

Groupes fuchsien

Cyril HOUDAYER et Olivier JAULENT

exposé proposé par Frédéric Paulin

26 juin 2002

Table des matières

1	Prérequis	2
1.1	Géométrie hyperbolique	2
	Le modèle \mathcal{H} et sa métrique	2
	L'action sur \mathcal{H} du groupe $PSL_2(\mathbb{R})$	3
	Classification des éléments de $PSL_2(\mathbb{R})$	3
	Géodésiques de \mathcal{H}	4
	Le modèle \mathcal{U}	5
1.2	Algèbres de quaternions	5
	Algèbres centrales simples	5
	Les K -algèbres vues comme anneaux artiniens non commutatifs	7
	Algèbres de quaternions	8
2	Groupes fuchsien	11
2.1	Définition et première caractérisation	11
2.2	Domaines fondamentaux	12
	Domaine fondamental de Dirichlet	12
	Exemple du groupe modulaire	13
2.3	Groupes fuchsien d'aire finie	14
3	Groupes fuchsien arithmétiques	15
3.1	Groupes fuchsien et algèbres de quaternions	15
3.2	Caractérisation algébrique des groupes fuchsien dérivés d'algèbres de quaternions	16
	Démonstration de la nécessité des conditions 1 et 2 du théorème 56	18
	Démonstration de la suffisance des conditions 1 et 2 du théorème 56	19
3.3	Critère d'arithméticité des groupes fuchsien	21

Introduction

L'objet de cet exposé est l'étude de quelques propriétés des groupes fuchsien, sous-groupes discrets de $PSL_2(\mathbb{R})$. Or, le groupe $PSL_2(\mathbb{R})$ est constitué des isométries conservant l'orientation du demi-plan de Poincaré muni de la métrique hyperbolique. C'est pour cette raison que nous commencerons par présenter quelques aspects de la géométrie hyperbolique. Les algèbres de quaternions, quant à elles, permettent de fabriquer certains groupes fuchsien.

Après ces prérequis, nous étudierons quelques propriétés géométriques des groupes fuchsien en lien avec le demi-plan de Poincaré. Enfin, nous expliquerons pourquoi certains groupes fuchsien dérivent d'algèbres de quaternions et nous énoncerons une caractérisation algébrique de tels groupes fuchsien. Ceci permettra de comprendre une classe importante de groupes fuchsien : les groupes fuchsien arithmétiques.

Nous remercions tout particulièrement Frédéric PAULIN pour le temps qu'il nous a consacré et ses très nombreux conseils et Gaëtan CHENEVIER pour son aide précieuse.

1 Prérequis

1.1 Géométrie hyperbolique

Le modèle \mathcal{H} et sa métrique

On considère le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im } z > 0\}$ et on le munit de la métrique riemannienne (dite hyperbolique) d'élément de longueur $ds = \frac{|dz|}{\text{Im}(z)}$. La longueur hyperbolique d'un chemin γ de classe \mathcal{C}^1 par morceaux paramétré par $\gamma(t) = (x(t), y(t))$ est par définition

$$\ell(\gamma) = \int_0^1 \frac{|\dot{\gamma}(t)|}{y(t)} dt = \int_0^1 \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)} dt. \quad (1)$$

La distance hyperbolique entre deux points z et w de \mathcal{H} est définie par :

$$d(z, w) = \inf_{\gamma \text{ chemin de } z \text{ à } w} \ell(\gamma)$$

et on appelle segment géodésique tout chemin réalisant le minimum de longueur des chemins de classe \mathcal{C}^1 par morceaux entre ses extrémités. Enfin, l'aire hyperbolique d'un domaine D de \mathcal{H} est, compte tenu de la métrique,

$$A(D) = \int_D \frac{dx dy}{y^2}.$$

Proposition 1. *L'application d est une distance sur \mathcal{H} et la topologie qu'elle induit est la topologie euclidienne.*

Démonstration. Il s'agit en fait d'une propriété générale des métriques riemanniennes que l'on ne montrera que dans ce cas particulier. L'application d est clairement symétrique, nulle sur la diagonale et vérifie l'inégalité triangulaire. Le fait que $d(x, y) = 0$ implique $x = y$ découle de ce qui suit.

On notera $B_{euc}(z, r)$ et $B_{hyp}(z, r)$ les boules respectivement euclidienne et riemannienne de centre z et de rayon r . Soit un point z dans \mathcal{H} ; considérons $B_{euc}(z, \epsilon)$ avec $0 < \epsilon < \text{Im } z$. Soit $\delta = \frac{\epsilon}{\epsilon + \text{Im } z}$ et considérons un point w extérieur à $B_{euc}(z, \epsilon)$. Alors, tout chemin β de z à w coupe le cercle $\mathcal{C}_{euc}(z, \epsilon)$ une première fois en un point c . On obtient : $l(\beta) \geq d_{hyp}(z, c) \geq \int_0^1 \frac{|\dot{\gamma}(t)|}{y(t)} dt \geq \int_0^1 \frac{|\dot{\gamma}(t)|}{\epsilon + \text{Im } z} dt \geq \frac{\epsilon}{\epsilon + \text{Im } z} = \delta$ pour tout chemin γ de z à c d'où $d_{hyp}(z, w) \geq \delta$. On a donc finalement $B_{hyp}(z, \delta) \subset B_{euc}(z, \epsilon)$.

Inversement, considérons une boule $B_{hyp}(z, \epsilon)$ avec $\epsilon > 0$ et posons cette fois $\delta = \frac{\epsilon \text{Im } z}{1 + \epsilon}$ d'où $\delta < \text{Im } z$. Alors, pour tout $w \in B_{euc}(z, \delta)$, en considérant le chemin γ rectiligne de z à w , on obtient : $d_{hyp}(z, w) \leq l(\gamma) \leq \int_0^1 \frac{|\dot{\gamma}(t)|}{\text{Im } z - \delta} dt \leq \frac{\delta}{\text{Im } z - \delta} = \epsilon$ d'où $B_{euc}(z, \delta) \subset B_{hyp}(z, \epsilon)$. \square

L'action sur \mathcal{H} du groupe $PSL_2(\mathbb{R})$

Définition et proposition 2. On associe à toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ à coefficients réels vérifiant $ad - bc = 1$ l'application de \mathcal{H} dans lui-même définie par $z \mapsto \frac{az+b}{cz+d}$. On identifie alors l'ensemble de ces applications avec $PSL_2(\mathbb{R}) = SL_2(\mathbb{R})/\{-Id, Id\}$. Cela définit une action sur \mathcal{H} , par homéomorphismes, du groupe $PSL_2(\mathbb{R})$.

Démonstration. Soit une application T de $PSL_2(\mathbb{R})$, T est donc de la forme $T(z) = \frac{az+b}{cz+d}$. On vérifie que l'on a : $\forall z \in \mathcal{H}$, $T(z) \in \mathcal{H}$ qui se déduit de :

$$\operatorname{Im} T(z) = \frac{T(z) - \overline{T(z)}}{2i} = \frac{\operatorname{Im} z}{|cz+d|^2}. \quad (2)$$

Il s'agit d'une action de groupe car l'application associée à la matrice identité est l'application identique sur \mathcal{H} et la composition correspond à la multiplication matricielle. Enfin l'application T est bijective, continue et son inverse $z \mapsto \frac{dz-b}{-cz+a}$ l'est aussi. \square

Proposition 3. Les éléments de $PSL_2(\mathbb{R})$ sont des isométries de \mathcal{H} qui transforment donc géodésiques en géodésiques et conservent l'aire.

Démonstration. Soient $T \in PSL_2(\mathbb{R})$, $z \in \mathcal{H}$ et $w = T(z)$; écrivons $T(z) = \frac{az+b}{cz+d}$ avec $ad - bc = 1$. Remarquons que $T'(z) = \frac{1}{(cz+d)^2}$. Notons ds l'élément de longueur infinitésimale en le point z et dt celui en $w = T(z)$. En utilisant l'équation 2, on obtient : $dt = \frac{|dw|}{\operatorname{Im} w} = |T'(z)| |dz| \frac{|cz+d|^2}{\operatorname{Im} z} = ds$. \square

Remarque. On peut montrer plus précisément que $PSL_2(\mathbb{R})$ est le sous groupe d'indice 2 du groupe des isométries de \mathcal{H} constitué des isométries préservant l'orientation.

Lemme 4. Étant donnés deux points de \mathcal{H} , il existe une application de $PSL_2(\mathbb{R})$ qui envoie ces deux points sur l'axe imaginaire.

Démonstration. Considérons deux points z et w dans \mathcal{H} . Si z et w sont sur la même demi-droite verticale d'équation $x = \lambda$, alors l'isométrie $z \mapsto z - \lambda$ convient. Sinon, il existe un demi-cercle unique \mathcal{C} centré sur l'axe réel et passant par les points z et w . Notons γ l'affixe du centre et r le rayon de \mathcal{C} d'où \mathcal{C} est l'ensemble $\{\gamma + re^{i\theta}, \theta \in [0, \pi]\}$. Soit T définie par $T(z) = -\frac{1}{z-\gamma+r} + \frac{1}{2r}$. On a bien $T \in PSL_2(\mathbb{R})$ et $T(\mathcal{C}) = \{-\frac{1}{r(1+e^{i\theta})} + \frac{1}{2r}, \theta \in [0, \pi]\} = \{i \tan(\frac{\theta}{2}), \theta \in [0, \pi]\} = i\mathbb{R}_+^*$. \square

Remarque. Ce lemme entraîne immédiatement que $PSL_2(\mathbb{R})$ agit transitivement sur les couples de points de \mathcal{H} à distance hyperbolique donnée, *i.e.* étant donnés quatre points x, y, x', y' de \mathcal{H} , si $d(x, y) = d(x', y')$ alors il existe un élément g de $PSL_2(\mathbb{R})$ tel que l'on ait $x' = gx$ et $y' = gy$.

Classification des éléments de $PSL_2(\mathbb{R})$

Définition 5. On prend comme représentant d'un élément de $PSL_2(\mathbb{R})$ toute matrice de déterminant 1 qui lui est associée. Comme $PSL_2(\mathbb{R})$ est le groupe $SL_2(\mathbb{R})/\{-Id, Id\}$, on peut définir la trace d'un élément de $PSL_2(\mathbb{R})$ comme un élément de $\mathbb{R}/\{1, -1\}$ donné par la classe de la trace des représentants. On classe alors les éléments de $PSL_2(\mathbb{R})$ en 4 catégories selon leur trace :

1. l'identité,
2. les éléments dits elliptiques, de trace en valeur absolue strictement inférieure à 2,
3. les éléments dits paraboliques, de trace en valeur absolue égale à 2, à l'exception de l'identité,
4. les éléments dits hyperboliques, de trace en valeur absolue strictement supérieure à 2.

Proposition 6. 1. Un élément elliptique est conjugué à un unique élément dont les représentants sont $\pm \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$ avec $\theta \in]0, \pi[$, et admet deux points fixes conjugués dans $\mathbb{C} \setminus \mathbb{R}$ donc un seul dans \mathcal{H} .

2. Un élément parabolique est conjugués à une unique matrice de la forme $\pm \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$ avec $\lambda \in \mathbb{R}^*$, et admet un unique point fixe dans $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ (et aucun point fixe dans \mathcal{H}).

3. Un élément hyperbolique est conjugué à une unique matrice de la forme $\pm \begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}$ avec $\lambda \in]1, +\infty[$, et admet deux points fixes dans $\overline{\mathbb{R}}$ (et aucun dans \mathcal{H}).

Démonstration. Le polynôme caractéristique de tout élément g de $SL_2(\mathbb{R})$ est $\chi(g) = X^2 - \text{Tr}(g)X + 1$ et on suppose dans la suite que $\text{Tr}(g) \geq 0$. La recherche de points fixes se ramène à la recherche de points fixes pour une matrice conjuguée.

