Des homographies à l'énumération des triplets pythagoriciens

Nathan Noiry

21 juin 2013

On se propose dans ce document d'énumérer les triplets pythagoriciens à l'aide d' un sous-groupe du groupe $\mathrm{PSL}_2(\mathbb{Z})$. Pour cela, on commencera par énoncer quelques généralités sur les homographies, on étudiera ensuite l'action d'un groupe d'homographie particulier. On sera alors en mesure de faire le lien entre un sous-groupe de $\mathrm{PSL}_2(\mathbb{Z})$ et les triplets pythagoriciens. Le lien en question a été exposé dans [1].

1 Généralités sur les homographies

Une homographie est une application de $\mathbb{P}^1$ dans $\mathbb{P}^1$, l'ensemble $\mathbb{P}^1$ étant l'ensemble des nombres complexes auquel on ajoute un point à l'infini : $\mathbb{P}^1 = \mathbb{C} \cup \{\infty\}$. On associe une homographie à une matrice 2×2 à coefficients complexes.
Plus précisément, à $A \in \mathcal{M}_2(\mathbb{C})$, on associe l'homographie h_A de $\mathbb{P}^1$ dans $\mathbb{P}^1$ définie par :

$$\forall z \in \mathbb{P}^1, \quad h_A(z) = \frac{az+b}{cz+d}, \quad \text{où} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

On utilise les conventions habituelles sur l'infini. Ainsi, lorsque $c = 0$, $h_A(\infty) = \infty$. Sinon lorsque $c \neq 0$, on a $h_A(-d/c) = \infty$ et $h_A(\infty) = a/c$. L'homographie h_A est une bijection lorsque $ad - bc \neq 0$, dans le cas contraire c'est la fonction constante égale à a/c. On ne considèrera pas ici ce second cas, qui présente peu d'intérêt. On nommera ainsi abusivement homographie une application h_A avec $A \in \mathrm{GL}_2(\mathbb{C})$, et l'on notera H l'ensemble de ces homographies.

1.1 Le groupe des homographies

On va montrer dans cette partie que H est un groupe et que H est isomorphe à un sous-groupe quotient particulier de $\mathrm{GL}_2(\mathbb{C})$. Un petit lemme pour commencer.

Lemme 1. *Pour A et A' dans $\mathrm{GL}_2(\mathbb{C})$, on a $h_A \circ h_{A'} = h_{AA'}$.*

Démonstration. Fixons $a, b, c, d, a', b', c', d' \in \mathbb{C}$ tels que $ad - bc \neq 0$ et $a'd' - b'c' \neq 0$. On a :

$$AA' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}, \quad \text{où} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{et} \quad A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}.$$

De plus, on a bien $AA' \in \mathrm{GL}_2(\mathbb{C})$ car $\det(AA') = \det(A)\det(A') \neq 0$. Soit alors $z \in \mathbb{P}^1$, on a :

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

□

Proposition 1. *L'ensemble H est un sous-groupe des bijections de $\mathbb{P}^1$.*

Démonstration. L'identité de $\mathbb{P}^1$ est l'homographie associée à la matrice identité. La composition des applications est associative. Le lemme 1.1 montre que H est stable pour la composition, et que tout homographie admet un inverse dans H, en effet, pour $A \in \mathrm{GL}_2(\mathbb{C})$ il existe par définition $A^{-1} \in \mathrm{GL}_2(\mathbb{C})$ telle que $AA^{-1} = A^{-1}A = I$. Ainsi H est un sous-groupe des bijections de $\mathbb{P}^1$. □

Proposition 2. *Soient $A, A' \in \mathrm{GL}_2(\mathbb{C})$. Alors, $h_A = h_{A'}$ si et seulement s'il existe $\lambda \in \mathbb{C}^*$ tel que $A' = \lambda A$.*

Démonstration. Le sens réciproque est le plus facile : fixons A, A' dans $\mathrm{GL}_2(\mathbb{C})$ et $\lambda \in \mathbb{C}^*$ tel que $A' = \lambda A$. Soit $z \in \mathbb{P}^1$. On a :

$$h_{A'}(z) = \frac{\lambda a z + \lambda b}{\lambda c z + \lambda d} = \frac{az+b}{cz+d} = h_A(z), \quad \text{où} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Pour le sens direct, on va utiliser le lemme 1.1. Soient $A, A' \in \mathrm{GL}_2(\mathbb{C})$. Supposons que $h_A = h_{A'}$. En composant à droite par $h_{A^{-1}}$ il vient $h_{A'A^{-1}} = \mathrm{Id}$. Fixons alors $\lambda, b, c, d \in \mathbb{C}$ tels que :

$$A'A^{-1} = \begin{pmatrix} \lambda & b \\ c & d \end{pmatrix}.$$

On a alors :

$$\forall z \in \mathbb{C}, \quad z \neq -d/c, \quad \frac{\lambda z + b}{cz+d} = z \quad \Longleftrightarrow \quad cz^2 + (d-\lambda)z - b = 0$$

Ainsi le polynôme $cz^2 + (d-\lambda)z - b$ s'annule en une infinité de valeurs de z, c'est donc le polynôme nul. Il vient $c = d - \lambda = b = 0$, donc $A'A^{-1} = \lambda I$, et $\lambda \neq 0$ sinon $\det(A'A^{-1}) = 0$.
Finalement, $A' = \lambda A$. Ceci achève la démonstration. □

La proposition 2 nous permet d'identifier H au groupe $\mathrm{PGL}_2(\mathbb{C})$ qui n'est autre que le quotient de $\mathrm{GL}_2(\mathbb{C})$ par le sous-groupe $\mathbb{C}^*\mathrm{Id}$: on identifie une matrice et ses multiples non nuls.

1.2 Le birapport

On donne la définition du birapport pour commencer.

Définition . *Soient quatre complexes distincts z_1, z_2, z_3 et z_4, on définit leur birapport par :*

$$[z_1, z_2, z_3, z_4] = \frac{z_1 - z_3}{z_1 - z_4} \times \frac{z_2 - z_4}{z_2 - z_3}$$

Remarque : la définition s'étend à quatre éléments distincts de $\mathbb{P}^1$ car si un des z_i est ∞, l'expression est une homographie en ce z_i.

On va montrer que loin d'être un outil uniquement calculatoire, le birapport est un invariant : étant donné quatre éléments de $\mathbb{P}^1$, une homographie conserve leur birapport. Et même, réciproquement, on verra que si deux quadruplets de points ont le même birapport, alors ils sont images l'un de l'autre par une homographie. Le lemme suivant est la clé de voûte de notre démonstration.

Lemme 2. *Soient $z_1, z_2, z_3, z_4 \in \mathbb{P}$ distincts, il existe une unique homographie h telle que*

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

On a alors : $h(z_4) = [z_1, z_2, z_3, z_4]$.

