L'équation de Pell-Fermat non commutative

Aurel Page

14 octobre 2010

Résumé

On s'intéresse dans ce texte à la conception d'algorithmes pour résoudre une généralisation non commutative de l'équation de Pell-Fermat. Après avoir brièvement décrit l'équation de Pell-Fermat classique, on en introduit une généralisation non commutative en lien avec les algèbres de quaternions et on explique comment résoudre cette équation de manière effective. Enfin, on généralise encore l'équation pour ne plus se placer sur les rationnels mais sur un corps de nombres, et on expose comment ce problème est relié à de nombreuses autres questions, par exemple sur la cohomologie des groupes arithmétiques ou les variétés hyperboliques de dimension 3.

Table des matières

1 L'équation de Pell-Fermat

1.1 Anneaux d'entiers quadratiques

Soit d un entier strictement positif qui n'est pas un carré (de sorte que $\sqrt{d}$ est irrationnel). On appelle *équation de Pell-Fermat* l'équation

$$x^2 - dy^2 = 1,\ x, y \in \mathbb{Z}. \tag{1}$$

Remarquons dès maintenant que (1) admet les *solutions triviales* $(\pm 1, 0)$, et que si d est un carré, alors (1) n'admet pas de solution non triviale. On sait depuis longtemps que l'ensemble des solutions de cette équation forme un groupe abélien pour la loi

$$(x_1, y_1) * (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)$$

grâce à l'identité de Brahmagupta

$$(x_1^2 + dy_1^2)(x_2^2 + dy_2^2) = (x_1x_2 + dy_1y_2)^2 + d(x_1y_2 + x_2y_1)^2.$$

Nous allons voir que cette identité n'est pas miraculeuse, puis nous décrirons précisément la structure de l'ensemble des solutions.

Ayant factorisé l'équation en $x^2 - dy^2 = (x + \sqrt{d}y)(x - \sqrt{d}y)$, il est naturel d'introduire l'anneau $A = \mathbb{Z}\big[\sqrt{d}\big]$. Cet anneau est muni d'un automorphisme $\bar{\cdot} : x + \sqrt{d}y \mapsto x - \sqrt{d}y$. Le polynôme caractéristique d'un élément $a \in A$ est $(X-a)(X-\bar{a}) = X^2 - \mathrm{tr}(a)X + \mathrm{N}(a) \in \mathbb{Z}[X]$, la *trace* tr est additive et la *norme* N est multiplicative. La multiplicativité de la norme est exactement l'identité de Brahmagupta, et $(x, y) \in \mathbb{Z}^2$ est solution de (1) si et seulement si $\mathrm{N}(x + \sqrt{d}y) = 1$. On notera $A_1^\times = \{a \in A \mid \mathrm{N}(a) = 1\} \subset A^\times$.

1.2 Géométrie euclidienne

Afin d'étudier la structure du groupe $A_1^\times$, on souhaite le réaliser géométriquement, c'est-à-dire comme un sous-groupe discret d'un groupe d'isométries. Remarquons tout d'abord que l'inclusion $A \subset \mathbb{R}$ ne convient pas puisque A est dense dans $\mathbb{R}$. Affinons cependant cette inclusion et considérons l'application

$$\iota : \begin{cases} A \longrightarrow \mathbb{R}^2 \\ a \longmapsto (a, \bar{a}) \end{cases}$$

L'application ι est un homomorphisme injectif d'anneaux et son image est discrète, puisque pour $\iota(a)$ dans un compact de $\mathbb{R}^2$, a et $\bar{a}$ sont bornés, donc les coefficients du polynôme caractéristique de a sont bornés et il n'y a donc qu'un nombre fini de possibilités pour a. On a donc réalisé géométriquement le groupe additif A, c'est un bon début.

L'image $\iota(A_1^\times)$ est incluse dans l'hyperbole H d'équation $xy = 1$. Considérons donc l'application

$$\ell : \begin{cases} H \longrightarrow \mathbb{R}^2 \\ (x, y) \longmapsto (\log|x|, \log|y|) \end{cases}$$

Alors ℓ est un homomorphisme de groupes, de noyau $\{\pm(1,1)\}$ et d'image la droite d'équation $x+y=0$, et l'image $L=\ell\circ\iota(A_1^\times)$ est discrète. On en déduit immédiatement l'isomorphisme $A_1^\times\cong\{\pm1\}\times L$, et L est ou bien trivial, ou bien isomorphe à $\mathbb{Z}$. Nous allons maintenant montrer qu'on est toujours dans le second cas.