1. Si g est elliptique dans $SL_2(\mathbb{R})$ de matrice M , alors on a $\chi(g) = (X - e^{i\theta})(X - e^{-i\theta})$ avec $\theta \in]0, \pi[$ tel que $2 \cos(\theta) = \text{Tr}(g)$. Montrer que deux matrices sont conjuguées est une question d'algèbre linéaire. Oublions donc momentanément les homographies et plongeons-nous dans $\mathcal{M}_2(\mathbb{C})$. Il existe donc U vecteur propre dans \mathbb{C}^2 pour la valeur propre $e^{i\theta}$ c'est-à-dire $MU = e^{i\theta}U$ d'où, M étant réelle, $M\overline{U} = e^{-i\theta}\overline{U}$. On obtient :

$$\begin{cases} M(\text{Re } U) = M\left(\frac{U+\overline{U}}{2}\right) = \text{Re}(e^{i\theta}U) = \cos(\theta) \text{Re}(U) - \sin(\theta) \text{Im}(U) \\ M(\text{Im } U) = M\left(\frac{U-\overline{U}}{2i}\right) = \text{Im}(e^{i\theta}U) = \cos(\theta) \text{Im}(U) + \sin(\theta) \text{Re}(U) \end{cases}$$

d'où la matrice cherchée dans la base réelle $(\text{Re } U, \text{Im } U)$. Or θ doit vérifier $2 \cos(\theta) = \text{Tr}(g)$ ce qui garantit l'unicité si on impose $\theta \in]0, \pi[$. Enfin, la recherche des points fixes s'écrit $\frac{\cos(\theta)z + \sin(\theta)}{-\sin(\theta)z + \cos(\theta)} = z$ ce qui conduit à $z = \pm i$.

2. Si g est parabolique dans $SL_2(\mathbb{R})$, il vient $\chi(g) = (X - 1)^2$ d'où la valeur propre unique 1 et la forme demandée car on a $g \neq id$. Le vecteur propre est unique à constante multiplicative près et on vérifie que changer le deuxième vecteur de base ne modifie pas λ . Enfin, la matrice obtenue admet l'unique point fixe ∞ .

3. Si g est hyperbolique dans $SL_2(\mathbb{R})$, sa matrice admet deux valeurs propres réelles de produit 1 et de somme positive donc positives, d'où la forme cherchée et son unicité. Un point fixe vérifie $\lambda^2 z = z$ qui équivaut à $z = 0$ ou $z = \infty$.

□

Géodésiques de \mathcal{H}

Proposition 7. Les géodésiques de \mathcal{H} sont les demi-droites verticales et les demi-cercles centrés sur l'axe réel.

Démonstration de la proposition. Considérons d'abord le cas de deux points appartenant à l'axe imaginaire : ia et ib avec $a, b \in \mathbb{R}$. La formule 1 donne une minoration de la longueur d'un chemin γ entre ia et ib :

$$\ell(\gamma) = \int_0^1 \frac{\sqrt{\left(\frac{dx}{dt}\right)^2 + \left(\frac{dy}{dt}\right)^2}}{y(t)} dt \geq \int_0^1 \frac{\left|\frac{dy}{dt}\right|}{y(t)} dt \geq \left| \int_0^1 \frac{dy}{y(t)} \right| = \left| \ln\left(\frac{b}{a}\right) \right|.$$

Or $\left| \ln\left(\frac{b}{a}\right) \right|$ est la longueur du chemin rectiligne entre ia et ib qui constitue donc un segment de géodésique. Un chemin γ qui vérifie en un point $\frac{dx}{dt} \neq 0$ réalise une minoration stricte ci-dessus et ne peut être un segment de géodésique. Enfin, une géodésique ne peut passer deux fois au même point ce qui garantit que $\frac{dy}{dt}$ est de signe constant et on obtient l'unicité de la géodésique précédemment obtenue.

Par le lemme 4, on se ramène pour deux points quelconques au cas ci-dessus puisque les éléments de $PSL_2(\mathbb{R})$ transforment géodésiques en géodésiques (proposition 3) et on obtient finalement les géodésiques cherchées. \square

Le modèle \mathcal{U}

Notons $\mathcal{U} = \{z \in \mathbb{C} \mid |z| < 1\}$. On le munit d'une structure de surface riemannienne en considérant la bijection f de \mathcal{H} sur \mathcal{U} définie par $f(z) = \frac{zi+1}{z+i}$ (on peut vérifier facilement que c'est une bijection dont la réciproque est l'application $w \mapsto \frac{1-yi}{y-i}$) et en prenant comme métrique sur \mathcal{U} la métrique induite par f à partir de la métrique sur \mathcal{H} . En remarquant que $\frac{2|f'(z)|}{1-|f(z)|^2} = \frac{1}{\text{Im } z}$, on obtient la métrique suivante sur \mathcal{U} : $ds = \frac{2|dw|}{1-|w|^2}$ en un point $w \in \mathcal{U}$.

Proposition 8. *Les géodésiques de \mathcal{U} sont les arcs de cercles et les segments orthogonaux au cercle unité \mathbb{S}^1 qui borde \mathcal{U} .*

Démonstration. On sait que les homographies transforment droites et cercles en droites ou cercles. De plus, elles conservent les angles car ce sont des fonctions méromorphes donc dont la différentielle en tout point non pôle est une similitude. Comme les géodésiques de \mathcal{U} sont les images des géodésiques de \mathcal{H} et que l'homographie f envoie \mathbb{R} sur \mathbb{S}^1 , on obtient les géodésiques cherchées. \square

Enfin, déterminons quelle est l'image par f des éléments de $PSL_2(\mathbb{R})$: soit $T : z \mapsto \frac{az+b}{cz+d}$ avec $a, b, c, d \in \mathbb{R}$ et $ad - bc = 1$. Le conjugué U de T par f vérifie, d'après l'expression de f^{-1} et en notant w l'image d'un point z ,

$$\frac{1 - iU(w)}{U(w) - i} = \frac{a \frac{1-iw}{w-i} + b}{c \frac{1-iw}{w-i} + d}.$$

Tous calculs faits, on obtient le représentant principal (celui de déterminant 1 et de trace positive) de U :

$$U(w) = \frac{\alpha z + \bar{\gamma}}{\gamma z + \bar{\alpha}} \quad \text{avec} \quad \begin{cases} \alpha = \frac{1}{2}(a + ib - ic + d) \\ \gamma = \frac{1}{2}(-ia + b + c + id) \end{cases}.$$

On remarque que (α, γ) décrit \mathbb{C}^2 lorsque (a, b, c, d) décrit \mathbb{R}^4 et que la condition $ad - bc = 1$ est équivalente à $|\alpha|^2 - |\gamma|^2 = 1$. Enfin, on constate que la trace est conservée : $\text{Tr}(U) = \text{Tr}(T)$. Ceci est important car cela signifie que la classification qui précède des éléments de $PSL_2(\mathbb{R})$ demeure inchangée dans le modèle \mathcal{U} .

Dans la suite, la notation \mathbb{H}^2 désignera indifféremment l'un des deux modèles \mathcal{H} ou \mathcal{U} .

1.2 Algèbres de quaternions

Dans toute cette section, k désigne un corps et A une algèbre unitaire de dimension finie sur k .

Algèbres centrales simples

Le but de ce paragraphe est de présenter les algèbres centrales simples en vue de comprendre ce que sont les algèbres de quaternions.

Définition 9. *Une k -algèbre A est une algèbre centrale simple si son centre est k et ses seuls idéaux bilatères sont A et l'idéal trivial.*

Le premier exemple d'une telle algèbre est donné par $M_n(k)$, l'espace des matrices carrées d'ordre n sur le corps k . En fait cet exemple est fondamental puisque l'on a le théorème suivant :

Théorème 10. *Si k est algébriquement clos, les seules algèbres centrales simples sur k sont les $M_n(k)$ à isomorphisme près.*

Démonstration. La preuve résulte ici du théorème général suivant. \square

Théorème 11. *Soit K/k une extension de corps. Si A est une algèbre centrale simple sur k , alors $A \otimes_k K$ est une algèbre centrale simple sur K . De plus si A est de dimension finie n sur k alors $A \otimes_k K$ est aussi de dimension n sur K .*

Démonstration. Soit A une algèbre centrale simple sur k . Par les propriétés du produit tensoriel, il est clair que $A \otimes_k K$ est un K -espace vectoriel de dimension n .

Prouvons d'abord que le centre de $A \otimes_k K$ est K . Le centre est un K -espace vectoriel. Soit x un élément du centre, on peut donc l'écrire $\sum_{i=1}^r x_i \otimes \lambda_i$ telle que cette écriture soit de longueur minimale, ce qui entraîne notamment que les x_i et λ_i forment des familles libres. Si toutefois il existait un entier i tel que x_i ne soit pas dans k , alors il existerait un élément u de A tel que $x_i u \neq u x_i$. Ainsi par minimalité de l'écriture, on obtient $x(u \otimes 1) \neq (u \otimes 1)x$, ce qui contredit évidemment le fait que x est dans le centre de $A \otimes_k K$.

Prouvons enfin que $A \otimes_k K$ est simple. Soit I un idéal bilatère de $A \otimes_k K$ différent de 0. Soit donc x un élément non nul de I que l'on écrit $\sum_{i=1}^r x_i \otimes \lambda_i$ de longueur minimale, ce qui entraîne notamment que les x_i et λ_i forment des familles libres, comme précédemment. Comme A est simple, $Ax_1A = A$ et ainsi on peut trouver des éléments u_j et v_j dans A tels que $\sum_j u_j x_1 v_j = 1$.

Comme I est un idéal bilatère, on obtient $\sum_j u_j x v_j \in I$; cet élément est non nul par liberté des λ_i , donc quitte à remplacer x par cet élément, on peut supposer $x_1 = 1$. Toujours par minimalité de l'écriture, on obtient $x(a \otimes 1) = (a \otimes 1)x$ et $ax_i = x_i a$ pour tout i et tout a dans A . Finalement les éléments x_i sont dans le centre de A , à savoir k , et donc x est un élément de $1 \otimes K$; comme K est un corps et I est un idéal, on obtient de suite $I = A \otimes K$. \square

Nous nous proposons à présent de démontrer le résultat suivant qui nous sera utile pour la caractérisation des groupes fuchsien arithmétiques.

Théorème 12. *Une algèbre centrale simple de dimension finie a pour dimension le carré d'un entier.*

Démonstration. Pour cette preuve nous avons besoin du lemme suivant dont une démonstration figure dans le cours d'algèbre de Marc Rosso.

Lemme 13 (Burnside). *Soit G un monoïde de transformations linéaires dans un espace vectoriel V de dimension finie sur un corps algébriquement clos K qui agit irréductiblement sur V au sens où les seuls sous-espaces stables par G sont V et 0. Alors G contient une base pour $End(V)$ sur K .*

On suppose pour l'instant k algébriquement clos. Soit A une algèbre centrale simple non nulle sur k de dimension finie. Prenons I un idéal à gauche minimal pour A . Considérons à présent le morphisme de k -algèbre suivant :

$$\varphi: \begin{array}{l} A \rightarrow End(I) \\ a \mapsto (x \mapsto ax) \end{array} .$$

Il est clairement non nul et $ker(\varphi)$ est un idéal bilatère de A , il est donc nul. Comme I est un idéal à gauche de A , en particulier c est un k -espace vectoriel de dimension finie; $im(\varphi)$ est alors un monoïde de transformations linéaires de I ; de plus comme I est minimal dans A , $im(\varphi)$ agit irréductiblement sur I . En effet soit E un k -sous-espace vectoriel de I stable par tous les éléments de $im(\varphi)$; ainsi pour tout a dans A , aE est inclus dans E et donc E est un idéal de A inclus dans I ; comme I est minimal $E = I$ ou $E = 0$. Donc $im(\varphi)$ contient une base de $End(I)$. Or $im(\varphi)$ est un sous- k -espace vectoriel de $End(I)$, donc $im(\varphi) = End(I)$. D'où φ est un isomorphisme et la dimension de A dans ce cas est bien un carré.