Démonstration. Soit $a, b, c, d \in \mathbb{C}$. On va résoudre le système

$$(E) : \begin{cases} \frac{az_1+b}{cz_1+d} = \infty \\ \frac{az_2+b}{cz_2+d} = 0 \\ \frac{az_3+b}{cz_3+d} = 1. \end{cases}$$

Supposons dans un premier temps que $z_1, z_2, z_3 \in \mathbb{C}$. On a :

$$(E) \iff \begin{cases} cz_1 + d = 0 \\ az_2 + b = 0 \\ az_3 + b = cz_3 + d. \end{cases}$$

Il vient alors $a(z_3 - z_2) = c(z_3 - z_1)$ et donc :

$$\begin{cases} a = c\frac{z_3-z_1}{z_3-z_2} \\ d = -cz_1 \\ b = -cz_2\frac{z_3-z_1}{z_3-z_2}. \end{cases}$$

Aucun dénominateur ne s'annule car, par hypothèse, les quatre complexes sont distincts. Rappelons qu'une homographie est déterminée par la donnée d'un élément de $\mathrm{PGL}_2(\mathbb{C})$. Ainsi en appelant h l'homographie associé à la matrice :

$$\begin{pmatrix} \frac{z_3-z_1}{z_3-z_2} & -z_2\frac{z_3-z_1}{z_3-z_2} \\ 1 & -z_1 \end{pmatrix},$$

on a $h(z_1) = \infty, \quad h(z_2) = 0, \quad h(z_3) = 1$ et h est unique (on a pris $c = 1$ et on a le droit avec la remarque ci-dessus : n'importe quel choix de c non nul donne lieu à la même homographie).
On calcule alors $h(z_4)$:

$$h(z_4) = \frac{\frac{z_3-z_1}{z_3-z_2}z_4 - z_2\frac{z_3-z_1}{z_3-z_2}}{z_4 \times 1 - z_1} = \frac{(z_4 - z_2)(z_3 - z_1)}{(z_4 - z_1)(z_3 - z_2)} = [z_1, z_2, z_3, z_4]$$

Il nous faut maintenant considérer trois autres cas (on détaillera moins les étapes qui sont exactement les même que ci-dessus).
Si $z_1 = \infty$, on a :

$$(E) \iff \begin{cases} c = 0 \\ b = -az_2 \\ d = a(z_3 - z_2). \end{cases}$$

Cette fois le paramètre est a est on a bien une unique homographie associée.
Si $z_2 = \infty$, on a :

$$(E) \iff \begin{cases} d = -cz_1 \\ a = 0 \\ b = c(z_3 - z_1). \end{cases}$$

Ici le paramètre est c, on a bien toujours une unique homographie associée.

Si $z_3 = \infty$, on a :

$$(E) \iff \begin{cases} d = -cz_1 \\ b = -cz_2 \\ a = c. \end{cases}$$

Le paramètre est encore c et on a bien une unique homographie associée. □

On montre alors, comme annoncé, que le birapport est un invariant, autrement dit :

Théorème 1. *Soient $z_1, z_2, z_3, z_4, z_1', z_2', z_3', z_4' \in \mathbb{C}$ tels que x, y, z (resp. x', y', z') soient deux à deux distincts. Les énoncés suivants sont équivalents.*

(i) il existe une homographie h telle que : $h(z_i) = z_i'$ pour tout i ;

(ii) $[z_1, z_2, z_3, z_4] = [z_1', z_2', z_3', z_4']$.

Démonstration. On procède par double implication.
$(i) \Rightarrow (ii)$ On considère l'homographie g telle que $g(z_1) = \infty$, $g(z_2) = 0$ et $g(z_3) = 1$, et l'homographie g' telle que $g'(z_1') = \infty$, $g'(z_2') = 0$ et $g'(z_3') = 1$ données par le lemme 1.2. On alors alors $g' \circ h(z_1) = \infty$, $g' \circ h(z_2) = 0$ et $g' \circ h(z_3) = 1$. Le lemme montre ainsi que les homographies g et $g' \circ h$ sont égales, et l'on a :

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

$(ii) \Rightarrow (i)$ Supposons que $[z_1, z_2, z_3, z_4] = [z_1', z_2', z_3', z_4']$. On considère les mêmes applications g et g'. Par le lemme, $g(z_4) = [z_1, z_2, z_3, z_4]$ et $g'(z_4) = [z_1', z_2', z_3', z_4']$. Mais alors $h = g'^{-1} \circ g$ est une homographie et :

$$\begin{cases} h(z_1) = g'^{-1} \circ g(z_1) = g'^{-1}(\infty) = z_1' \\ h(z_2) = g'^{-1} \circ g(z_2) = g'^{-1}(0) = z_2' \\ h(z_3) = g'^{-1} \circ g(z_3) = g'^{-1}(1) = z_3' \\ h(z_1) = g'^{-1} \circ g(z_4) = g'^{-1}([z_1, z_2, z_3, z_4]) = g'^{-1}([z_1', z_2', z_3', z_4']) = z_4' \quad (*). \end{cases}$$

$(*)$: on a utilisé l'hypothèse. □

Le birapport donne un critère de cocyclicité pratique. Rappelons que quatre points distincts A, B, C, D sont cocycliques ou alignés si, et seulement si :

$$(\widehat{\overrightarrow{AC}, \overrightarrow{AD}}) \equiv (\widehat{\overrightarrow{BC}, \overrightarrow{BD}}) \quad [\pi].$$

Ce qui est équivalent, en notant les affixes correspondantes respectives z_A, z_B, z_C, z_D, à :

$$\exists k \in \mathbb{Z}, \quad \arg(\frac{z_D - z_A}{z_C - z_A}) = \arg(\frac{z_D - z_B}{z_C - z_B}) + k\pi. \qquad (1)$$

On obtient alors aisément la caractérisation suivante.

Proposition 3. *Quatre points distincts sont cocycliques ou alignés si, et seulement si leur birapport est réel.*

Démonstration. En effet, en reprenant l'équivalence ci-dessus :
(1) $\iff$ $\exists k \in \mathbb{Z}, \quad \arg(\frac{z_D - z_A}{z_C - z_A} \times \frac{z_C - z_B}{z_D - z_B}) = k\pi$
$\iff [z_A, z_B, z_C, z_D] \in \mathbb{R}$. □

Proposition 4. *Une homographie transforme un cercle ou une droite en un cercle ou une droite.*

Démonstration. Soit $\mathcal{C}$ un cercle-droite (par cercle-droite, on entend « un cercle ou une droite ») et $A, B, C \in \mathcal{C}$ distincts. Soit h une homographie. Pour un point M distinct de A, B et C, on a $M \in \mathcal{C}$ si et seulement si $[A, B, C, M] \in \mathbb{R}$, si et seulement si $[h(A), h(B), h(C), h(M)] \in \mathbb{R}$, si et seulement si $h(M) \in \mathcal{C}$ où $\mathcal{C}$ est le cercle circonscrit à $h(A), h(B), h(C)$ – ou la droite $(h(A)h(B))$ si ces points sont alignés. Donc $h(\mathcal{C}) \subset \mathcal{C}'$. Réciproquement pour $N \in \mathcal{C}'$ par surjectivité de h, il existe $M \in \mathbb{P}^1$ tel que $h(M) = N$ et par le même raisonnement, $M \in \mathcal{C}$: on a l'inclusion réciproque. □

En résumé, une homographie est entièrement déterminée par la donnée de l'image de trois points distincts, on dit qu'elle sont 3-transitives (le lecteur s'en convaincra en utilisant le lemme et les homographies g et g' de la démonstration ci-dessus). Le birapport de quatre points distincts est invariant par une homographie. Notons que nous avons défini le birapport algébriquement, puis nous en avons déduit qu'il était un invariant ; mais la démarche inverse est également possible : on renvoie à [5] pour plus d'informations sur le sujet.