Il s'agit de montrer qu'il existe toujours une solution non triviale de (1). Il existe une approche classique utilisant des approximations de $\sqrt{d}$ par des fractions continues. Elle possède l'avantage de fournir un algorithme pour trouver une solution. Nous n'utiliserons pourtant pas cette méthode, mais nous en exposerons ici une autre qui présente l'avantage de se généraliser au cas qui nous intéressera par la suite. Pour plus de détails sur l'équation de Pell-Fermat et les fractions continues, on pourra par exemple se référer à [Hin08].

Nous allons étudier un peu plus précisément la géométrie de A. Un *réseau* L d'un espace vectoriel réel V est un sous-groupe discret qui engendre V comme espace vectoriel, ce qui est équivalent au fait que V/L soit compact. Dans le cas qui nous intéresse, l'image $\iota(A)$ est un réseau de $\mathbb{R}^2$, et nous identifierons $\iota(A)$ et A. Le théorème essentiel que nous allons utiliser est le

Théorème 1 (Minkowski)**.** *Soit V un espace vectoriel réel de dimension n muni d'une mesure de Lebesgue λ, L un réseau dans V et $C\subset V$ une partie convexe compacte symétrique par rapport à l'origine telle que*

$$\lambda(C)\geq 2^n\lambda(V/L).$$

Alors $C\cap(L\setminus\{0\})\neq\varnothing$.

Nous allons alors montrer que $H/A_1^\times$ est compact, ce qui donnera immédiatement $L\cong\mathbb{Z}$.

Commençons par une première remarque : si on pose pour tout $r\in\mathbb{Z}\setminus\{0\}$, $A_r=\{a\in A\mid \mathrm{N}(x)=r\}$, on a $A_r/A_1^\times$ est fini. En effet si $a,b\in A_r$, alors $\mathrm{N}(ab^{-1})=1$, donc on a $a\equiv b\pmod{A_1^\times}$ si et seulement si $ab^{-1}\in A$ si et seulement si $a\bar{b}\in rA$ (car $b^{-1}=\bar{b}/r$), donc cela ne dépend que des classes de a et b modulo r, et A/rA est fini. On peut donc choisir Y_r un système fini de représentants pour $A_r/A_1^\times$.

On peut maintenant prouver le résultat annoncé. On munit $\mathbb{R}^2$ de la mesure de Lebesgue usuelle et on étend N à $\mathbb{R}^2$ en posant $\mathrm{N}(x,y)=xy$. Soit C un compact convexe symétrique de $\mathbb{R}^2$ tel que $\lambda(C)\geq 4\lambda(\mathbb{R}^2/A)$. Pour tout $r\in\mathbb{Z}\setminus\{0\}$, on pose $C_r=\{x\in C\mid \mathrm{N}(x)=r\}$ et $K_r=Y_r^{-1}C_r\subset H$, qui est compact. Soient enfin $R=\mathrm{N}(C)\cap\mathbb{Z}\setminus\{0\}$, qui est fini, et $K=\cup_{r\in R}K_r$. Alors $K\subset H$ est un compact tel que tout élément de H est équivalent sous $A_1^\times$ à un élément de K.

En effet, soit $h\in H$. Alors la multiplication par h préserve λ, donc on a $\lambda(\mathbb{R}^2/Ah)=\lambda(\mathbb{R}^2/A)$. On peut donc appliquer le Théorème de Minkowski au réseau Ah : il existe $a\in A\setminus\{0\}$ tel que $ah\in C$. Mais alors $r=\mathrm{N}(ah)=\mathrm{N}(a)\in R$. Comme $a\in A_r$, il existe $y\in Y_r$ et $u\in A_1^\times$ tels que $a=yu$. On obtient alors $h=a^{-1}(ah)=u^{-1}y^{-1}(ah)\in A_1^\times Y_r^{-1}C_r=A_1^\times K_r$, ce qui conclut. On a prouvé le

