge n^2 = m'^2 \wedge n'^2 = 1$, donc n^2/m^2 et n'^2/m'^2 sont des fractions irréductibles, d'où : $m^2 = m'^2$ et $n^2 = n'^2$. On en déduit que (m,n) et (m',n') coïncident aux signes près.
En d'autres termes, A' et l'une des matrices A, $-A$, $\Phi(A)$ et $-\Phi(A)$ ont la même première colonne. D'après III.B.3), elles diffèrent d'une puissance de U.

IV.C.3) D'après la question précédente et III.A.4), un TP primitif positif (x, y, z) *non trivial ($xyz \neq 0$), où x est impair* est l'image par f d'un élément $A \in \tilde{\Gamma}$ de la forme $A = \varepsilon W_1^{k_1} W_2^{k_2} \cdots W_r^{k_r}$ (dans les notations de III.A.4)). Comme $f(A) = f(\varepsilon A)$, quitte à remplacer A par εA, on peut supposer que $\varepsilon = 1$. Comme $f(A) = f(AU^k)$ pour tout k, quitte à remplacer A par AU^{-k_r} si $W_r = U$, on peut supposer que $W_r = V$. Enfin, comme $f(A) = f(\Phi(A))$, quitte à remplacer A par $\Phi(A)$, on peut supposer $k_r > 0$. Il n'y a plus qu'à renuméroter les W_i (selon la parité de r).
Pour l'unicité, la clé est III.A.5). Détails laissés au lecteur assidu.

On peut à présent ranger les TP primitifs positifs sur les sommets d'un graphe. On met une arête entre les sommets $f(A)$ et $f(A')$ si on a $A' = WA$ pour un certain $W \in \{U^{\pm 1}, V^{\pm 1}\}$. Le fait que $\Gamma(2)$ soit un groupe libre entraîne que le graphe obtenu est un arbre, évidemment ternaire. En voici le début.



Sources

- la partie I est très classique ; voir par exemple M. Audin, *Géométrie* ;
- l'argument utilisant les disques pour montrer que $\Gamma(2)$ est libre dans la partie II est tiré du superbe et très riche livre *Indra's pearls*, de D. Mumford, C. Series et D. Wright, Cambridge University Press ;
- l'argument relatif au domaine fondamental est inspiré par le *Cours d'arithmétique* de J.-P. Serre ;
- l'argument provenant des manipulations sur les lignes et les colonnes pour montrer l'engendrement de $\tilde{\Gamma}$ par U, V et $-\mathrm{Id}$ est semi-classique ; c'est A. Tchoudjem qui m'a aidé à le mettre au clair (récurrence sur $\max(|a|, |c|)$, et pas sur $c^2 + d^2$!) ;
- l'utilisation de $\tan(\theta/2)$ pour paramétrer les points à coordonnées rationnelles du cercle unité, puis les triplets pythagoriciens, est classique ;
- la façon de "ranger" les triplets pythagoriciens selon un arbre ternaire a été inventée par plein de gens :
  - le premier aurait été J. F. M. Barning vers 1963 ;
  - on trouve une version totalement élémentaire (traduire : lisible) et un peu "magique" dans l'article de P. Préau, *Un graphe ternaire associé à l'équation $X^2 + Y^2 = Z^2$*, C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), no. 7, pp. 665–668 ;
  - sous la forme ci-dessus, la source d'inspiration principale a été l'article de R. Alperin, *The modular tree of Pythagoras*, *Amer. Math. Monthly* 112, November 2005, voir `www.math.sjsu.edu/~alperin/pt.pdf` ;
  - le premier dessin du sujet est classique, mais je l'ai trouvé dans l'article de D. Romik, *The dynamics of Pythagorean triples*, voir par exemple `http://cm.bell-labs.com/who/romik/a/explanations/pyth.html`.