2 Etude d'un groupe libre : $\Gamma(2)$

2.1 Groupe engendré par une partie

On rappelle ici deux résultats classiques – on pourra par exemple voir [4] – sur les groupes engendrés par une partie, s'appuyant sur le lemme suivant.

Lemme 3. *Toute intersection d'une famille non vide de sous-groupes est un sous-groupe.*

Démonstration. Soit G un groupe. Donnons nous une famille $(H_i)_{i\in I}$ non vide de sous-groupes de G – i.e. I est un ensemble non vide et pour $i \in I$, H_i est un sous-groupe de G. Soit alors $H = \bigcap_{i\in I} H_i$. L'ensemble H est non vide car pour tout $i \in I$, $e_G \in H_i$. Soient $h, h' \in H$, pour tout $i \in I$, on a $h, h' \in H_i$ et donc $h'h^{-1} \in H_i$, ce qui donne $h'h^{-1} \in H$. □

Définition . *Soit X une partie d'un groupe G. On appelle sous-groupe engendré par X l'intersection de tous les sous-groupes de G contenant X. On note $\langle X \rangle$.*

On a la caractérisation suivante :

Proposition 5. *En reprenant les notations ci-dessus, le sous-groupe engendré par X est le plus petit sous-groupe de G contenant X.*

Démonstration. Notons $\mathcal{H}$ l'ensemble des sous-groupes de G contenant X. Comme $G \in \mathcal{H}$, cet ensemble est non vide. On a $\langle X \rangle = \bigcap_{H\in\mathcal{H}} H$. Soit alors $K \in \mathcal{H}$. Pour tout $x \in \langle X \rangle$ on a $x \in K$ par définition de $\langle X \rangle$, en particulier $x \in K$. Ainsi $K \subset \langle X \rangle$, ce qui prouve que $\langle X \rangle$ est bien le plus petit sous-groupe de G contenant X. □

Cette proposition nous donne une caractérisation du groupe engendré, mais pas une description, d'où l'intérêt de la proposition suivante.

Proposition 6. *Soit X une partie non vide d'un groupe G. On a :*

$$\langle X \rangle = \left\{ \prod_{i=1}^{n} x_i^{\varepsilon_i}, \quad n \in \mathbb{N}, \quad x_i \in X, \quad \varepsilon_i \in \{0, 1, -1\} \right\}.$$

Démonstration. On suppose $X \neq \emptyset$ sinon la propriété est immédiate. Soit $n \in \mathbb{N}$, on se donne $(x_1, ..., x_n) \in X^n$ et $(\varepsilon_1, ..., \varepsilon_n) \in \{0, 1, -1\}^n$. Comme $\langle X \rangle$ est un sous-groupe :

$$\prod_{i=1}^{n} x_i^{\varepsilon_i} \in \langle X \rangle.$$

Il suffit alors de remarquer que l'ensemble des éléments $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$ où $n \in \mathbb{N}$, $x_i \in I$ et $\varepsilon_i \in \{0, 1, -1\}$ est un sous-groupe de G. □

Définition . *Soit G un groupe. On dit que G est de type fini s'il existe X finie tel que $G = \langle X \rangle$.*

2.2 Le groupe $\Gamma(2)$

Ceci étant posé, rentrons dans le vif du sujet. On notera

$$U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

et $u = h_U$, $v = h_V$ les homographies associées. On définit alors le groupe $\Gamma(2)$ comme le groupe engendré par u et v. Par le lemme 2.1, un élément g de $\Gamma(2)$ s'écrit sous la forme $w_1^{k_1} w_2^{k_2} ... w_n^{k_n}$, où $n \in \mathbb{N}^*$, $(w_1, ..., w_n) \in \{u, v\}^n$ et $(k_1, ..., k_n) \in \mathbb{Z}^{*n}$. Remarquons que pour $i \in \{1, ..., n-1\}$, si $w_i = w_{i+1}$:

- soit $k_i + k_{i+1} = 0$ et alors on peut écrire $g = w_1^{k_1} \cdots w_{i-1}^{k_{i-1}} w_{i+2}^{k_{i+2}} \cdots w_n^{k_n}$
- soit $k_i + k_{i+1} \neq 0$ et alors on peut écrire $g = w_1^{k_1} \cdots w_{i-1}^{k_{i-1}} w_i^{k_i + k_{i+1}} w_{i+2}^{k_{i+2}} \cdots w_n^{k_n}$.

Ainsi, de deux choses l'une : soit tous les w_i consécutifs sont distincts et alors on ne peut rien faire, soit ce n'est pas le cas et on peut se ramener à une écriture de longueur $n-1$ (la longueur étant le nombre de w_i).
En procédant ainsi on peut se ramener à une forme réduite de g. Plus précisément, on peut montrer par récurrence la proposition suivante.

Proposition 7. *Soit $g \in \Gamma(2) - \{Id\}$. Il existe $n \in \mathbb{N}^*$, et deux n-uplet $(w_1, ..., w_n) \in \{u, v\}^n$ et $(k_1, ..., k_n) \in \mathbb{Z}^{*n}$ tels que :*

$$g = w_1^{k_1} w_2^{k_2} ... w_n^{k_n} \quad et \quad \forall i \in \{1, ..., n-1\}, \quad w_i \neq w_{i+1}.$$

On va maintenant montrer que $\Gamma(2)$ est un groupe libre, en d'autre termes que toute expression de cette forme décrit un élément non trivial.

2.3 Liberté de $\Gamma(2)$

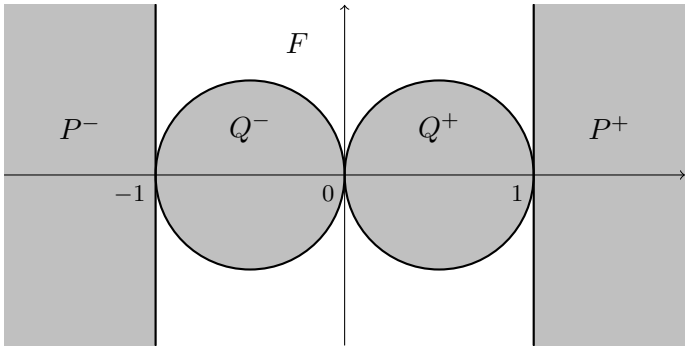
Désormais on notera :

$$\mathcal{P}^- = \{z \in \mathbb{C}, \quad \Re(z) < -1\}, \quad \mathcal{P}^+ = \{z \in \mathbb{C}, \quad \Re(z) > 1\}, \quad \mathcal{P}_0 = \{z \in \mathbb{C}, \quad -1 < \Re(z) < 1\},$$

$$\mathcal{Q}^- = \left\{z \in \mathbb{C}, \quad \left|z + \frac{1}{2}\right| < \frac{1}{2}\right\}, \quad \mathcal{Q}^+ = \left\{z \in \mathbb{C}, \quad \left|z - \frac{1}{2}\right| < \frac{1}{2}\right\}, \quad \mathcal{Q}_0 = \mathbb{C} \setminus \overline{\mathcal{Q}^- \cup \mathcal{Q}^+} \quad .$$

On définit aussi $F = \mathcal{P}_0 \cap \mathcal{Q}_0$.