Théorème 2. *On a*

$$A_1^\times\cong\{\pm1\}\times\mathbb{Z}.$$

2 L'équation de Pell-Fermat non commutative

2.1 Algèbres de quaternions

On veut maintenant généraliser l'équation de Pell-Fermat, c'est-à-dire trouver une équation quadratique $Q(x_1, \dots, x_n) = 1$ dont l'ensemble des solutions forme un groupe. On peut tenter d'ajouter simplement une variable, c'est-à-dire de considérer la forme $x^2+ay^2+by^2$. Cependant cette tentative va échouer : en effet l'ensemble des valeurs prises par une forme quadratique ternaire n'est pas multiplicatif, par exemple pour $a = b = 1$ on a $3 = 1^2 + 1^2 + 1^2$ et $5 = 2^2 + 1^2 + 0^2$ mais $3 \times 5 = 15$ n'est pas une somme de trois carrés (réduire modulo 8 pour le voir). On peut également tenter de généraliser les anneaux que l'on a considéré et augmenter le degré, mais si on garde des anneaux commutatifs, la norme ne sera plus une forme quadratique. Nous allons voir que la bonne généralisation de l'équation de Pell-Fermat est la suivante, pour $a, b \in \mathbb{Z} \setminus \{0\}$ non tous les deux négatifs :

$$x^2 - ay^2 - bz^2 + abt^2 = 1,\ x, y, z, t \in \mathbb{Z}. \tag{2}$$

Encore une fois l'équation (2) admet les solutions triviales $(\pm 1, 0, 0, 0)$ et la condition sur a, b permet d'assurer que l'ensemble des solutions n'est pas trivialement fini. Nous allons maintenant décrire la structure sous-jacente à cette équation.

Soit F un corps de caractéristique différente de 2 et $a, b \in F^\times$. L'algèbre de quaternions sur F de paramètres (a, b), notée $\left(\frac{a,b}{F}\right)$, est l'unique algèbre unitaire engendrée par deux éléments i, j tels que

$$i^2 = a,\ j^2 = b \text{ et } ji = -ij.$$

Une telle algèbre est de dimension 4 sur F avec pour base $(1, i, j, ij)$, et est naturellement munie d'une involution F-linéaire $\bar{\cdot} : x + yi + zj + tij \mapsto x - yi - zj - tij$. Pour tout $v, w \in \left(\frac{a,b}{F}\right)$ on a $\overline{vw} = \overline{w}\,\overline{v}$. Tout élément $w \in \left(\frac{a,b}{F}\right)$ est annulé par le polynôme $(X - w)(X - \bar{w}) = X^2 - \mathrm{trd}(w)X + \mathrm{nrd}(w) \in F[X]$, la *trace réduite* trd est F-linéaire et la *norme réduite* nrd est multiplicative. En remarquant que $\mathrm{nrd}(x + yi + zj + tij) = x^2 - ay^2 - b^2 + abz^2$ on voit maintenant le rapport avec l'équation (2).

Donnons deux exemples d'algèbres de quaternions.

- L'algèbre de matrices $\mathcal{M}_2(F)$ est isomorphe à $\left(\frac{1,1}{F}\right)$ via le morphisme d'algèbres

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \mapsto i\ ;\ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto j.$$

  La trace réduite correspond à la trace usuelle et la norme au déterminant.
- L'anneau $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ est une algèbre de quaternions à division sur $\mathbb{R}$. La norme réduite est le carré de la norme L^2 usuelle dans la base $(1, i, j, ij)$.

Une algèbre de quaternions est à division si et seulement si elle n'est pas isomorphe à l'algèbre des matrices 2×2.

Les algèbres $\mathcal{M}_2(\mathbb{R})$ et $\mathbb{H}$ sont les seules algèbres de quaternions sur $\mathbb{R}$, et $\mathcal{M}_2(\mathbb{C})$ est la seule algèbre de quaternions sur $\mathbb{C}$. En effet pour tout corps F on a les isomorphismes élémentaires $\left(\frac{a,b}{F}\right) \cong \left(\frac{b,a}{F}\right) \cong \left(\frac{a,-ab}{F}\right) \cong \left(\frac{u^2a,v^2b}{F}\right)$ pour tout $a, b, u, v \in F^\times$.