Soit à présent k quelconque. Considérons K une clôture algébrique de k . $A \otimes_k K$ devient une K -algèbre centrale simple de dimension celle de A sur k . On applique alors le raisonnement précédent à cette nouvelle algèbre. \square

On voit que cette démonstration prouve le théorème 10 car pour k algébriquement clos, A se retrouve isomorphe à $End(I)$ et donc isomorphe à $M_n(k)$.

Les K -algèbres vues comme anneaux artiniens non commutatifs

Dans cette partie, A désigne un anneau non commutatif *a priori*. Lorsque l'on parlera d'idéal, il sera toujours sous-entendu qu'il s'agit d'idéal à gauche ; de même pour les A -modules, ils seront des A -modules à gauche.

Définition 14 (Modules simples et semi-simples). *On dit qu'un A -module M est simple s'il ne contient pas de sous A -module strict autre que 0 et qu'il est semi-simple si pour tout sous A -module N , il existe un sous-module P tel que $M = N \oplus P$. Un tel sous-module P est appelé un supplémentaire de N dans M .*

Définition 15 (Anneau semi-simple). *Un anneau A est dit semi-simple si en tant que A -module, il est semi-simple.*

Remarque. Nous ne définirons pas la notion d'anneau simple trop délicate et inutile pour notre étude. Nous pouvons à présent énoncer le lemme suivant que nous ne démontrerons pas et qui constitue un excellent exercice d'algèbre.

Lemme 16. *Soit M un A -module. Les trois conditions suivantes sont équivalentes :*

1. M est semi-simple
2. M est somme de sous-modules simples
3. M est somme directe de sous-modules simples

Définition 17 (Radical). *On définit le radical d'un anneau A comme étant l'intersection de ses idéaux maximaux. On le note $Rad(A)$.*

Proposition 18. *Le radical d'un anneau A est un idéal bilatère.*

Démonstration. Il convient tout d'abord de remarquer que a appartient à $Rad(A)$ si et seulement si $1 - xa$ est inversible dans A , pour tout x dans A . En effet, supposons que a n'appartienne pas à $Rad(A)$. Donc il existe un idéal maximal \wp ne contenant pas a . Par suite, on a $\wp A + aA = A$ d'où 1 s'écrit $1 = mb + ac$ avec $m \in \wp$ et $b, c \in A$, donc $1 - ac$ appartient à \wp et n'est donc pas inversible. Inversement si a appartient au radical de A , on ne peut avoir $1 - xa$ non inversible pour un certain x de A , sinon $1 - xa$ serait contenu dans un idéal maximal contenant a et cet idéal contiendrait 1 ce qui est impossible.

Soit donc $a \in Rad(A)$ et $b \in A$; on a $1 - bxa$ est inversible dans A pour tout x de A ; or un lemme astucieux et classique nous affirme que dans un anneau $1 - ba$ est inversible si et seulement si $1 - ab$ l'est. (En effet, si $1 - ba$ a pour inverse x , alors $(1 - ab)(1 + axb) = 1 - ab + axb - abaxb = 1 - ab + a(x - bax)b = 1$.) Donc $1 - xab$ est inversible pour tout x de A , donc ab appartient à $Rad(A)$. Par conséquent, $Rad(A)$ est un idéal à droite donc bilatère puisqu'on savait déjà que c'était un idéal à gauche. \square

Définition 19 (Anneau artinien). *Un anneau est dit artinien si toute suite décroissante d'idéaux est stationnaire.*

Théorème 20 (Caractérisation de la semi-simplicité). *Soit A un anneau artinien. Alors A est semi simple si et seulement si $Rad(A) = 0$.*

Démonstration. Soit A un anneau artinien. Supposons tout d'abord $Rad(A) = 0$; puisque A est artinien, notons \wp_1, \dots, \wp_n les idéaux maximaux de A dont l'intersection est le radical de A ; considérons alors la surjection canonique

$$A \longrightarrow \bigoplus_{i=1}^n A/\wp_i.$$

Comme $\text{Rad}(A) = 0$ il s'agit d'une injection et donc A s'avère être somme directe de sous- A -modules simples donc A est bien semi-simple.

Réciproquement, supposons A semi-simple; on peut donc écrire

$$A = \bigoplus_{i=1}^n A/\wp_i$$

avec \wp_i idéal maximal de A pour tout i ; il devient alors immédiat que l'intersection des \wp_i est nulle et *a fortiori* le radical est nul. \square

L'idée à présent va être d'appliquer ces différents résultats à des K -algèbres pour K un corps.

Proposition 21. *Toute K -algèbre A est un anneau artinien.*

Nous n'en donnerons pas la preuve, elle constitue un exercice d'algèbre. Nous allons terminer cette partie en énonçant le théorème de Wedderburn, que nous admettrons et qui nous servira pour caractériser la structure des algèbres de quaternions :

Théorème 22 (Wedderburn). *Soient K un corps commutatif, A une K -algèbre de dimension finie sur K . Alors A est semi-simple si et seulement si A est isomorphe à une somme directe finie d'algèbres de matrices sur des corps gauches (de dimension finie sur K).*

Pour voir une démonstration de ce résultat, on pourra consulter [2].

Algèbres de quaternions

Ici K désigne un corps de caractéristique différente de 2 et A une K -algèbre.

Définition 23. *L'algèbre A est une algèbre de quaternions si c'est une algèbre centrale simple de dimension 4.*

Cette définition est en fait équivalente à la suivante, constamment utilisée par la suite :

Proposition-Définition 24. *L'algèbre A est une algèbre de quaternions si :*

1. le radical de A est nul,
2. son centre est K ,
3. sa dimension sur K est 4.

Démonstration. Si A est une algèbre de quaternions alors comme $\text{Rad}(A)$ est un idéal bilatère d'après ce qui précède, on a bien $\text{Rad}(A) = 0$ et ce que l'on veut.

Réciproquement, si A est une K -algèbre vérifiant les trois conditions de l'énoncé, il nous reste à montrer que A est simple. Déjà comme $\text{Rad}(A) = 0$, A est semi-simple et elle est somme directe finie d'algèbres de matrices sur des corps gauches de dimension finie sur K d'après le théorème de

Wedderburn. Or $\dim_K(A) = 4$ et $A = \bigoplus_{i=1}^n M_{n_i}(D_i)$. Soit m le minimum des n_i , on effectue une discussion sur la valeur de m .

Si $m = 2$, alors par un argument de dimension évident, $n = 1$, $D_m = K$ et donc $A = M_2(K)$, A est clairement simple. Si $m = 1$, la dimension de D_m sur K peut-être 1, 2, 3 ou 4; si c'est 4 alors A est un corps gauche forcément simple; si c'est 3 alors D_m est commutatif par le théorème 11 (si D_m était centrale, sa dimension serait un carré ce qui est exclu). En considérant le reste de la somme dans le théorème de Wedderburn, en appliquant la même méthode et en utilisant le fait que $\dim_K(A) = 4$, on obtient que A est somme directe de K et d'un corps commutatif de dimension 3 sur K , A est commutative, ce qui est exclu. Les autres cas, à savoir 1 et 2, bien que laborieux sont tout aussi faciles à traiter; on obtient toujours que A est simple. \square

Définition 25. *Soit A une K -algèbre de base $(1, i, j, k)$ telle qu'il existe a et b dans $K \setminus \{0\}$ avec $i^2 = a$, $j^2 = b$ et $ij = -ji = k$.*

Une telle algèbre est unique à isomorphisme près. Nous noterons cette algèbre, munie de cette présentation, $(\frac{a,b}{K})$.

Proposition 26. Pour a et b dans $K \setminus \{0\}$, $(\frac{a,b}{K})$ est une algèbre de quaternions.

Démonstration. Elle découle immédiatement de la définition. \square

Proposition 27. Pour tout a et b dans $K \setminus \{0\}$, si l'on note A l'algèbre de quaternions $(\frac{a,b}{K})$ on a :

$$A \simeq (\frac{b,a}{K})$$

$$A \simeq (\frac{a,-ab}{K})$$

Démonstration. La preuve résulte du fait que dans la base $(1, i, j, k)$, i, j et k jouent des rôles symétriques. \square

Théorème 28. Toute algèbre de quaternions A sur K est isomorphe à $(\frac{a,b}{K})$ pour un certain a et b dans K .

Démonstration. La preuve est délicate et utilise de nouveau le théorème de Wedderburn. En effet, comme A est simple, elle est en particulier semi-simple car son radical est nul ; on peut donc lui appliquer le théorème de Wedderburn.

Soit A une algèbre de quaternions sur le corps K ; on a par ce qui précède $A \simeq \bigoplus_{i=1}^n M_{n_i}(D_i)$ avec D_i corps gauche de dimension finie sur K . Comme la dimension de A est 4 sur K , en étudiant les différents cas comme dans la démonstration de la proposition-définition 24, on montre que soit $A \simeq M_2(K)$ et alors le théorème est trivial, soit A est un corps gauche. Tout revient à démontrer le théorème dans ce second cas.

Soit donc A un corps gauche, algèbre de quaternions sur K . Prenons $x \in A \setminus K$, $K[x]$ est donc une extension de K de degré supérieur ou égal à deux. Or $\dim_K(A) = \dim_{K[x]}(A)\dim_K(K[x])$ donc nécessairement $\dim_K(K[x]) = 2$ ou 4 ; mais $\dim_K(K[x]) = 4$ est impossible car alors on aurait $A = K[x]$ et A serait commutative. Donc $\dim_K(K[x]) = 2$; le polynôme minimal de X est donc de degré 2, ainsi quitte à retrancher un élément du corps K à x , on peut supposer $x^2 = a$ avec $a \in K$. De même on peut recommencer pour trouver $y \in A$ tel que la famille $(1, x, y)$ soit K -libre et $y^2 = b$ avec $b \in K$.

La famille $(1, x, y, xy)$ est K -libre car sinon on pourrait écrire xy sous la forme $xy = \alpha + \beta x + \gamma y$ avec $\alpha, \beta, \gamma \in K$. Mais alors $xy - \beta x \in K[y]$ et donc comme $y - \beta$ est inversible dans $K[y]$ on aurait $x \in K[y]$ ce qui est absurde car $(1, x, y)$ est K -libre.

Posons à présent $\alpha = xy + yx$ pour alléger les notations. Un calcul trivial montre que α appartient au centre de A et donc à K car A est centrale. L'idée est de rendre maintenant α égal à 0. Au lieu de considérer x , on va plutôt prendre $x - \frac{\alpha}{2b}y$ et on le nomme z . On a toujours que la famille $(1, z, y, zy)$ est K -libre, $z^2 \in K$ et cette fois par choix de z on a bien $zy + yz = 0$. C'est ce qu'il nous fallait démontrer. \square

On peut déjà donner deux exemples fondamentaux. Une algèbre de quaternions hamiltonienne est isomorphe à $(\frac{-1,-1}{\mathbb{R}})$. L'algèbre $M_2(K)$ est isomorphe à $(\frac{1,1}{K})$ avec pour base associée $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$,

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Plus généralement on a la proposition suivante :

Proposition 29. Pour toute K -algèbre de quaternions isomorphe à $(\frac{a,b}{K})$, on a le morphisme de K -algèbre suivant injectif :

$$\begin{aligned} \psi: A &\longrightarrow M_2(K(\sqrt{a})) \\ i &\longmapsto \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix} \\ j &\longmapsto \begin{pmatrix} 0 & 1 \\ b & 0 \end{pmatrix} \\ k &\longmapsto \begin{pmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{pmatrix}. \end{aligned}$$

Ici, le morphisme ψ dépend a priori de la présentation que l'on a choisie pour l'algèbre A .