En étudiant l'action de u et v sur $\mathbb{P}^1$, on sera en mesure de montrer la liberté de $\Gamma(2)$.



Action de u. Pour $z \in \mathbb{C}$, par définition, pour $k \in \mathbb{Z}^*$, $u^k(z) = h_{U^k}(z)$. Par récurrence immédiate on montre que

$$U^k = \begin{pmatrix} 1 & 2k \\ 0 & 1 \end{pmatrix},$$

ainsi $u^k(z) = z + 2k$ et donc u est la translation de vecteur $(2k, 0)$.
Soit $z \in \mathcal{P}_0$, par définition $-1 < \Re(z) < 1$. Donc : $-1 + 2k < \Re(u^k(z)) < 1 + 2k$. Ainsi de deux choses l'une : soit $k \leq -1$ auquel cas $\Re(u^k(z)) < -1$ et alors $u^k(z) \in \mathcal{P}^-$, soit $k \geq 1$ auquel cas $\Re(u^k(z)) > 1$ et alors $u^k(z) \in \mathcal{P}^+$.

Action de v. Remarquons d'abord qu'en posant j l'homographie définie par : $j(z) = 1/z$ pour $z \in \mathbb{P}^1$, on a $v = juj^{-1}$ (on laissera le soin au lecteur de s'en persuader). Il nous faut d'abord étudier de plus près l'homographie j.
Montrons que $j(\mathcal{P}^+) = \mathcal{Q}^+$ et $j(\mathcal{P}^-) = \mathcal{Q}^-$. On va d'abord établir que j envoie la droite $D_1 = \{z \in \mathbb{C}, \quad \Re(z) = 1\}$ sur le cercle C de centre $1/2$ et de rayon $1/2$, privé de 0. On procède par double inclusion.

D'abord, on a : $j(D_1) \subset C$. En effet, soit $z \in D_1$ et $a \in \mathbb{R}$ tel que $z = 1 + ai$. On a :

$$\left| j(z) - \frac{1}{2} \right| = \left| \frac{1 - ai}{1 + a^2} - \frac{1}{2} \right| = \left| \frac{2 - 2ai - 1 - a^2}{2(1 + a^2)} \right| = \left| \frac{(ai - 1)^2}{2(1 + a^2)} \right| = \frac{1}{2}$$

Ainsi $j(z) \in C$ et on a bien l'inclusion annoncée.

Ensuite, on a : $C \subset j(D_1)$. Par bijectivité de j (de réciproque $j^{-1} = j$), cela revient à montrer que $j(C) \subset D_1$. Soit $z \in C$, on se donne $a, b \in \mathbb{R}$ tel que $z = a + ib$. On sait que $\Re(j(z)) = \frac{a}{a^2+b^2}$. Or par définition de C, $|a+ib-\frac{1}{2}| = \frac{1}{2}$, donc $\left(a - \frac{1}{2}\right)^2 + b^2 = \frac{1}{4}$ et il vient $\frac{a}{a^2+b^2} = 1$. Ainsi $j(z) \in D_1$.

On a donc bien $j(D_1) = C$. Ceci étant fait, on montre alors que pour tout $s > 1$, la droite $D_s = \{z \in \mathbb{C}, \quad \Re(z) = s\}$ est envoyée par j sur un cercle contenu dans $\mathcal{Q}^+$ privé de 0. Moyennant l'homothétie $h_s : z \mapsto sz$, c'est facile. En effet il suffit de remarquer que $D_s = h(D_1)$, vient alors : $j(D_s) = jh(D_1) = h^{-1}j(D_1) = h^{-1}(C)$. Ainsi $j(D_s)$ est le cercle C_s de centre $\frac{1}{2s}$ et de rayon $\frac{1}{2s}$, privé de 0. Et ce cercle est bien inclus dans $\mathcal{Q}^+$.
En fait, comme $\mathcal{P}^+ = \bigcup_{s>1} D_s$, on vient de montrer que $j(\mathcal{P}^+) \subset \mathcal{Q}^+$. Réciproquement un point de $\mathcal{Q}^+$ peut être vu comme un élément de C_s (pour un s convenable), que l'on sait envoyer sur la droite D_s : on a donc l'inclusion réciproque.
On montre que $j(\mathcal{P}^-) = \mathcal{Q}^-$ par le même raisonnement.

On peut maintenant étudier l'action de v sur $\mathcal{Q}_0$. Soit $z \in \mathcal{Q}_0$ et $k \in \mathbb{Z}^*$. De $v = juj$, on tire

pour tout $k \in \mathbb{Z}^*$, $v^k = ju^kj$. Il faut distinguer plusieurs cas selon que k est positif ou négatif, et selon que z est dans $\mathcal{P}^+$ ou $\mathcal{P}^-$ ou F.

- Si $k > 0$ et $z \in \mathcal{P}^+$, alors $j(z) \in \mathcal{Q}^+$ puis $u^kj(z) \in \mathcal{P}^+$ et donc $v^k(z) = ju^kj(z) \in \mathcal{Q}^+$.
- Si $k > 0$ et $z \in \mathcal{P}^-$ alors $j(z) \in \mathcal{Q}^-$ puis $u^kj(z) \in \mathcal{P}^+$ et donc $v^k(z) = ju^kj(z) \in \mathcal{Q}^+$.
- Si $k < 0$ et $z \in \mathcal{P}^+$, alors $j(z) \in \mathcal{Q}^+$ puis $u^kj(z) \in \mathcal{P}^-$ et donc $v^k(z) = ju^kj(z) \in \mathcal{Q}^-$.
- Si $k < 0$ et $z \in \mathcal{P}^-$, alors $j(z) \in \mathcal{Q}^-$ puis $u^kj(z) \in \mathcal{P}^-$ et donc $v^k(z) = ju^kj(z) \in \mathcal{Q}^-$.
- Si $k > 0$ et $z \in F$, j étant bijective, $j(z) \in F$ puis $u^k(z) \in \mathcal{P}^+$ et donc $v^k(z) = ju^kj(z) \in \mathcal{Q}^+$.
- Si $k < 0$ et $z \in F$, j étant bijective, $j(z) \in F$ puis $u^k(z) \in \mathcal{P}^-$ et donc $v^k(z) = ju^kj(z) \in \mathcal{Q}^-$.

On peut résumer nos résultats sur les actions de u et v dans la formule suivante.

$$\forall k \in \mathbb{N}^*, \forall \varepsilon, \eta \in \{+,-\}, \quad u^{\varepsilon k}(\mathcal{Q}^\eta) \subset \mathcal{P}^\varepsilon, \quad v^{\varepsilon k}(\mathcal{P}^\eta) \subset \mathcal{Q}^\varepsilon, \quad u^{\varepsilon k}(F) \subset \mathcal{P}^\varepsilon, \quad v^{\varepsilon k}(F) \subset \mathcal{Q}^\varepsilon.$$

On est maintenant en mesure de prouver la liberté de $\Gamma(2)$.