Pour étudier l'équation (2), nous devons introduire des structures entières sur les algèbres de quaternions. Soit B une algèbre de quaternions sur $\mathbb{Q}$. Un *ordre* de B est un sous-groupe de type fini $\mathcal{O} \subset B$ tel que $\mathbb{Q}\mathcal{O} = B$ et qui est également un sous-anneau unitaire. On notera alors $\mathcal{O}_1^\times = \{w \in \mathcal{O} \mid \mathrm{nrd}(w) = 1\} \subset \mathcal{O}^\times$. Par exemple, $\mathcal{M}_2(\mathbb{Z})$ est un ordre dans $\mathcal{M}_2(\mathbb{Q})$. Si $a, b \in \mathbb{Z} \setminus \{0\}$, alors $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ est un ordre dans $B = \left(\frac{a,b}{\mathbb{Q}}\right)$, et $(x, y, z, t) \in \mathbb{Z}^4$ est solution de (2) si et seulement si $x + yi + zj + tij \in \mathcal{O}_1^\times$.

Les algèbres de quaternions sur $\mathbb{Q}$ admettent une classification très simple que nous décrivons ici. Soit $\mathcal{O}$ un ordre dans une $\mathbb{Q}$-algèbre de quaternions B et (x_1, x_2, x_3, x_4) une $\mathbb{Z}$-base de $\mathcal{O}$. Le *discriminant* de $\mathcal{O}$ est

$$\mathrm{disc}(\mathcal{O}) = \det\big(\mathrm{trd}(x_i x_j)_{1 \le i,j \le 4}\big) \in \mathbb{Z} \setminus \{0\},$$

qui ne dépend pas de la $\mathbb{Z}$-base choisie. Si $\mathcal{O}' \subset \mathcal{O}$ sont deux ordres de B, alors on a l'identité $\mathrm{disc}(\mathcal{O}') = [\mathcal{O} : \mathcal{O}']^2 \,\mathrm{disc}(\mathcal{O})$ où $[\mathcal{O} : \mathcal{O}']$ est l'indice de $\mathcal{O}'$ dans $\mathcal{O}$. On peut montrer que le discriminant d'un ordre est toujours un carré au signe près, le *discriminant réduit* d'un ordre est la racine carrée (positive) de la valeur absolue de son discriminant. Le *discriminant* de B est le discriminant réduit d'un ordre maximal de B. On a alors le

Théorème 3. *Le discriminant D d'une algèbre de quaternions B sur $\mathbb{Q}$ est un entier sans facteur carré. Le nombre de facteurs premiers de D est pair si $B_\mathbb{R} \cong \mathcal{M}_2(\mathbb{R})$, impair si $B_\mathbb{R} \cong \mathbb{H}$. De plus, l'application donnée par le discriminant*

$$\left\{\begin{array}{c}\textit{Classes d'isomorphisme}\\ \textit{d'algèbres de quaternions sur } \mathbb{Q}\end{array}\right\} \longrightarrow \left\{\begin{array}{c}\textit{entiers naturels}\\ \textit{sans facteur carré}\end{array}\right\}$$

est une bijection.

Remarquons que la propriété sur le nombre de facteurs premiers du discriminant est équivalente à la célèbre loi de réciprocité quadratique de Gauss.

La difficulté algorithmique du calcul du discriminant et d'un ordre maximal d'une algèbre de quaternions sur $\mathbb{Q}$ est « la même » (en un sens qu'on ne précisera pas) que celle de la factorisation de a et b.

2.2 Géométrie hyperbolique

On considère maintenant l'équation (2), $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ et $\mathcal{O} = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij$ l'algèbre de quaternions et l'ordre associés. Encore une fois on veut réaliser $\mathcal{O}_1^\times$ géométriquement. Considérons l'algèbre de quaternions réelle $B_\mathbb{R} = \left(\frac{a,b}{\mathbb{R}}\right)$. D'après la condition sur a, b on a l'isomorphisme $B_\mathbb{R} \cong \left(\frac{\mathrm{sgn}(a),\mathrm{sgn}(b)}{\mathbb{R}}\right) \cong \mathcal{M}_2(\mathbb{R})$. De plus $\mathcal{O} \subset B_\mathbb{R}$ est un réseau. En fixant un isomorphisme, on identifiera maintenant $B_\mathbb{R}$ et $\mathcal{M}_2(\mathbb{R})$. Alors le sous-groupe $\mathcal{O}_1^\times \subset \mathrm{SL}_2(\mathbb{R})$ est discret. Afin d'étudier les sous-groupes discrets de $\mathrm{SL}_2(\mathbb{R})$, on va introduire un peu de géométrie hyperbolique. Pour plus de détails sur la géométrie hyperbolique en dimension 2 on pourra se référer à [Kat92].