Démonstration. Comme A est une algèbre centrale simple, ψ est non nul et $\ker(\psi)$ est un idéal bilatère de A , $\ker(\psi)$ est nul et donc ψ est injectif. Enfin les relations $\psi(i)^2 = aI_2$, $\psi(j)^2 = bI_2$, $\psi(i)\psi(j) = -\psi(j)\psi(i) = \psi(k)$ montrent que ψ est bien un morphisme de K -algèbre. \square

Proposition 30. *Si a est un carré dans K alors $(\frac{a,b}{K}) \simeq M_n(K)$. Pour tout λ dans K , $(\frac{a,b}{K}) \simeq (\frac{\lambda^2 a, b}{K})$.*

Démonstration. Si a est un carré dans K alors $K(\sqrt{a}) = K$ et il est immédiat que ψ est surjectif. \square

Corollaire 31. *Si K est algébriquement clos, alors pour tout a et b dans K on a $(\frac{a,b}{K}) \simeq M_n(K)$.*

On retrouve ici un cas particulier d'un résultat plus général énoncé précédemment.

Corollaire 32. *Sur le corps \mathbb{R} , les seules algèbres de quaternions sont $M_2(\mathbb{R})$ et le corps \mathbb{H} de Hamilton.*

Démonstration. Elle résulte immédiatement de la proposition précédente et de la proposition 27. \square

Proposition-Définition 33. *Soit $A = (\frac{a,b}{K})$ avec pour base $(1, i, j, k)$. Chaque x dans A s'écrit alors $x = x_0 + x_1i + x_2j + x_3k$. Notons \bar{x} le conjugué de x avec $\bar{x} = x_0 - x_1i - x_2j - x_3k$.*

Le vecteur \bar{x} est en fait indépendant de la base $(1, i, j, k)$ vérifiant les conditions de la définition 25. On définit la trace et la norme réduites de x par :

$$\text{Tr}(x) = x + \bar{x} = 2x_0$$

$$\text{N}(x) = x\bar{x} = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$$

Démonstration. Fixons une base $(1, i, j, k)$ de l'algèbre $A = (\frac{a,b}{K})$. Prenons $x \in A$ qui s'écrit $x = x_0 + x_1i + x_2j + x_3k$; le conjugué de x par rapport à cette première base est $x_0 - x_1i - x_2j - x_3k$.

Soit une seconde base de A notée $(1, \alpha, \beta, \gamma)$; x s'écrit dans cette nouvelle base $x = y_0 + y_1\alpha + y_2\beta + y_3\gamma$ et le conjugué de x par rapport à cette seconde base est $y_0 - y_1\alpha - y_2\beta - y_3\gamma$.

Il nous reste à vérifier que ces deux conjugués sont égaux. Or les deux bases $(1, i, j, k)$ et $(1, \alpha, \beta, \gamma)$ vérifient les conditions de la définition 25; écrivons

$$\alpha = \alpha_0 + \alpha_1i + \alpha_2j + \alpha_3k$$

$$\beta = \beta_0 + \beta_1i + \beta_2j + \beta_3k$$

$$\gamma = \gamma_0 + \gamma_1i + \gamma_2j + \gamma_3k.$$

Or le calcul de α^2 , β^2 et γ^2 entraîne comme α^2 , β^2 et γ^2 appartiennent à K que α , β et γ n'ont pas de composante selon 1 dans la base $(1, i, j, k)$.

Enfin un calcul explicite trivial montre le résultat recherché. \square

Corollaire 34. *Les applications Tr et N définies sur A ne dépendent pas de la base $(1, i, j, k)$ vérifiant les conditions de la définition 25. De plus, si $\varphi : A \rightarrow B$ est un isomorphisme de K -algèbres avec A et B algèbres de quaternions, on a les égalités :*

$$\text{Tr}_B(\varphi(x)) = \text{Tr}_A(x)$$

$$\text{N}_B(\varphi(x)) = \text{N}_A(x)$$

Démonstration. La première assertion est claire.

Pour la seconde, il suffit de remarquer que l'image par φ d'une base $(1, i, j, k)$ de A est une base de B vérifiant les conditions de la définition 25. \square

Proposition 35. *Avec les mêmes notations que précédemment pour le morphisme ψ , on a $\text{Tr}(x) = \text{trace}(\psi(x))$ et $\text{N}(x) = \det(\psi(x))$. La trace réduite est donc K -linéaire et la norme réduite est multiplicative.*

Démonstration. Le calcul est immédiat. □

Proposition 36. *Soit A une K -algèbre de quaternions. Alors A est un corps gauche si et seulement si $\text{N}(x) \neq 0$ pour tout $x \in A \setminus \{0\}$.*

Démonstration. Évidente. □

2 Groupes fuchsien

2.1 Définition et première caractérisation

Définition 37. *On munit $PSL_2(\mathbb{R})$ de la topologie quotient de celle induite par la topologie naturelle de \mathbb{R}^4 sur $SL_2(\mathbb{R})$, vu comme sous-ensemble de \mathbb{R}^4 . On appelle alors groupe fuchsien tout sous-groupe discret de $PSL_2(\mathbb{R})$.*

Définition 38. *Soit Γ un groupe topologique discret agissant continûment sur un ensemble X localement compact. On dit que Γ agit proprement discontinûment sur X si pour tout compact $K \subset X$, l'ensemble $\{T \in \Gamma \mid T(K) \cap K \neq \emptyset\}$ est fini.*

Pour plus de détails sur cette définition, on pourra se référer à [5]. La proposition qui suit énonce une première caractérisation des groupes fuchsien. La démonstration du sens direct nécessitera un lemme préparatoire.

Proposition 39. *Soit Γ un sous-groupe de $PSL_2(\mathbb{R})$. Alors Γ est un groupe fuchsien si et seulement si Γ agit proprement discontinûment sur \mathbb{H}^2 .*

Lemme 40. *Soient z_0 un point de \mathcal{H} , K un compact de \mathcal{H} . Alors $E = \{T \in PSL_2(\mathbb{R}) \mid T(z_0) \in K\}$ est compact.*

Démonstration du lemme. Notons ψ la projection $\psi : SL_2(\mathbb{R}) \longrightarrow PSL_2(\mathbb{R})$ et considérons l'ensemble $E_1 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \mid \frac{az_0+b}{cz_0+d} \in K \right\}$. Il suffit de montrer que E_1 est compact puisque l'on a $E = \psi(E_1)$ avec ψ continue ce qui se déduit des 2 points suivants :

1. L'ensemble E_1 est fermé. En effet, en notant f l'application $f : \begin{matrix} SL_2(\mathbb{R}) & \longrightarrow & \mathcal{H} \\ S & \longmapsto & \psi(S)(z_0) \end{matrix}$, il n'est autre que l'image réciproque de K par l'application continue f .
2. L'ensemble E_1 est borné. En effet, K étant compact, pour toute matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ appartenant à E_1 , il existe $M_1, M_2 > 0$ tels que $|\frac{az_0+b}{cz_0+d}| \leq M_1$ et $\text{Im}(\frac{az_0+b}{cz_0+d}) \geq M_2$. On en déduit d'après l'égalité 2 que : $\frac{\text{Im } z_0}{|cz_0+d|^2} \geq M_2$ d'où $|cz_0+d| \leq \sqrt{\frac{\text{Im } z_0}{M_2}}$ puis $|az_0+b| \leq M_1 \sqrt{\frac{\text{Im } z_0}{M_2}}$. Ces deux dernières inégalités entraînent que E_1 est borné car z_0 a une partie imaginaire non nulle. □

Démonstration de la proposition 39. Supposons que Γ est un groupe fuchsien. Soit K un compact de \mathcal{H} et z_0 un point de K . Le compact K étant borné, il existe $r > 0$ tel que K soit inclus dans la boule $B_{hyp.}(z_0, r)$. Notons $\overline{B}()$ la boule fermée hyperbolique ; l'ensemble $\{T \in \Gamma \mid T(z_0) \in \overline{B}(z_0, 2r)\} = \{T \in PSL_2(\mathbb{R}) \mid T(z_0) \in \overline{B}(z_0, 2r)\} \cap \Gamma$ est un ensemble fini comme intersection d'un ensemble compact d'après le lemme 40 et d'un ensemble discret. Enfin, l'ensemble $\{T \in \Gamma \mid T(K) \cap K \neq \emptyset\}$ est inclus dans $\{T \in \Gamma \mid T(z_0) \in \overline{B}(z_0, 2r)\}$ puisque si T et z vérifient $T(z) \in K$, alors $d(T(z_0), z_0) \leq d(T(z_0), T(z)) + d(T(z), z_0) = d(z_0, z) + d(T(z), z_0) \leq r + r$. Ainsi, $\{T \in \Gamma \mid T(K) \cap K \neq \emptyset\}$ est fini donc Γ agit proprement discontinûment.

Réciproquement, supposons que Γ agit proprement discontinûment sur \mathcal{H} et par l'absurde que Γ n'est pas discret. Donc il existe une suite $(T_n)_{n \in \mathbb{N}}$ d'éléments de Γ deux à deux distincts convergeant vers l'identité. Soit un point z_0 quelconque de \mathcal{H} ; la suite $(T_n(z_0))_{n \in \mathbb{N}}$ converge vers z_0 . De plus, soit K un voisinage compact de z_0 ; comme l'ensemble $\{T \in \Gamma \mid T(K) \cap K \neq \emptyset\}$ est fini, l'ensemble $\{T \in \Gamma \mid T(z) \in K\}$ l'est aussi. Par suite, il existe deux entiers m et n distincts tels que $T_n = T_m$, ce qui est exclus. \square

Remarque. On a également la caractérisation suivante : un sous-groupe Γ de $PSL_2(\mathbb{R})$ est fuchsien si et seulement si les orbites de \mathcal{H} sous l'action de Γ sont discrètes. Le sens direct est immédiat avec la proposition 39. Pour la réciproque, il suffit de remarquer que si les orbites sont discrètes et si K est compact, alors l'ensemble $\{T \in \Gamma \mid T(z) \in K\}$ est fini ce qui permet d'utiliser la fin de la démonstration qui précède et de conclure.

On peut également en déduire en prenant K un singleton que le stabilisateur de tout point de \mathcal{H} est d'ordre fini.

2.2 Domaines fondamentaux

Définition 41. On appelle domaine fondamental pour un groupe fuchsien Γ tout fermé F de \mathbb{H}^2 vérifiant :

1. $\bigcup_{T \in \Gamma} T(F) = X$
2. $\forall T \in \Gamma \setminus \{id\}, \overset{\circ}{F} \cap T(\overset{\circ}{F}) = \emptyset$.

On note ∂F la frontière de F .

Proposition 42. Soient F_1 et F_2 deux domaines fondamentaux pour un groupe fuchsien Γ . On suppose de plus que $\mathcal{A}(\partial F_1) = \mathcal{A}(\partial F_2) = 0$. Alors $\mathcal{A}(F_2)$ est égal à $\mathcal{A}(F_1)$ (et sont éventuellement infinis).

Démonstration. Remarquons que :

$$F_1 \supset (F_1 \cap \bigcup_{T \in \Gamma} T(\overset{\circ}{F}_2)) = \bigcup_{T \in \Gamma} (F_1 \cap T(\overset{\circ}{F}_2)).$$

Or F_2 est un domaine fondamental donc les ensembles $F_1 \cap T(\overset{\circ}{F}_2)$ sont distincts, ce qui entraîne que $\mathcal{A}(F_1) \geq \sum_{T \in \Gamma} \mathcal{A}(F_1 \cap T(\overset{\circ}{F}_2)) = \sum_{T \in \Gamma} \mathcal{A}(T(F_1) \cap \overset{\circ}{F}_2)$. On déduit de $\bigcup_{T \in \Gamma} T(F_1) = X$ que $\bigcup_{T \in \Gamma} (T(F_1) \cap \overset{\circ}{F}_2) = \overset{\circ}{F}_2$, donc finalement l'inégalité $\mathcal{A}(F_1) \geq \mathcal{A}(\overset{\circ}{F}_2) = \mathcal{A}(F_2)$ et la conclusion car F_1 et F_2 jouent des rôles symétriques. \square

Définition 43. La proposition précédente permet de définir l'aire $\mathcal{A}(\Gamma)$ d'un groupe fuchsien Γ comme étant l'aire d'un de ses domaines fondamentaux ayant un bord d'aire nulle. En effet, un tel domaine existe, nous allons en construire.