Théorème 2. *Soit $g \in \Gamma(2)$ dont une écriture sous forme réduite est : $g = w_1^{k_1} w_2^{k_2} ... w_n^{k_n}$. Alors g n'est pas l'identité.*

Démonstration. Soit $z \in F$. Montrons par récurrence que : $\forall n \in \mathbb{N}^*, g(z) \in \mathcal{P}^+ \cup \mathcal{P}^- \cup \mathcal{Q}^+ \cup \mathcal{Q}^-$. Pour $n = 1$, la formule (1) montre que $g(z) \in \mathcal{P}^+ \cup \mathcal{P}^- \cup \mathcal{Q}^+ \cup \mathcal{Q}^-$. Donc $g(z) \notin F$, ainsi g n'est pas l'identité. Soit $n \in \mathbb{N}^*$, on suppose la propriété vraie au rang n. Soit $(w_1, ..., w_{n+1}) \in \{u, v\}^{n+1}$ et $(k_1, ..., k_{n+1}) \in \mathbb{Z}^{*n+1}$ tels que l'écriture sous forme réduite de g est $w_1^{k_1} \cdots w_{n+1}^{k_{n+1}}$. Par hypothèse, l'homographie $w_2^{k_2} \cdots w_{n+1}^{k_{n+1}}$ envoie $z \in F$ sur $z' \in \mathcal{P}^+ \cup \mathcal{P}^- \cup \mathcal{Q}^+ \cup \mathcal{Q}^-$, or la formule (1) assure que $w_1^{k_1}(z') \in \mathcal{P}^+ \cup \mathcal{P}^- \cup \mathcal{Q}^+ \cup \mathcal{Q}^-$. Donc $g(z) \neq z$ et on conclut par récurrence. □

Corollaire 1. *Tout élément de $\Gamma(2)$ différent de l'identité possède une écriture unique sous forme réduite.*

Démonstration. Soient $n, n' \in \mathbb{N}^*$, $(w_1, ..., w_n) \in \{u, v\}^n$, $(w'_1, ..., w'_n) \in \{u, v\}^{n'}$ et $(k_1, ..., k_n) \in \mathbb{Z}^{*n}$, $(k'_1, ..., k'_{n'}) \in \mathbb{Z}^{*n'}$ tels que $w_i \neq w_{i+1}$ et $w'_j \neq w'_{j+1}$ pour tout $1 \leq i \leq n-1, \quad 1 \leq j \leq n'-1$. Supposons que ${w_1}^{k_1} \cdots {w_n}^{k_n} = {w'_1}^{k'_1} \cdots {w'_{n'}}^{k'_{n'}}$. Comme u et v sont inversibles, posons :

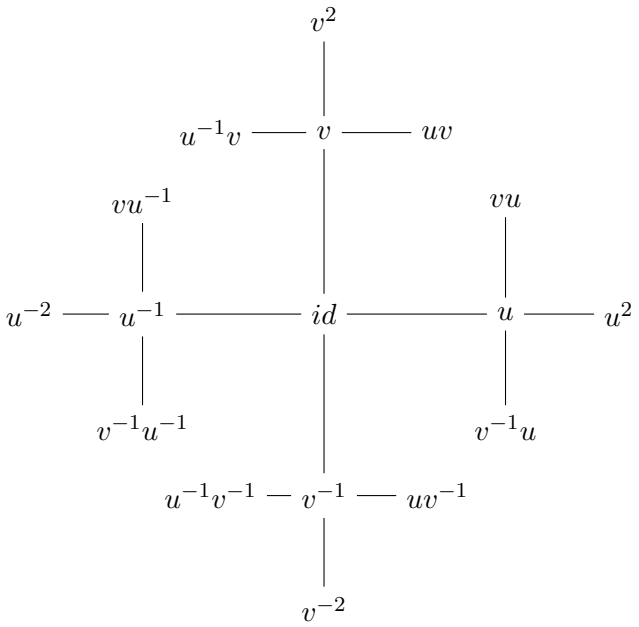
$$g = {w'_{n'}}^{k'_{-n'}} \cdots {w'_1}^{-k'_1} {w_1}^{k_1} \cdots {w_n}^{k_n} = Id.$$

Raisonnons par l'absurde, si $w_1 \neq w'_1$, alors g est sous forme réduite et le théorème 2.3 nous donne la contradiction recherchée. Ainsi $w_1 = w'_1$. De même si $k_1 \neq k'_1$ alors on aurait g sous forme réduite ce qui est exclu. Donc $k_1 = k'_1$ et par suite $g = {w'_{n'}}^{k'_{-n'}} \cdots {w'_2}^{-k'_2} {w_2}^{k_2} \cdots {w_n}^{k_n}$. De proche en proche – pour être rigoureux on effectue une récurrence fini de 1 à $\min\{n, n'\}$ –, on simplifie l'écriture de g – on montre que pour tout $i \in \{1, ..., \min\{n, n'\}\}$, $w_i = w'_i$ et $k_i = k'_i$. On termine en montrant que nécessairement $n = n'$ sinon, encore une fois, g serait sous forme réduite ce qui est exclu. □

En résumé, le groupe de type fini $\Gamma(2)$ est libre. On a pu établir ce résultat grâce à une étude de l'action de u et v, les générateurs du groupe, sur le plan complexe. La caractérisation utilisée pour montrer la liberté de $\Gamma(2)$ est tirée de [2].

2.4 Graphe de Cayley

Etant donné un groupe G de type fini, et un système de générateurs de G : $X = \{x_i\}_{i\in I}$ (par hypothèse, I est un ensemble fini), on va définir le graphe de Cayley associé, que l'on notera $Cay(G, X)$. Supposons que $\mathrm{Card}(I) = n \in \mathbb{N}$. On procède comme suit : le premier sommet est le neutre du groupe, de ce sommets partent $2n$ arêtes, correspondant à la multiplication à gauche [1] par les x_i et ${x_i}^{-1}$. De chaque nouveau sommet ainsi défini, on recommence l'opération, en prenant en compte les simplification nécessaires, à savoir, par exemple : si la multiplication à droite donne un élément du groupe déjà présent dans les sommets définis, l'arête joindra ce sommet. L'exemple le plus simple est le graphe $Cay(\mathbb{Z}/n\mathbb{Z}, 1)$ qui est un cercle, de nombreux autres groupes sont représentés sous forme de graphe dans [3]. On comprend l'intérêt de cette représentation : elle permet de mieux visualiser « l'organisation » du groupe considéré. Dans le cas du groupe $\Gamma(2)$, le graphe $Cay(\Gamma(2), \{u, v\})$ commence par :



On sent bien, via cette représentation que le groupe $\Gamma(2)$ est libre : sur le graphe, cela se traduit par le fait qu'il n'existe pas de boucle. L'intérêt n'est pas que visuel : la représentation sous forme d'arbre donne accès à une méthode efficace pour énumérer les éléments du groupe via un programme informatique, on renvoie le lecteur à [6] pour plus d'informations. Ici, l'arbre est qualifié de ternaire, car de chaque sommet part trois arêtes. Deux groupes isomorphes possède le même graphe de Cayley (sous réserve d'avoir choisi un système de générateurs équivalents).