Le *demi-plan de Poincaré* est $\mathcal{H}^2 = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ muni de la métrique d induite par l'élément de longueur

$$\mathrm{d}\ell^2 = \frac{\mathrm{d}x^2 + \mathrm{d}y^2}{y^2}$$

et de l'aire μ induite, donnée par

$$\mathrm{d}S = \frac{\mathrm{d}x\,\mathrm{d}y}{y^2}$$

où $z \in \mathcal{H}^2$, $z = x + yi$ et $y > 0$. Les géodésiques pour cette métrique sont les demi-cercles et les droites orthogonaux à la droite réelle. L'espace $\mathcal{H}^2$ est complet, simplement connexe et de courbure constante -1. Le groupe $\mathrm{SL}_2(\mathbb{R})$ agit transitivement sur $\mathcal{H}^2$ par homographies :

$$g \cdot z = \frac{az+b}{cz+d} \text{ pour tout } z \in \mathcal{H}^2 \text{ et } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}).$$

Cette action induit un isomorphisme entre $\mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm 1\}$ et le groupe des isométries directes de $\mathcal{H}^2$. Le stabilisateur de tout point est conjugué au stabilisateur $\mathrm{SO}_2(\mathbb{R})$ du point i. Un *groupe fuchsien* est un sous-groupe discret de $\mathrm{PSL}_2(\mathbb{R})$. Un tel groupe Γ est *cocompact* si $\Gamma\backslash\mathcal{H}^2$ est compact ; il est *de coaire finie* si $\mu(\Gamma\backslash\mathcal{H}^2) < \infty$.

Soit B une $\mathbb{Q}$-algèbre de quaternions. On dit que B est *définie* si $B_{\mathbb{R}} \cong \mathbb{H}$ et *indéfinie* si $B_{\mathbb{R}} \cong \mathcal{M}_2(\mathbb{R})$. Supposons B indéfinie, et soit $\mathcal{O}$ un ordre dans B. On a vu que dans ce cas $\Gamma(\mathcal{O}) = \mathcal{O}_1^\times/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{R})$ est un groupe fuchsien. On a alors le

Théorème 4. *Soit B une $\mathbb{Q}$-algèbre de quaternions indéfinie de discriminant D et $\mathcal{O}$ un ordre dans B. Alors le groupe fuchsien $\Gamma(\mathcal{O})$ est de coaire finie. De plus $\Gamma(\mathcal{O})$ est cocompact si et seulement si B est une algèbre à division, si et seulement si $B \ncong \mathcal{M}_2(\mathbb{Q})$. Enfin, si $\mathcal{O}$ est un ordre maximal de B, alors*

$$\mu(\Gamma(\mathcal{O})\backslash\mathcal{H}^2) = \frac{\pi}{3}\phi(D)$$

où ϕ est l'indicatrice d'Euler définie par $\phi(n) = n\prod_{p|n}(1-p^{-1})$.

Notons que la démonstration de la partie sur la cocompacité de $\Gamma(\mathcal{O})$ est exactement la même que celle donnée à la section précédente pour l'équation de Pell-Fermat classique. Maintenant que nous en savons un peu plus sur $\mathcal{O}_1^\times$, nous pouvons déterminer algorithmiquement sa structure. C'est en fait équivalent à la détermination de la structure de $\Gamma(\mathcal{O})$, le passage de l'un à l'autre n'est pas compliqué mais ne sera pas explicité ici.