Domaine fondamental de Dirichlet

Définition 44. On appelle domaine de Dirichlet centré en un point p de \mathbb{H}^2 pour un groupe fuchsien Γ l'ensemble :

$$\begin{aligned} D_p(\Gamma) &= \{z \in \mathbb{H}^2 \mid \forall T \in \Gamma, d(z, p) \leq d(z, T(p))\} \\ &= \bigcap_{T \in \Gamma} \{z \in \mathbb{H}^2 \mid d(z, p) \leq d(z, T(p))\}. \end{aligned}$$

Nous allons d'abord montrer que les ensembles $\{z \in \mathbb{H}^2 \mid d(z, p) = d(z, T(p))\}$ ne sont autre que des géodésiques. Un domaine de Dirichlet est donc en fait l'intersection de "demi-plans hyperboliques" limités par ces géodésiques. On verra ensuite que l'on a bien construit un domaine fondamental si p n'est pas point fixe.

Lemme 45 (Les médiatrices sont des géodésiques). *Si z_1 et z_2 sont deux points distincts de \mathbb{H}^2 , l'ensemble $\{z \in \mathcal{H} \mid d(z, z_1) = d(z, z_2)\}$ est l'unique géodésique passant par le milieu hyperbolique du segment $[z_1, z_2]$ et orthogonale à la géodésique passant par z_1 et z_2 .*

Démonstration. On se place dans le modèle \mathcal{U} . Quitte à faire agir une isométrie, on peut supposer que le milieu m de $[z_1, z_2]$ est en l'origine et que z_1 et z_2 sont sur l'axe horizontal. Alors la géodésique perpendiculaire en m à la géodésique passant par z_1 et z_2 est l'axe vertical. Il est immédiat que l'application $(x, y) \mapsto (-x, y)$ est une isométrie de \mathcal{U} , fixant m et permutant z_1 et z_2 . On en déduit que l'axe vertical, aussi fixé par cette isométrie, est formé de points équidistants à z_1 et z_2 , et est en fait l'ensemble de ces points. \square

Proposition 46. *Si p n'est fixé par aucun élément de $\Gamma \setminus \{id\}$, alors $D_p(\Gamma)$ est un domaine fondamental convexe pour Γ vérifiant $A(\partial D_p(\Gamma)) = 0$.*

Démonstration. Soit une orbite \mathcal{O} dans \mathbb{H}^2 sous l'action de Γ . Elle est discrète d'où l'existence de $z_0 \in \mathcal{O}$ tel que $d(z_0, p) = \inf_{z \in \mathcal{O}} d(z, p)$ qui vérifie donc : $\forall T \in \Gamma, d(z_0, T(p)) = d(T^{-1}(z_0), p) \geq d(z_0, p)$. Donc, par définition du domaine de Dirichlet, on a $z_0 \in D_p(\Gamma)$; ainsi toute orbite admet un représentant dans $D_p(\Gamma)$.

Soit z_1 un point dans l'intérieur de $D_p(\Gamma)$ et soit $z_2 = T(z_1)$ pour un certain $T \in \Gamma \setminus \{id\}$. Comme z_1 appartient à l'intérieur de $D_p(\Gamma)$, on a $d(z_1, p) < d(z_1, T^{-1}(p))$ d'où $d(z_2, T(p)) < d(z_2, p)$ car T conserve les distances. Par suite, z_2 n'appartient pas à $D_p(\Gamma)$ donc l'intérieur de $D_p(\Gamma)$ contient au plus un point par orbite.

Enfin, l'ensemble $D_p(\Gamma)$ est intersection de demi-plans hyperboliques fermés. C'est donc un convexe fermé de frontière un nombre dénombrable de segments hyperboliques ce qui entraîne $A(\partial D_p(\Gamma)) = 0$. \square

Remarque. L'existence d'un point p de \mathbb{H}^2 non fixé par les éléments de $\Gamma \setminus \{id\}$ résulte de ce qu'un groupe fuchsien est dénombrable et que chaque élément du groupe distinct de l'identité a au plus un point fixe dans \mathbb{H}^2 . On obtient ainsi un ensemble dénombrable de points fixés dans \mathbb{H}^2 , qui est non dénombrable. On a donc montré l'existence pour tout groupe Γ d'un domaine fondamental dont l'aire du bord soit nulle. Ceci assure la consistance de la définition 43.

Exemple du groupe modulaire

Nous allons maintenant donner un exemple de groupe fuchsien et construire un domaine de Dirichlet de ce groupe. Considérons le groupe $\Gamma = PSL_2(\mathbb{Z})$, appelé groupe modulaire, et le domaine $F = \{z \in \mathcal{H} \mid |z| = 1, |\operatorname{Re}(z)| \leq \frac{1}{2}\}$. Nous allons montrer qu'il s'agit du domaine de Dirichlet pour le groupe modulaire centré en n'importe quel point de la forme $p = \lambda i$ avec $\lambda > 1$.

Remarquons tout d'abord que les applications $T : z \mapsto z + 1$ et $V : z \mapsto -\frac{1}{z}$ appartiennent à Γ et que l'ensemble $\{z \in \mathcal{H} \mid \forall U \in \{T, T^{-1}, V\} d(z, p) \leq d(z, U(p))\}$ n'est autre que F . Il en résulte l'inclusion $D_p(\Gamma) \subset F$.

Maintenant, par l'absurde, si on avait $D_p(\Gamma) \neq F$ alors il existerait $z \in \overset{\circ}{F}$ et $U \in \Gamma$ tels que $U(z) \in \overset{\circ}{F}$. Écrivons U sous la forme $U(z) = \frac{az+b}{cz+d}$ avec $a, b, c, d \in \mathbb{Z}$ et $ad - bc = 1$, cette dernière

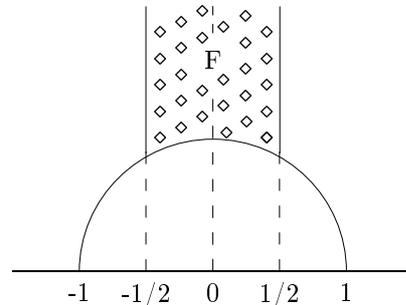


FIG. 1: Un domaine fondamental de $PSL_2(\mathbb{Z})$

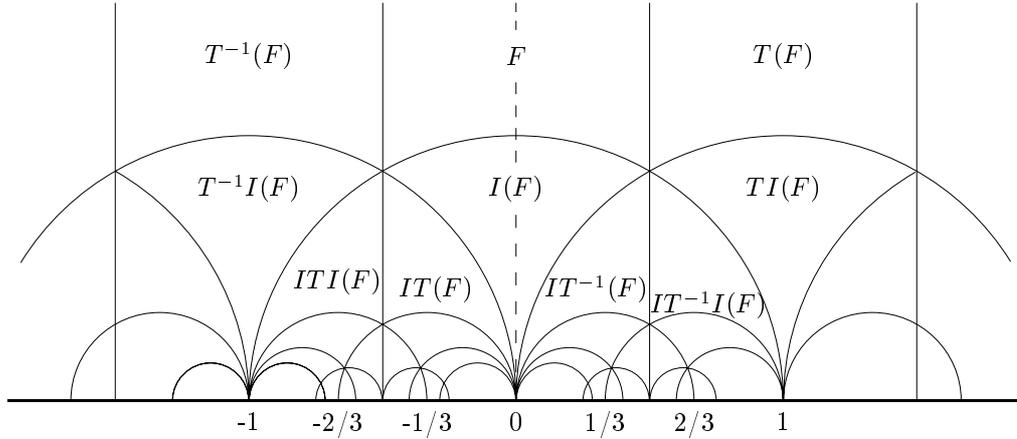


FIG. 2 – Partition pour Γ associée au domaine fondamental F

égalité entraînant immédiatement $c \neq 0$ ou $d \neq 0$. La relation 2 donne $\text{Im } U(z) = \frac{\text{Im } z}{|cz+d|^2}$. Si on montre l'inégalité $|cz+d| > 1$, on obtiendra $\text{Im } U(z) < \text{Im } z$ et en remplaçant U par U^{-1} et z par $U(z)$, on aura également $\text{Im } z < \text{Im } U(z)$, une contradiction. Or les relations $|z| > 1$ et $|\text{Re } z| < 1$ entraînent $|cz+d|^2 = c^2|z|^2 + 2cd \text{Re } z + d^2 > c^2 - |cd| + d^2 = (|c| - |d|)^2 + |cd|$, inégalité stricte car on ne peut avoir $c = d = 0$. Finalement, $(|c| - |d|)^2 + |cd|$ est un entier naturel non nul d'où le résultat attendu.

Nous avons enfin représenté figure 2 une partie de la partition de \mathcal{H} par les images sous l'action du groupe modulaire du domaine fondamental F .

2.3 Groupes fuchsien d'aire finie

Dans la suite, nous allons nous intéresser plus particulièrement aux groupes fuchsien d'aire finie. Donnons-en déjà deux propriétés intéressantes.

Proposition 47. *Tout groupe fuchsien d'aire finie contient un élément hyperbolique.*

Démonstration. Soit un groupe fuchsien Γ ne contenant que des éléments elliptiques outre l'identité. Remarquons que la trace et l'aire d'un domaine de Dirichlet restent inchangées par conjugaison. Par suite, on peut conjuguer le groupe Γ par un élément de $PSL_2(\mathbb{R})$ et donc supposer qu'il existe un élément g de $\Gamma \setminus \{id\}$ fixant le point origine dans le modèle \mathcal{U} . La matrice de g est alors de la forme $\begin{pmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{pmatrix}$. Soit h un autre élément de Γ de matrice $\begin{pmatrix} a & \bar{c} \\ c & \bar{a} \end{pmatrix}$. Tous calculs faits, on obtient : $\text{Tr}(ghg^{-1}h^{-1}) = 2 + |c|^2|1 - \alpha^2|^2$. Comme cette trace doit être inférieure à 2, on en déduit que $c = 0$ ou $\alpha^2 = 1$. Ce dernier cas est impossible car g n'est pas l'identité. Ainsi, on a $c = 0$ et tous les éléments ont 0 pour point fixe. Le groupe s'identifie à un sous-groupe discret du groupe des complexes de module 1, et est donc fini. L'aire de \mathcal{U} étant infinie, on déduit de la relation $\bigcup_{T \in \Gamma} T(F) = \mathcal{U}$, vérifiée par tout domaine fondamental F , que Γ est d'aire infinie.

Si Γ contient un élément g parabolique, plaçons-nous cette fois dans le modèle \mathcal{H} . On peut supposer, quitte à conjuguer, que g fixe l'infini, d'où la forme de $g : g(z) = z + \beta$ avec $\beta \neq 0$. Si tous les éléments fixent l'infini et qu'il n'y a pas d'élément hyperbolique, alors tous les éléments sont paraboliques de la forme $z \mapsto z + \lambda$ et, le groupe étant discret, λ décrit $\alpha\mathbb{Z}$ avec $\alpha \in \mathbb{R}^*$. Les domaines de Dirichlet sont des bandes verticales donc d'aire infinie. Sinon, il existe h ne fixant pas l'infini donc de matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $c \neq 0$. Tous calculs faits, on a : $\text{Tr}(g^n h) = |a + d + n\beta c|$ qui dépasse 2 pour n suffisamment grand ce qui assure l'existence d'un élément hyperbolique. \square

Proposition 48. *Tout groupe fuchsien d'aire finie est de type fini (i.e. admet une partie génératrice finie).*

Nous admettons cette proposition dont une démonstration figure dans [3].