3 Le groupe $\tilde{\Gamma} = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}))$

Le groupe $\mathrm{SL}_2(\mathbb{Z})$ est défini comme suit :

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}), \quad ad - bc = 1 \right\}.$$

On parle du groupe spécial linéaire. On note π la projection naturelle de $\mathrm{SL}_2(\mathbb{Z})$ dans $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$, autrement dit :

1. C'est un parti pris, on aurait pu choisir de définir le graphe à partir de la multiplication à droite de la même manière, cependant, notre choix s'expliquera à la fin de ce document.

$$\pi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}, \quad \text{où} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Ici, par $\overline{n}$, on entend le reste de n dans sa division euclidienne par 2. On vérifie que π est un morphisme de groupe, si bien que $\tilde{\Gamma}$ est un sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$. De plus, on a clairement $U, V \in \tilde{\Gamma}$. On peut écrire :

$$\tilde{\Gamma} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}), \quad ad - bc = 1, \quad a \equiv d \equiv 1[2], \quad b \equiv c \equiv 0[2] \right\}.$$

Le but de ce paragraphe est de montrer que le groupe $\tilde{\Gamma}$ est un groupe virtuellement libre, autrement dit que l'un de ses groupes quotients l'est. Pour cela, on montre que U et V engendrent le groupe $\tilde{\Gamma}$, au signe près. La démarche effectuée est classique : on va procéder par récurrence. Le lemme suivant sera utile pour prouver l'hérédité.

Lemme 4. *Soient a et c deux entiers non nuls tels que $|a| \neq |c|$. On a alors :*

$$|\ |a| - 2|c|\ | < \max(|a|, |c|) \quad \text{ou} \quad |\ |c| - 2|a|\ | < \max(|a|, |c|).$$

Démonstration. On se place dans le cas où $|a| > |c|$. On a clairement :

$$|a| > |a| - 2|c| > -|c| > -|a|.$$

Ainsi $|\ |a| - 2|c|\ | < |a| \leq \max(|a|, |c|)$. Par symétrie, si $|a| < |c|$ on a $|\ |c| - 2|a|\ | < \max(|a|, |c|)$. D'où le résultat attendu. □

On introduit ici quelques notations pour ne pas alourdir la démonstration du prochain théorème. Soit $A \in \tilde{\Gamma}$, on écrit

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

On note δ l'application de $\tilde{\Gamma}$ dans $\mathbb{N}$ qui à A associe $\delta(A) = \max(|a|, |c|)$. Notons que nécessairement $\delta(A) \geq 1$ car dans le cas contraire, $a = 0$ ce qui est exclu par définition de $\tilde{\Gamma}$. On montre alors le résultat annoncé.

Théorème 3. *Pour tout $A \in \tilde{\Gamma} \setminus \{\mathrm{Id}\}$, il existe $\varepsilon \in \{-1, 1\}$, $n \in \mathbb{N}^*$, $(W_1, ..., W_n) \in \{U, V\}^n$ et $(k_1, ..., k_n) \in \mathbb{Z}^{*n}$ tels que :*

$$A = \varepsilon W_1^{k_1} W_2^{k_2} ... W_n^{k_n} \quad \text{et} \quad \forall i \in \{1, ..., n-1\}, W_i \neq W_{i+1}.$$

Cette écriture est unique.

Démonstration. On prouve le résultat par récurrence sur $\delta(A)$.
Supposons $\delta(A) = 1$. Alors $a = 1$ ou $a = -1$ et $c = 0$. Comme $ad - bc = ad = 1$ et que $d \equiv 1[2]$, on a $d = a$. La seule information disponible sur l'entier b est que son reste dans sa division euclidienne par 2 est 0. Autrement dit, il existe $l \in \mathbb{Z}$ tel que $b = 2l$. Il vient alors :

$$A = \begin{pmatrix} 1 & 2l \\ 0 & 1 \end{pmatrix} = U^l \quad \text{ou} \quad A = -\begin{pmatrix} 1 & -2l \\ 0 & 1 \end{pmatrix} = -U^{-l}.$$

On peut conclure car on vient de montrer :

$$\forall A \in \tilde{\Gamma}, \quad \exists \varepsilon \in \{-1, 1\}, \quad \exists k \in \mathbb{Z}, \quad A = \varepsilon U^k.$$

Soit $n \in \mathbb{N}^*$. On suppose la propriété vérifié jusqu'au rang $n-1$. Soit alors $A \in \tilde{\Gamma}$ telle que $\delta(A) = n$. On remarque que :

$$UA = \begin{pmatrix} a+2c & b+2d \\ c & d \end{pmatrix}, \quad U^{-1}A = \begin{pmatrix} a-2c & b-2d \\ c & d \end{pmatrix},$$

et :

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

Le lemme 3 nous permet alors d'affirmer qu'il existe $W \in \{U, U^{-1}, V, V^{-1}\}$ telle que :

$$\delta(WA) < \max(|a|, |c|) = \delta(A).$$

Ainsi, par hypothèse, il existe $\varepsilon \in \{-1, 1\}$, $n \in \mathbb{N}^*$, $(W_1, ..., W_n) \in \{U, V\}^n$ et $(k_1, ..., k_n) \in \mathbb{Z}^{*n}$ tels que :

$$WA = \varepsilon W_1^{k_1} W_2^{k_2} ... W_n^{k_n} \quad \text{et} \quad \forall i \in \{1, ..., n-1\}, W_i \neq W_{i+1}.$$

Mais alors :

$$A = \varepsilon W^{-1} W_1^{k_1} W_2^{k_2} ... W_n^{k_n} \quad \text{et} \quad \forall i \in \{1, ..., n-1\}, W_i \neq W_{i+1}.$$

On peut conclure car si $W^{-1} \neq W_1$ on a une forme réduite, sinon on concatène W^{-1} et $W_1^{k_1}$.
Supposons alors qu'il existe $A' = \varepsilon' W'^{-1} W'^{l_1}_1 W'^{l_2}_2 \cdots W'^{l_{n'}}_{n'} \in \tilde{\Gamma} \setminus \{\mathrm{Id}\}$ telle que $A' = A$. Les homographies associées dans $\Gamma(2)$ sont alors égales, ce qui donne $n' = n$, $l_i = k_i$, et $W'_i = W_i$ pour tout i par le corollaire 2.3, puis on obtient $\varepsilon' = \varepsilon$. □

On comprend pourquoi on parle ici de groupe virtuellement libre : on a besoin de $-I$ en plus de U et V pour engendré $\tilde{\Gamma}$, et malheureusement $(-I)^2 = I$, autrement dit $\tilde{\Gamma}$ n'est pas libre. Pour obtenir un groupe libre, il ne faut plus différencier une matrice et son opposée : il suffit de considérer le groupe quotient $\tilde{\Gamma}/\{-I, I\}$, en effet, ce dernier est isomorphe à $\Gamma(2)$! L'astuce – c'est notre lemme – utilisée dans la récurrence est classique, on montre d'ailleurs de la même manière que les matrices

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$.

4 Une énumération des triplets pythagoriciens

4.1 Résultats préliminaires

Un premier mot sur les équations diophantiennes.

Lemme 5. *Soient $a, b, d \in \mathbb{Z}$ tels que $a \wedge b = 1$, l'équation $ax + by = d$ d'inconnues entières x et z admet une infinité de solutions. Plus précisément, pour (x_0, y_0) une solution particulière, on peut décrire l'ensemble des solutions est : $\{(x_0 - bk, y_0 + ak), \quad k \in \mathbb{Z}\}$.*

Démonstration. Soient $a, b, d \in \mathbb{Z}$. Commençons par montrer l'existence d'une solution particulière. Comme $a \wedge b = 1$, le théorème de Bézout donne l'existence de $u, v \in \mathbb{Z}$ tels que $au + bv = 1$. Par suite, le couple $(x_0, y_0) = (du, dv)$ est solution de (E).
Soit maintenant $(x, y) \in \mathbb{Z}^2$. Donnons une condition nécessaire pour que ce couple soit solution de l'équation. Si c'est le cas, on a $a(x_0 - x) = b(y - y_0)$ et comme $a \wedge b = 1$, $a \mid (y - y_0)$. Il existe donc $k \in \mathbb{Z}$ tel que $y = y_0 + ak$. Mais alors $a(x_0 - x) = bak$ et par suite, $x = x_0 - bk$.
Réciproquement, les couples de la forme $(x_0 - bk, y_0 + ak)$ où $k \in \mathbb{Z}$ sont solutions de (E). □

Lemme 6. *Soient $m, n \in \mathbb{Z}$ tels que m est impair, n est pair et $m \wedge n = 1$. Alors il existe $p, q \in \mathbb{Z}$ tels que :*

$$\begin{pmatrix} m & p \\ n & q \end{pmatrix} \in \tilde{\Gamma}.$$

Démonstration. Soient de tels entiers m et n. On a $m \wedge n = 1$, ainsi, le théorème de Bézout donne l'existence de deux entiers p_0 et q_0 tels que $mq_0 - np_0 = 1$. Si q_0 est impair et p_0 est pair c'est gagné. Sinon le lemme 5 permet d'affirmer que l'ensemble des solutions de l'équation $mq+n(-p) = 1$ d'inconnues $(q, p) \in \mathbb{Z}^2$ est $\{(q_0 - kn, p_0 - km), \quad k \in \mathbb{Z}\}$. Un raisonnement sur les parités permet alors de trouver un couple satisfaisant dans le cas où p_0 et q_0 sont impairs, et dans le cas où p_0 est impair et q_0 est pair (le cas où ces deux entiers sont pairs est exclus car sinon $2 \mid 1$!).
Détaillons cela pour le premier cas : si p_0 et q_0 sont impairs, il nous suffit de choisir un entier k impair car alors $p = p_0 - km$ est pair comme somme de deux impairs et $q = q_0 - kn$ est impair comme somme d'un entier impair et d'un entier pair. □

Notons que pour une matrice

$$\begin{pmatrix} m & n \\ p & q \end{pmatrix} \in \tilde{\Gamma},$$

on a nécessairement $m \wedge n = 1$. En effet, comme $mq - np = 1$, le théorème de Bézout donne le résultat. Finalement, on obtient une caractérisation pratique :

Proposition 8. *Soient $m, n \in \mathbb{Z}$ tels que m est impair et n est pair. Soient $p, q, p', q' \in \mathbb{Z}$. Si les matrices*

$$A = \begin{pmatrix} m & p \\ n & q \end{pmatrix} \quad \text{et} \quad A' = \begin{pmatrix} m & p' \\ n & q' \end{pmatrix}$$

appartiennent à $\tilde{\Gamma}$ alors il existe $k \in \mathbb{Z}$ tel que $A' = AU^k$.

Démonstration. Soient de telles matrices A et A'. On a par hypothèse $m(q - q') = n(p - p')$. Le lemme se Gauss donne alors – car $m \wedge n = 1$ – l'existence d'un entier l tel que $q' = q + ln$ et $p' = p + lm$. Il faut alors remarquer que comme p' et p sont pairs et m est impair par hypothèse, on a nécessairement l pair. En notant k l'entier tel que $l = 2k$, on a le résultat voulu. □

4.2 Les triplets pythagoriciens

Définition . *Soit $(x, y, z) \in \mathbb{Z}^3$. On dit que (x, y, z) est un triplet pythagoricien si $x^2 + y^2 = z^2$.*

4.2.1 Les triplets primitifs

Définition . *Soit (x, y, z) un triplet pythagoricien. On dit que ce triplet est primitifs si x, y et z sont premiers entre eux dans leur ensemble.*

Proposition 9. *Tout triplet pythagoricien différent de $(0, 0, 0)$ est de la forme (dx, dy, dz) où $d \in \mathbb{Z}$ et (x, y, z) est un triplet pythagoricien primitif.*

Démonstration. C'est presque immédiat. Soit (x, y, z) un triplet pythagoricien. De deux choses l'une, soit x, y et z sont premiers entre eux dans leur ensemble et il n'y a rien à faire, soit ce n'est pas le cas auquel cas on pose $d = pgcd(x, y, z)$. Alors il existe x', y' et z' premiers entre eux tels que $x = dx'$, $y = dx'$ et $z = dz'$ et (x', y', z') est encore un triplet primitif. □

Si (x, y, z) est un triplet pythagoricien primitif, alors x, y et z sont premiers entre eux deux à deux. En effet si p premier divisait par exemple x et y, il diviserait alors z^2 donc il diviserait z. Cela explique la proposition suivante.

Proposition 10. *Soit (x, y, z) un triplet primitifs, alors x et y sont de parité différente. En particulier, z est impair.*

Démonstration. Le cas x et y pair est exclu, car cela contredirait la primalité entre les deux entiers. Pour montrer que x et y ne peuvent pas être tous les deux impairs, il y a un peu plus de travail. Si tel était le cas, z^2 serait pair comme somme de deux impairs et donc z serait pair. Il existerait d'autre part $m, n \in \mathbb{Z}$ tels que $x = 2m + 1$ et $y = 2n + 1$. Mais alors :

$$z^2 = 4(m^2 + m + n^2 + n) + 2 \equiv 2[4]$$

ce qui est impossible. □

Finalement, on donne une caractérisation pratique – et classique – des triplets primitifs.

Théorème 4. *Soient $x, y, z \in \mathbb{Z}$. Le triplet (x, y, z) est un triplet pythagoricien primitif si et seulement si il existe $m, n \in \mathbb{Z}$ de parités différentes et premiers entre eux tels que :*

$$\begin{cases} x = m^2 - n^2 \\ y = 2mn \\ z = m^2 + n^2 \end{cases} \quad ou \quad \begin{cases} x = 2mn \\ y = m^2 - n^2 \\ z = m^2 + n^2. \end{cases}$$

Démonstration. Le sens réciproque est une simple vérification. Montrons le sens direct. On se place dans le cas où x est impair, on a alors y pair. Il existe donc un entier u tel que $y = 2u$. Par suite, en posant $s = z + x$ et $t = z - x$, on obtient : $st = 4u^2$. Comme z et x sont impair, s et t sont pairs, donc il existe $p, q \in \mathbb{Z}$ tels que $s = 2p$ et $t = 2q$. Il vient alors :

$$pq = u^2.$$

On va alors montrer que p et q sont des carrés parfaits. Tout d'abord, comme $x = p - q$ et $z = p + q$, tout diviseur commun à p et q divise x et z, autrement dit, $p \wedge q = 1$. Ainsi, les facteurs premiers de p et de q sont différents, et l'égalité ci-dessus assure alors qu'ils sont tous affectés d'un exposant pair : p et q sont des carrés parfaits. En posant $p = m^2$ et $q = n^2$ on a presque le résultat voulu... En effet, il faut encore vérifier que m et n sont de parités différentes, mais m a la même parité que p et n la même que q, et si p et q avaient la même parité, on aurait $z = p + q$ pair ce qui est exclu. Enfin, comme $p \wedge q = 1$, $m \wedge n = 1$. □