3 Groupes fuchsien arithmétiques

Nous nous proposons dans cette section de démontrer certains critères concernant l'arithmétique des groupes fuchsien. La première partie définit précisément ces notions ; la seconde plus technique démontre l'essentiel des résultats.

3.1 Groupes fuchsien et algèbres de quaternions

Définition 49. *Soit K/\mathbb{Q} une extension algébrique sur \mathbb{Q} de degré n . Comme \mathbb{Q} est parfait, K/\mathbb{Q} est séparable et il y a donc n \mathbb{Q} -plongements de K dans \mathbb{C} .*

On dit que K est totalement réel si ces n plongements sont à valeurs réelles. Dans ce cas, K est appelé corps de nombres totalement réel.

Notons O_K l'anneau des entiers de K , corps de nombres totalement réel.

Proposition-Définition 50. *Soit A une algèbre de quaternions sur K . Nous allons donner trois définitions équivalentes d'un ordre O dans A .*

1. *O est un sous-anneau de A contenant 1 et est un O_K -module de type fini engendrant A sur K .*
2. *Si $[K : \mathbb{Q}] = n$, alors O est un sous-anneau de A contenant 1 et est un \mathbb{Z} -module libre de rang $4n$.*
3. *O est un sous-anneau d'éléments entiers de A (ce qui signifie que pour chaque x dans O , $N(x)$ et $Tr(x) \in O_K$) avec O engendre A sur K .*

Nous admettons l'équivalence de ces trois définitions. Prenons à présent O un ordre dans A . Posons $O^1 = \{x \in O, N(x) = 1\}$. Avec les notations de la première section, $\psi(O^1) \subset SL_2(\mathbb{R})$ car $N(x) = \det(\psi(x))$.

Exemples. L'anneau des entiers de \mathbb{Q} est \mathbb{Z} . Ce résultat est immédiat en considérant un élément entier x que l'on écrit $x = \frac{a}{b}$ avec a, b appartenant à \mathbb{Z} premiers entre eux. Choisissons un polynôme annulateur unitaire P de degré n ; en multipliant l'équation $P(x) = 0$ par b^n , on obtient que b divise a donc x appartient à \mathbb{Z} . Il résulte immédiatement de chacune des trois propositions équivalentes qui précèdent que dans $M_2(\mathbb{Q})$, $M_2(\mathbb{Z})$ est un ordre.

L'extension $\mathbb{Q}(\sqrt{2})$ est un corps de nombres totalement réel. Ainsi $M_2(\mathbb{Z}(\sqrt{2}))$ est un ordre de l'algèbre de quaternions $M_2(\mathbb{Q}(\sqrt{2}))$ en utilisant la deuxième définition puisque $M_2(\mathbb{Z}(\sqrt{2}))$ est un \mathbb{Z} -module de rang 8 (il est facile d'exhiber une base).

On peut retrouver ce résultat à partir des deux autres définitions en déterminant l'anneau des entiers de $\mathbb{Q}(\sqrt{2})$. Un résultat général énoncé et démontré dans [7] affirme que si d est un entier vérifiant $d \equiv 2$ ou $d \equiv 3 \pmod{4}$, alors l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}(\sqrt{d})$. Démontrons ce résultat dans le cas particulier qui nous intéresse à savoir $d = 2$. Soit un élément entier $x = a + b\sqrt{2}$ avec $a, b \in \mathbb{Z}$. L'élément $a - b\sqrt{2}$ est aussi entier donc par stabilité par addition et multiplication, $2a$ et $a^2 - 2b^2$ sont également entiers sur \mathbb{Z} . Comme l'anneau des entiers de \mathbb{Q} est \mathbb{Z} , ils sont dans \mathbb{Z} . De $(2a)^2 - 2(2b)^2 \in \mathbb{Z}$ et $2a \in \mathbb{Z}$, on tire $2(2b)^2 \in \mathbb{Z}$ d'où $2b \in \mathbb{Z}$ grâce à la présence du carré. Par suite, l'entier $2a$ est pair donc $a \in \mathbb{Z}$. Il résulte alors de $a^2 - 2b^2 \in \mathbb{Z}$ que b appartient à \mathbb{Z} . Réciproquement, tout élément x de la forme $x = a + b\sqrt{2}$ avec $a, b \in \mathbb{Z}$ est racine du polynôme $x^2 - 2ax + a^2 - 2b^2$.

Définition 51. *On pose dans ces conditions $\Gamma(A, O) = \psi(O^1)/\{\pm Id\}$. Ainsi on obtient que $\Gamma(A, O)$ est un sous-groupe de $PSL_2(\mathbb{R})$.*

Proposition 52. *Ce sous-groupe $\Gamma(A, O)$ est un groupe fuchsien.*

Démonstration. Dans la preuve qui suit, nous allons supposer que A est une algèbre de quaternions sur \mathbb{Q} du type $\left(\frac{a,b}{\mathbb{Q}}\right)$ avec $a > 1$ et $b > 1$; de plus ici $O = \{x \in A; x_0, x_1, x_2, x_3 \in \mathbb{Z}\}$. On identifiera par la suite $\psi(O^1)$ et O^1 .

Il est évident que pour prouver que $\Gamma(A, O)$ est discret il suffit de trouver un voisinage de Id dans $SL_2(\mathbb{R})$ qui ne contient aucun élément de O^1 hormis Id .

Notons U l'ensemble des matrices $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ avec :

$$|a_{11} - 1| < \frac{1}{2}, |a_{22} - 1| < \frac{1}{2}, |a_{12}| < \frac{1}{2}, |a_{21}| < \frac{1}{2},$$

qui est un voisinage de Id .

Prenons à présent $\psi(x) \in O^1 \cap U$ avec $\psi(x) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$. Or ces coefficients s'écrivent :

$$\begin{aligned} a_{11} &= x_0 + x_1\sqrt{a} \\ a_{12} &= x_2 + x_3\sqrt{a} \\ a_{21} &= b(x_2 - x_3\sqrt{a}) \\ a_{22} &= x_0 - x_1\sqrt{a} \end{aligned}$$

avec x_0, x_1, x_2, x_3 dans \mathbb{Z} . On a donc $|a_{11} + a_{22} - 2| < 1$, d'où $|2x_0 - 2| < 1$. Ainsi $x_0 = 1$.

De même, comme $b > 1$, on a $|x_2 - x_3\sqrt{a}| < \frac{1}{2b} < \frac{1}{2}$, donc $|a_{12} + \frac{a_{21}}{b}| < 1$ et ainsi $|2x_2| < 1$ ce qui entraîne $x_2 = 0$. De même on obtient $|x_1\sqrt{a}| < \frac{1}{2}$ et $|x_3\sqrt{a}| < \frac{1}{2}$ ce qui entraîne $x_1 = x_3 = 0$ puisque l'on a aussi $a > 1$ et finalement $\psi(x) = Id$. Ainsi $\Gamma(A, O)$ est bien un sous-groupe discret de $PSL_2(\mathbb{R})$, c'est-à-dire un groupe fuchsien. \square

Définition 53. *Si Γ est un sous-groupe d'indice fini de $\Gamma(A, O)$, alors Γ est appelé un groupe fuchsien dérivé de l'algèbre de quaternions A .*

Définition 54. *Deux sous-groupes d'un groupe sont dits commensurables si leur intersection est d'indice fini dans chacun d'eux.*

Définition 55. *Le groupe Γ est appelé un groupe fuchsien arithmétique si Γ est commensurable avec un certain $\Gamma(A, O)$.*

3.2 Caractérisation algébrique des groupes fuchiens dérivés d'algèbres de quaternions

Nous nous proposons ici de démontrer le théorème de caractérisation suivant :

Théorème 56. *Soit Γ un groupe fuchsien d'aire finie. Alors Γ est dérivé d'une algèbre de quaternions A sur un corps de nombres totalement réel k qui vérifie les conditions de produit tensoriel (cette notion est proprement définie plus loin au cours de la démonstration) si et seulement si Γ satisfait les deux conditions suivantes :*

1. *Soit F le corps $\mathbb{Q}(\text{Tr}(\Gamma))$ engendré par l'ensemble $\text{Tr}(\Gamma)$ sur \mathbb{Q} . Alors F est un corps de nombres de degré fini et $\text{Tr}(\Gamma)$ est contenu dans l'anneau des entiers O_F de F .*
2. *Soit φ un plongement de F dans \mathbb{C} différent de l'identité. Alors $\varphi(\text{Tr}(\Gamma))$ est borné dans \mathbb{C} .*

Démonstration. La preuve est longue et technique, c'est pour cette raison que nous allons la décomposer en plusieurs étapes. Nous allons énoncer plusieurs lemmes et théorèmes nécessaires à la démonstration.

Lemme 57. Soit Γ un groupe fuchsien d'aire finie tel que l'ensemble $\text{Tr}(\Gamma)$ soit contenu dans un corps de nombres F de degré fini sur \mathbb{Q} . Alors il existe un élément g de $SL_2(\mathbb{R})$ et un corps de nombres K de degré fini sur \mathbb{Q} tel que $g^{-1}\Gamma g \subset PSL_2(K)$.

Démonstration du lemme. Comme ici par hypothèse, on a Γ d'aire finie, le groupe Γ contient un élément hyperbolique d'après la proposition 47. Ainsi il existe $g \in SL_2(\mathbb{R})$ et $\lambda \neq 1$ tel que $g^{-1}Tg = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$. Quitte à remplacer Γ par $g^{-1}\Gamma g$, ce qui ne change pas le résultat, on peut supposer $g = Id$. Posons $K = F(\lambda)$. Comme Γ est d'aire finie, on peut choisir S dans Γ tel que $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ avec $b > 0$ et $c \neq 0$. Le fait de pouvoir trouver un tel S avec $c \neq 0$ découle de la proposition 47, sinon on obtient un groupe de translation qui n'est pas d'aire finie. Si b est non nul, on peut toujours trouver un représentant avec $b > 0$. Sinon de la même manière, il existe un élément $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ avec b' non nul (par conjugaison par un élément échangeant 0 et ∞); le produit

de ces deux éléments donne l'élément cherché. Si l'on pose $h = \begin{pmatrix} \sqrt{b} & 0 \\ 0 & \frac{1}{\sqrt{b}} \end{pmatrix}$, $h^{-1}\Gamma h$ contient deux éléments :

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} (\lambda \neq 1) \text{ et } T_1 = \begin{pmatrix} \alpha & 1 \\ \beta & \gamma \end{pmatrix} (\beta \neq 0)$$

Prenons alors un élément $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ quelconque de $h^{-1}\Gamma h$,

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a\lambda & b\lambda \\ c\lambda^{-1} & d\lambda^{-1} \end{pmatrix}$$

est un élément de $h^{-1}\Gamma h$ et ainsi $a + d$ et $a\lambda + d\lambda^{-1}$ sont dans K . Donc a et d sont dans K . En particulier, α et γ sont dans K et comme $\det(T_1) = 1$, β est dans K . Enfin la relation

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \alpha & 1 \\ \beta & \gamma \end{pmatrix} = \begin{pmatrix} a\alpha + b\beta & a + b\gamma \\ c\alpha + d\beta & c + d\gamma \end{pmatrix}$$

entraîne $a\alpha + b\beta$ et $c + d\gamma$ sont dans K . Donc comme a, α, d, γ et β sont dans K on en déduit que b et c sont dans K . \square

Théorème 58. Plaçons-nous sous les mêmes hypothèses que le lemme. Soit $F = \mathbb{Q}(\text{Tr}(\Gamma))$ et $A = F[\Gamma] = \left\{ \sum_{i=1}^d a_i T_i, a_i \in F, T_i \in \Gamma \right\}$. Alors A est une algèbre de quaternions sur F .