Terminons cette partie préliminaire en introduisant la fonction ϕ, bijection de $\tilde{\Gamma}$ dans $\tilde{\Gamma}$, qui correspond à la conjugaison par la matrice $D = diag(-1, 1)$. Un calcul immédiat donne :

$$\phi(A) = DAD^{-1} = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}, \quad \text{où} \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

4.3 Une énumération habile

On va finalement parvenir à énumérer les triplets pythagoriciens primitifs positifs (on notera l'ensemble correspondant $\mathcal{T}$), l'énumération sous forme d'arbre provient du fait que $\tilde{\Gamma}/\{\pm I_2\}$ est libre. Considérons l'application f de $\tilde{\Gamma}$ dans $\mathcal{T}$ définie par :

$$f(A) = (|m^2 - n^2|, 2|mn|, m^2 + n^2) \quad avec \quad A = \begin{pmatrix} m & p \\ n & q \end{pmatrix}.$$

La caractérisation des triplets primitifs assure que f est surjective. La proposition suivante est centrale dans la construction de l'arbre qui énumérera les triplets primitifs et positifs.

Proposition 11. *Soient A et A' dans $\tilde{\Gamma}$. On a $f(A) = f(A')$ si et seulement si il existe $\varepsilon \in \{-1, 1\}$ tel que :*

$$\exists k \in \mathbb{Z}, \quad A' = \varepsilon A U^k \quad ou \quad \exists k \in \mathbb{Z}, \quad A' = \varepsilon \phi(A) U^k.$$

Démonstration. Soient $A, A' \in \tilde{\Gamma}$ telles que $f(A) = f(A')$. On écrit :

$$A = \begin{pmatrix} m & p \\ n & q \end{pmatrix} \quad et \quad A' = \begin{pmatrix} m' & p' \\ n' & q' \end{pmatrix}.$$

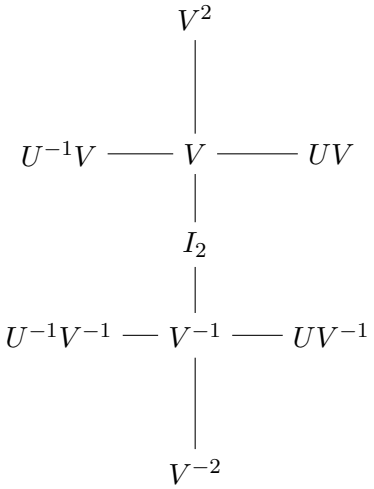
pour $m, n, p, q, m', n', p', q' \in \mathbb{Z}$ convenables. Sans rentrer dans le détail – une résolution de système – on trouve $m' = \pm m$ et $n' = \pm n$. Il nous faut donc traiter quatre cas. Si $m' = m$ et $n' = n$, on applique la proposition 4.1 et on a alors l'existence d'un entier k tel que $A' = AU^k$. Si $m' = -m$ et $n' = -n$, on raisonne sur A' et $-A$ et on a alors $A' = -AU^k$. Si $m' = m$ et $n' = -n$, on raisonne sur A' et $\phi(A)$ qui ont la même première colonne et on a $A' = \phi(A)U^k$. Enfin, si $m' = -m$ et $n' = n$, on raisonne sur A' et $-\phi(A)$ et on a $A' = -\phi(A)U^k$.
Réciproquement, on vérifie facilement que ces relations conviennent. □

Cette proposition montre en particulier que tout élément de $\mathcal{T}$ est l'image d'un unique

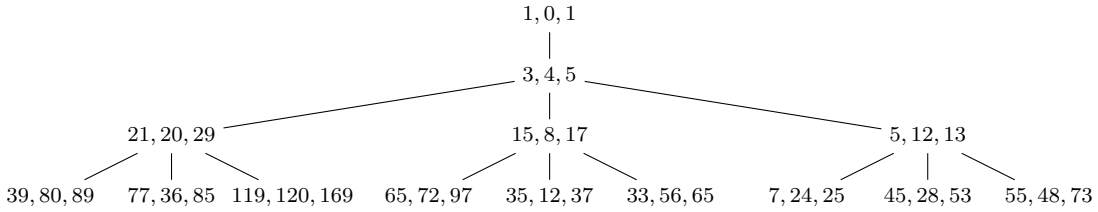
$$\varepsilon U^{k_1} V^{l_1} U^{k_2} V^{l_2} ... U^{k_s} V^{l_s},$$

où $\varepsilon \in \{-1, 1\}$, $s \geq 1$, $l_s \in \mathbb{N}^*$, $k_1 \in \mathbb{Z}$, $k_2, ..., k_s \in \mathbb{Z}^*$, $l_1, ..., l_{s-1} \in \mathbb{Z}$.

Ainsi, on a une énumération sous forme d'arbre des triplets pythagoriciens primitifs et positifs, car on a une bijection entre un quotient d'un groupe libre et $\mathcal{T}$. Plus précisément, on propose une visualisation du théorème ci-dessus, à l'aide du graphe de Cayley. Comme l'image d'une matrice et de son opposée par f sont les mêmes : on ne perd pas en généralité en restreignant l'ensemble de départ à $\tilde{\Gamma}/\{\pm I\} \simeq \Gamma(2)$: on retrouve le graphe donné dans la partie 2.4. Ensuite, comme la multiplication à droite par une puissance de U ne change pas l'image d'une matrice, on peut se restreindre à un seul représentant : au niveau du graphe, plusieurs simplifications ont lieues : les branches correspondant à U et à U^{-1} sont supprimées, ce qui, au passage, justifie la convention choisie dans la réalisation du graphe de Cayley. Le graphe qui en résulte commence alors comme ceci :



Enfin, une matrice et son image par ϕ donne lieu au même triplet pythagoricien, ce qui revient à ne considérer que la partie supérieure, car l'isomorphisme ϕ réalise une bijection entre la partie inférieure, et la partie supérieure du graphe – on considère les même écritures sous forme réduites, au signes des exposants près. On obtient donc une énumération sous forme d'arbre des triplets pythagoriciens. On donne le début de l'énumération, en substituant les matrices par leurs images par f :



On termine donc ce document par le théorème annoncé dans le titre :

Théorème 5. *L'ensemble des triplets pythagoriciens primitifs positifs est muni d'une structure d'arbre. Cet arbre est ternaire et relie les triplets à un quotient du groupe libre* $\Gamma(2)$.

Références

[1] Roger C. Alperin. The modular tree of Pythagoras. *Amer. Math. Monthly* **112**, (9) : 807–816, nov. 2005.

[2] Josette Calais. *Élements de théorie des groupes.* PUF, 1984.

[3] Nathan Carter. *Visual Group Theory.* The Mathematical Association of America, 2009.

[4] Anne Cortella. *Algèbre. Théorie des groupes.* Vuibert, 2011.

[5] Benoît Kloeckner. *Un bref aperçu de la géométrie projective.* Calvage and Mounet, 2010.

[6] David Mumford, Caroline Series, and David Wright. *Indra's Pearls. The Vision of Felix Klein.* Cambridge University Press, 2002.