Démonstration du théorème. D'après le lemme 57, nous savons, quitte à conjuguer Γ par des éléments de $SL_2(\mathbb{R})$, que Γ contient deux éléments

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} (\lambda \neq 1) \text{ et } T_1 = \begin{pmatrix} \alpha & 1 \\ \beta & \gamma \end{pmatrix} (\beta \neq 0)$$

et $\Gamma \subset PSL_2(K)$ avec $K = F(\lambda)$, K étant une extension quadratique de F ou bien $K = F$. On peut affirmer, comme $\Gamma \subset M_2(K)$, que $2 \leq \dim_F(A) \leq 8$. Prouvons à présent qu'il s'agit bien d'une algèbre de quaternions.

1. Son radical R est trivial; en effet soit $T \in R$, il existe donc n entier tel que $T^n = 0$, ainsi $\det(T) = 0$ et pour j tel que $1 \leq j \leq n$ on a $\text{Tr}(T^j) = \text{Tr}(T)^j$ d'où $\text{Tr}(T) = 0$. Si l'on écrit T sous la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on a $a + d = 0$; de plus R est un idéal d'où $T_0 T \in R$ et $\lambda a + \lambda^{-1} d = 0$ donc $a = d = 0$, de même on obtient $b = c = 0$. Donc T est nul.

2. Son centre est F ; si l'on écrit à nouveau T sous la forme $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, comme T commute avec T_0 et T_1 , on en déduit immédiatement $b = c = 0$ et $a = d$; mais $a = \frac{1}{2} \text{Tr}(T)$ et $\text{Tr}(T) \in F$ donc $a \in F$ et $T \in F$.
3. Sa dimension est 4; en effet avec ce que l'on a montré précédemment A est une algèbre centrale simple, ainsi sa dimension est un carré donc ce ne peut être que 4.

□

Lemme 59. *Soit Γ un groupe fuchsien d'aire finie et $F = \mathbb{Q}(\text{Tr}(\Gamma))$. On suppose que $\dim_{\mathbb{Q}}(F)$ finie, et $\text{Tr}(\Gamma)$ contenu dans l'anneau des entiers de F , noté O_F . Soit*

$$A = F[\Gamma] = \left\{ \sum_{i=1}^d a_i T_i, a_i \in F, T_i \in \Gamma \right\}$$

$$O = O_F[\Gamma] = \left\{ \sum_{i=1}^d a_i T_i, a_i \in O_F, T_i \in \Gamma \right\}$$

Alors O est un ordre de l'algèbre de quaternions A .

Démonstration du lemme. D'après le lemme 57, nous savons, quitte à conjuguer Γ par des éléments de $SL_2(\mathbb{R})$, que Γ contient deux éléments

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} (\lambda \neq 1) \text{ et } T_1 = \begin{pmatrix} \alpha & 1 \\ \beta & \gamma \end{pmatrix} (\beta \neq 0)$$

et $\Gamma \subset PSL_2(K)$ avec $K = F(\lambda)$, K étant une extension quadratique de F ou bien $K = F$. On remarque tout d'abord que O est bien un sous-anneau de A , qu'il contient l'identité et qu'il engendre A sur F . Il nous reste à voir que c'est un O_F -module de type fini.

Soit $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O$; comme $T_0 T \in O$, on obtient $a + d \in O_F$ et $\lambda a + \lambda^{-1} d \in O_F$. Remarquons que λ et λ^{-1} sont des unités de K et $O_F \subset O_K$. Ainsi a et d sont dans un idéal fractionnaire $\frac{1}{\lambda^2 - 1} O_F$ de K . De même comme $T T_1 \in O_K$, on a $a\alpha + b\beta$ et $c + d\gamma$ éléments de $\frac{1}{\lambda^2 - 1} O_F$. Ainsi on en déduit que b et c sont aussi éléments de $\frac{1}{\lambda^2 - 1} O_F$. Pour tout élément T de Γ , tous ses coefficients sont des éléments de l'idéal fractionnaire $\frac{1}{\lambda^2 - 1} O_F$.

Ainsi O est un sous- O_F -module d'un module libre de rang 4, c'est finalement un O_F -module de type fini car l'anneau O_F est noethérien. Pour voir une démonstration de ce théorème, on pourra consulter [7].

□

Démonstration de la nécessité des conditions 1 et 2 du théorème 56

Soit donc k un corps de nombres totalement réel de degré n . Donnons des notations qui nous seront utiles par la suite.

Proposition-Définition 60. *Si A est l'algèbre de quaternions $\left(\frac{a,b}{k}\right)$ et $\sigma : k \rightarrow K$ un morphisme de corps, alors on note A^σ l'algèbre de quaternions $\left(\frac{\sigma(a), \sigma(b)}{\sigma(k)}\right)$ et on a alors $A^\sigma \otimes K \simeq \left(\frac{\sigma(a), \sigma(b)}{K}\right)$.*

Démonstration. Il suffit simplement de démontrer la seconde assertion qui est en fait claire par propriétés du produit tensoriel.

□

Considérons à présent une algèbre de quaternions A sur le corps k ; posons φ_1 le morphisme identité de k dans \mathbb{R} et φ_i les autres morphismes de k dans \mathbb{R} pour $2 \leq i \leq n$.

Proposition-Définition 61. *Supposons qu'il existe des isomorphismes d'algèbres ρ_i tels que :*

$$\rho_1 : A^{\varphi_1} \otimes \mathbb{R} \longrightarrow M_2(\mathbb{R})$$

$$\rho_i : A^{\varphi_i} \otimes \mathbb{R} \longrightarrow \mathbb{H}$$

Dans ce cas, on dit que A n'est pas ramifiée en la place φ_1 et ramifiée en toutes les autres places φ_i . Alors on a les égalités suivantes :

$$\begin{aligned} N(x) &= \det(\rho_1(x)) \\ \text{Tr}(x) &= \text{trace}(\rho_1(x)) \\ \varphi_i(N(x)) &= N_{\mathbb{H}}(\rho_i(x)) \\ \varphi_i(\text{Tr}(x)) &= \text{Tr}_{\mathbb{H}}(\rho_i(x)) \end{aligned}$$

Démonstration. Elle est immédiate et résulte essentiellement des propriétés du produit tensoriel et de l'invariance du déterminant et de la trace par isomorphisme d'algèbre. \square

Si une algèbre de quaternions vérifie ces conditions, on dira qu'elle vérifie les conditions de produit tensoriel.

Nous sommes à présent en mesure d'entamer la démonstration de la condition nécessaire. Soit Γ un sous-groupe d'indice fini de $\Gamma(A, O)$ où A est une algèbre de quaternions sur k , corps de nombres totalement réel de degré n , vérifiant les hypothèses de produit tensoriel et O est un ordre de A . Pour tout élément T de Γ , $\text{Tr}(T) \in k$ et par conséquent F est contenu dans k et F est un corps de nombres totalement réel. Comme $\text{Tr}(O) \subset O_k$, nous voyons que $\text{Tr}(\Gamma) \subset O_F$ et la condition 1 est bien satisfaite. Démontrons alors la seconde condition et supposons bien sûr $2 \leq n$. La condition de produit tensoriel impose, pour $2 \leq i \leq n$, que $\varphi_i(\text{Tr}(\Gamma) \subset \text{Tr}_{\mathbb{H}}(\rho_i(O^1)))$. De plus pour tout x , on a $\varphi_i(N(x)) = N_{\mathbb{H}}(\rho_i(x))$; ainsi $\rho_i(O^1)$ est contenu dans l'ensemble $\mathbb{H}^1 = \{x \in \mathbb{H} \mid N_{\mathbb{H}}(x) = 1\}$. Or il est facile de voir que l'ensemble $\text{Tr}_{\mathbb{H}}(\mathbb{H}^1)$ coïncide avec le segment $[-2, 2]$, donc $\varphi_i(\text{Tr}(\Gamma))$ est borné dans \mathbb{R} pour $2 \leq i \leq n$. Il nous reste à montrer que $F = k$. Si toutefois k était une extension propre de F , il existerait alors un i ($2 \leq i \leq n$) tel que φ_i réduit à F soit l'identité. En utilisant ce φ_i et la définition de F , on voit que $\text{Tr}(\Gamma) = \varphi_i(\text{Tr}(\Gamma))$ est contenu dans le segment $[-2, 2]$. Mais ceci signifierait que Γ ne contiendrait aucun élément hyperbolique, ce qui est absurde. Donc $F = k$ et la nécessité est bien prouvée.

Démonstration de la suffisance des conditions 1 et 2 du théorème 56

Pour démontrer la suffisance ici, nous avons encore besoin de trois lemmes.

Lemme 62. *Soit Γ un groupe fuchsien d'aire finie et satisfaisant les conditions 1 et 2 du théorème 56. Alors $F = \mathbb{Q}(\text{Tr}(\Gamma))$ est un corps de nombres totalement réel. De plus, si φ est un plongement de F dans \mathbb{R} , alors $\varphi(\text{Tr}(\Gamma))$ est contenu dans l'intervalle $[-2, 2]$.*

Démonstration du lemme. Soient T un élément quelconque de Γ , u et $\frac{1}{u}$ ses valeurs propres. Soit φ un plongement de F dans \mathbb{C} différent de l'identité. Il s'étend en un morphisme ψ de $F(u)$ dans \mathbb{C} . Nous allons montrer que $|\psi(u)| = 1$. En effet, si toutefois l'on avait $|\psi(u)| \neq 1$, alors de l'inégalité

$$|\varphi(\text{Tr}(T^m))| = |\psi(u)^m + \frac{1}{\psi(u)^m}| \geq \left| |\psi(u)^m| - \left| \frac{1}{\psi(u)^m} \right| \right|$$

l'ensemble $\{\varphi(\text{Tr}(T^m)), m \in \mathbb{Z}\}$ ne serait pas borné, ce qui contredit la condition 2.

Ainsi $|\psi(u)| = 1$. D'où

$$\varphi(\text{Tr}(T)) = \psi(u) + \frac{1}{\psi(u)} = \psi(u) + \overline{\psi(u)}$$

Ceci implique que $\varphi(\text{Tr}(T))$ est un nombre réel compris entre -2 et 2. On voit notamment que pour un élément hyperbolique, ce nombre est compris strictement entre -2 et 2. \square

Lemme 63. Soit Γ un groupe fuchsien vérifiant $\mu(\Gamma \backslash \mathcal{H}) < \infty$ et satisfaisant les conditions 1 et 2 du théorème. Alors $A(\Gamma)$, l'algèbre de quaternions définie sur le corps F précédemment défini, à savoir

$$A(\Gamma) = \left\{ \sum_{i=1}^d a_i T_i, a_i \in F, T_i \in \Gamma \right\}$$

vérifie les conditions de produit tensoriel.

Démonstration. D'après le lemme 57, nous savons que Γ contient, quitte à conjuguer, les deux éléments suivants :

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} (\lambda \neq 1) \text{ et } T_1 = \begin{pmatrix} \alpha & 1 \\ \beta & \gamma \end{pmatrix} (\beta \neq 0)$$

Nous allons démontrer que $K = F(\lambda)$ est une extension quadratique de F . Pour cela deux cas de figure sont à étudier :

1. F est une extension propre de \mathbb{Q} ; il existe alors un plongement ψ de K dans \mathbb{C} tel que sur F , ψ ne soit pas l'identité. $\psi(\lambda)$ et $\frac{1}{\psi(\lambda)}$ sont les racines de l'équation $x^2 - \psi(t)x + 1 = 0$ où $t = \text{Tr}(T_0)$. Par le lemme précédent on obtient que $|\psi(t)| < 2$, car T_0 est hyperbolique, ainsi $\psi(K)$ est un corps imaginaire c'est-à-dire non réel. Or F est totalement réel donc $\psi(F)$ est réel. Donc K ne peut pas coïncider avec F .
2. $F = \mathbb{Q}$; dans ce cas, t est un nombre rationnel tel que $|t| > 2$. Par conséquent le polynôme $x^2 - tx + 1$ est irréductible sur \mathbb{Q} et K est une extension propre de F .

Pour a dans K , nous noterons a' son F -conjugué. Ainsi $\frac{1}{\lambda} = \lambda'$. Du fait que λ et λ' sont F -indépendants, $\text{Tr}(T_1) = \alpha + \gamma$ et $\text{Tr}(T_0 T_1) = \alpha\lambda + \gamma\lambda'$ appartiennent à F , on peut en déduire très facilement en écrivant α et γ selon la F -base (λ, λ') que $\alpha = \gamma'$ et puisque $\det(T_1) = 1$, $\beta \in F$. Ainsi on peut récrire

$$T_0 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} (\lambda \neq 1) \text{ et } T_1 = \begin{pmatrix} \alpha & 1 \\ \beta & \alpha' \end{pmatrix} (\beta \neq 0 \text{ et } \beta \in F)$$

Comme de plus Id , T_0 , T_1 et $T_0 T_1$ sont linéairement indépendants, il est facile de le démontrer, ils forment une F -base de $A(\Gamma)$ et l'on voit que

$$A(\Gamma) = \left\{ \begin{pmatrix} a & b \\ b'\beta & a' \end{pmatrix} \mid a, b \in K, \beta \in F \right\}.$$

Pour finir la preuve de ce lemme, nous avons besoin d'un autre lemme que nous allons énoncer et démontrer.

Lemme 64. Soit ψ un plongement de $K = F(\lambda)$ dans \mathbb{C} tel que ψ restreint à F soit différent de l'identité. Alors

1. pour tout élément $T = \begin{pmatrix} a & b \\ b'\beta & a' \end{pmatrix}$ de Γ on a $|\psi(a)| \leq 1$.
2. pour $T_1 = \begin{pmatrix} \alpha & 1 \\ \beta & \alpha' \end{pmatrix}$ on a $\psi(\beta) < 0$.

Démonstration du lemme intermédiaire. D'après le lemme 62, pour tout $T = \begin{pmatrix} a & b \\ b'\beta & a' \end{pmatrix}$ de Γ , on a l'inégalité $|\psi(TT_0^m)| \leq 2$. Notons que pour tout élément $a = \alpha_0\lambda + \alpha_1\lambda' \in K$, $\psi(a') = \psi(\alpha_0)\psi(\lambda') + \psi(\alpha_1)\psi(\lambda) = \psi(\alpha_0)\psi(\lambda) + \psi(\alpha_1)\psi(\lambda')$, puisque $|\psi(\lambda)| = 1$ d'après le lemme 62 et le fait que F soit un corps totalement réel. On a $\psi(TT_0^m) = \psi(a\lambda^m) + \psi(a'(\lambda')^m) = \psi(a\lambda^m) + \overline{\psi(a\lambda^m)} = 2\text{Re}(\psi(a)\psi(\lambda^m))$. Comme $\psi(\lambda)$ n'est pas une racine de l'unité, l'ensemble $\{\psi(\lambda)^m \mid m \in \mathbb{Z}\}$ est un sous-groupe dense du cercle unité S_1 . Ainsi pour tout $z \in S_1$ nous avons $|\text{Re}(\psi(a)z)| \leq 1$ ce qui implique $|\psi(a)| \leq 1$. Appliquons ceci à T_1 ; on obtient $|\psi(\alpha)| \leq 1$; comme $\det(T_1) = \alpha\alpha' - \beta = 1$ on a donc $\psi(\beta) < 0$. \square

Poursuivons alors la démonstration du lemme grâce à ce nouveau résultat. Posons comme toujours $(\varphi_i)_{1 \leq i \leq n}$ la famille des n plongements de F dans \mathbb{R} (en effet F est totalement réel) avec n la dimension de F sur \mathbb{Q} . On peut étendre chaque morphisme φ_i en un plongement ψ_i de $K = F(\lambda)$ dans \mathbb{C} ; on étend ensuite ψ_i en Ψ_i de la façon suivante :

$$\Psi_i : \begin{matrix} A(\Gamma) & \rightarrow & M_2(\mathbb{R}) \\ \begin{pmatrix} a & b \\ b'\beta & a' \end{pmatrix} & \mapsto & \begin{pmatrix} \psi_i(a) & \psi_i(b) \\ \psi_i(b'\beta) & \psi_i(a') \end{pmatrix} \end{matrix}$$

Alors $A^{\varphi_i} = A^{\psi_i} = \Psi_i(A(\Gamma))$ est une algèbre de quaternions sur le corps $\psi_i(F) = \varphi_i(F)$. On a immédiatement $A^{\varphi_i} \otimes \mathbb{R} \simeq M_2(\mathbb{R})$. Comme nous le voyons grâce à la preuve du lemme intermédiaire $\psi_i(a') = \psi_i(a)$ pour $2 \leq i \leq n$. Nous concluons en affirmant que

$$A^{\varphi_i} = \left\{ \begin{pmatrix} a & b \\ b'\psi_i(\beta) & a' \end{pmatrix} \mid a, b \in \psi_i(K), \beta \in F \right\}$$

En utilisant le lemme intermédiaire, comme $\psi_i(\beta) < 0$, on en déduit aisément $A^{\varphi_i} \otimes \mathbb{R} \simeq \mathbb{H}$. Il nous suffit d'exhiber une base convenable comme dans la définition 25 : prenons pour vecteur i la matrice $\begin{pmatrix} 0 & \psi_i(\lambda) \\ \frac{\psi_i(\beta)}{\psi_i(\lambda)} & 0 \end{pmatrix}$ et pour vecteur j la matrice $\begin{pmatrix} 0 & \frac{1}{\psi_i(\lambda)} \\ \psi_i(\lambda\beta) & 0 \end{pmatrix}$. \square

Achevons enfin la démonstration du théorème de caractérisation que nous nous étions promis de prouver.

Remarquons qu'en utilisant successivement les trois lemmes 59, 62 et 63 on obtient bien que F est un corps de nombres totalement réel; $A(\Gamma)$ est une algèbre de quaternions sur le corps F vérifiant les hypothèses de produit tensoriel et $O(\Gamma)$ est un ordre de $A(\Gamma)$. Il est clair que Γ est un sous-groupe de $\Gamma(A(\Gamma), O(\Gamma))$. Donc $\Gamma(A(\Gamma), O(\Gamma))$ est d'aire inférieure à celle de Γ ; comme Γ est d'aire finie, $\Gamma(A(\Gamma), O(\Gamma))$ est aussi d'aire finie, non nulle sinon un groupe fuchsien étant dénombrable, par recouvrement par les images du domaine fondamental sous l'action de Γ , \mathbb{H}^2 serait d'aire nulle. Ainsi Γ est d'indice fini dans $\Gamma(A(\Gamma), O(\Gamma))$, l'indice étant le quotient des deux aires. Donc Γ est bien un groupe fuchsien dérivé d'une algèbre de quaternions qui vérifie la propriété de produit tensoriel. \square

Cette caractérisation étant démontrée, nous allons en donner une version plus parlante dans le cas où $F = k = \mathbb{Q}$.

Théorème 65. *Soit Γ un groupe fuchsien d'aire finie. Alors Γ est dérivé d'une algèbre de quaternions sur \mathbb{Q} si et seulement si pour tout $T \in \Gamma$, on a $\text{Tr}(T) \in \mathbb{Z}$.*

Démonstration. Elle résulte immédiatement de la caractérisation précédente et du fait que $k = F$ en prenant $F = \mathbb{Q}$. \square

Remarque. On déduit de cette caractérisation que le groupe modulaire précédemment évoqué dérive d'une algèbre de quaternions sur \mathbb{Q} .

3.3 Critère d'arithméticité des groupes fuchiens

Nous avons vu précédemment qu'un groupe fuchsien Γ est dit arithmétique s'il est commensurable avec un groupe de la forme $\Gamma(A, O)$ ce qui revient à dire qu'il est commensurable à un groupe fuchsien dérivé d'une algèbre de quaternions. Nous allons maintenant pouvoir caractériser les groupes fuchiens arithmétiques mais nous ne démontrerons que le sens réciproque de la caractérisation. Pour le sens direct, on pourra se référer à [8].

Théorème 66. *Soit Γ un groupe fuchsien d'aire finie. Notons $\Gamma^{(2)}$ le sous-groupe de Γ engendré par $\{T^2 \mid T \in \Gamma\}$. Le groupe fuchsien Γ est arithmétique si et seulement si $\Gamma^{(2)}$ dérive d'une algèbre de quaternions vérifiant les conditions de produit tensoriel.*

Démonstration. D'après la propriété 48, le groupe Γ est de type fini. Le sous-groupe $\Gamma^{(2)}$ est distingué dans Γ car un élément de $\Gamma^{(2)}$ est de la forme T^2 avec $T \in \Gamma$ et pour tout U dans Γ , on a $U^{-1}TU = (U^{-1}TU)^2$ qui appartient bien à $\Gamma^{(2)}$. L'ensemble $\Gamma/\Gamma^{(2)}$ est donc un groupe, de type fini, et tous ses éléments T vérifient $T^2 = 1$ donc sont leur propre inverse. L'égalité $(TU)(UT) = 1$ entraîne donc $TU = UT$. Le groupe $\Gamma/\Gamma^{(2)}$ est donc abélien ce qui entraîne, compte-tenu des autres conditions, qu'il est fini. Si $\Gamma^{(2)}$ dérive d'une algèbre de quaternions, Γ est commensurable à un groupe dérivant d'une algèbre de quaternions donc est arithmétique. \square

On peut donc en déduire une caractérisation des groupes arithmétiques purement en terme de la trace.

Théorème 67. *Soit Γ un groupe fuchsien d'aire finie. Le groupe Γ est arithmétique si et seulement si le corps $F = \mathbb{Q}(\text{Tr}(\Gamma^{(2)}))$ est un corps de nombres tel que les éléments de $\text{Tr}(\Gamma^{(2)})$ soient entiers sur F et que pour tout plongement φ de F dans \mathbb{C} différent de l'identité, $\varphi(\text{Tr}(\Gamma^{(2)}))$ soit borné dans \mathbb{C} .*

Conclusion

Nous avons présenté quelques propriétés remarquables des groupes fuchsien. Le cadre de la géométrie hyperbolique permet d'obtenir des propriétés géométriques (domaine fondamental) et aboutit à une classification intéressante en terme d'aire de ce domaine. On pourrait prolonger cette étude vers les systèmes dynamiques discrets en étudiant le comportement des différents types d'éléments de $PSL_2(\mathbb{R})$: elliptique, parabolique ou hyperbolique.

Dans la dernière partie, nous nous sommes intéressés au lien avec les algèbres de quaternions. Le théorème de Wedderburn pour les algèbres non commutatives de petite dimension fournit des résultats exceptionnels : une algèbre de quaternions est soit un corps gauche soit une algèbre de matrices. Grâce à lui, nous avons abouti à une caractérisation algébrique des groupes fuchsien uniquement en terme de trace.

Références

- [1] N. Bourbaki, *Modules et anneaux semi-simples*, Algèbre, chapitre 8, Éléments de Mathématiques, vol. 23, Hermann, 1958.
- [2] N. Jacobson, *Basic algebra II*, deuxième édition, W. H. Freeman and company, janvier 1989.
- [3] S. Katok, *Fuchsian groups*, Chicago Lectures in Mathematics, The University of Chicago Press, 1992.
- [4] S. Lang, *Algebra*, troisième édition, Addison-Wesley Publishing Company, mars 1993.
- [5] F. Paulin, *Topologie algébrique élémentaire*, Cours de magistère 2001-2002 à l'École Normale Supérieure, disponible sur le site internet du Département de Mathématiques et Applications à l'adresse <http://www.dma.ens.fr/edition/index.html>.
- [6] A. Ramsay and R. D. Richtmyer, *Introduction to hyperbolic geometry*, Springer-Verlag, 1995.
- [7] P. Samuel, *Théorie algébrique des nombres*, deuxième édition, Hermann, 1971.
- [8] K. Takeuchi, *A characterization of arithmetic fuchsian groups*, Journal of the Mathematical Society of Japan **27** (1975), n° 4, 600–612.