2.3 Algorithmes

Pour calculer avec le groupe $\Gamma(\mathcal{O})$, il est naturel de considérer le quotient $\Gamma(\mathcal{O})\backslash\mathcal{H}^2$. La manipulation algorithmique de ce quotient se fait grâce à la notion de domaine fondamental. Soit Γ un groupe fuchsien. Un ouvert connexe $\mathcal{F} \subset \mathcal{H}^2$ est un *domaine fondamental* pour Γ si

(i) $\bigcup_{\gamma\in\Gamma} \gamma \cdot \overline{\mathcal{F}} = \mathcal{H}^2$;

(ii) Pour tout $\gamma \in \Gamma \setminus \{1\}$, $\mathcal{F} \cap \gamma \cdot \mathcal{F} = \varnothing$;

(iii) $\mu(\partial\mathcal{F}) = 0$

où $\partial\mathcal{F}$ désigne la frontière de $\mathcal{F}$. Nous allons immédiatement nous intéresser à une classe particulière de domaines fondamentaux. Soit $p \in \mathcal{H}^2$ un point dont le stabilisateur dans Γ est trivial. Alors le *domaine de Dirichlet centré en p*

$$D_p(\Gamma) = \{z \in \mathcal{H}^2 \mid \forall \gamma \in \Gamma \setminus \{1\},\ \mathrm{d}(z,p) < \mathrm{d}(\gamma \cdot z, p)\}$$

est un domaine fondamental pour Γ, et $D_p(\Gamma)$ est convexe au sens hyperbolique : tout segment géodésique entre deux points de $D_p(\Gamma)$ est inclus dedans. L'idée de cette construction est de choisir (génériquement) un point dans chaque orbite en prenant le plus proche de p. De plus, si Γ est de coaire finie, alors $D_p(\Gamma)$ est un *polygone* : sa frontière est une réunion d'un nombre fini de segments appelés ses *côtés* ; l'intersection de deux côtés successifs est un *sommet* de $D_p(\Gamma)$. Introduisons, pour $\gamma \in \Gamma$ son *cercle isométrique centré en p* : $\mathrm{I}_p(\gamma) = \{z \in \mathcal{H}^2 \mid \mathrm{d}(z,p) = \mathrm{d}(\gamma \cdot z, p)\}$ qui est aussi la bissectrice du segment $[p, \gamma^{-1} \cdot p]$. Chaque côté de $D_p(\Gamma)$ est contenu dans un unique cercle isométrique. De plus le cercle isométrique d'un élément $\gamma \in \Gamma$ contient un côté de $D_p(\Gamma)$ si et seulement si $\mathrm{I}_p(\gamma^{-1})$ contient aussi un côté, et on a $\gamma \cdot \mathrm{I}_p(\gamma) = \mathrm{I}_p(\gamma^{-1})$. On obtient alors la structure suivante, appelée *couplage*, pour les côtés : ils sont groupés par deux (éventuellement confondus), avec un élément de Γ et son inverse envoyant un côté sur l'autre (voir Figure 1). Les éléments du groupe qui associent deux côtés sont appelés *transformations du couplage*. On a alors la

Proposition 5. *Les transformations du couplage d'un domaine de Dirichlet pour* Γ *engendrent le groupe* Γ.

Cela provient du fait que les translatés de $\overline{D_p(\Gamma)}$ par les transformations du couplage recouvrent $\mathcal{H}^2$. Maintenant, si s_1 est un sommet de $D_p(\Gamma)$ avec $s_1 = \mathrm{I}_p(\gamma) \cap \mathrm{I}_p(\gamma_1)$, alors le point $s_2 = \gamma_1 \cdot s_1$ est encore un sommet de $D_p(\Gamma)$. On peut alors écrire $s_2 = \mathrm{I}_p(\gamma_1^{-1}) \cap \mathrm{I}_p(\gamma_2)$ et réitérer le processus. Cela partitionne l'ensemble des sommets en *cycles* $(s_1, s_2, \ldots, s_m)$ avec $s_{m+1} = s_1$ (voir Figure 1). Un cycle est bien défini à permutation circulaire et inversion de l'ordre près. On associe à chacun de ces cycles une *transformation de cycle* $h = \gamma_1^{-1}\gamma_2^{-1}\cdots\gamma_m^{-1}$ qui fixe s_1. Elle est bien définie à conjugaison par une tranformation du couplage et inversion près. Chaque transformation de cycle h est donc d'ordre fini e et la relation $h^e = 1$ est appelée une *relation de cycle*. De plus, un côté est couplé avec lui-même si et seulement si la transformation du couplage correspondant est d'ordre deux. La relation $\gamma^2 = 1$ pour une telle transformation γ est appelée une *relation de réflexion*. On a alors le

Théorème 6. *Pour tout domaine de Dirichlet* $D_p(\Gamma)$, *le groupe* Γ *admet une présentation dont les générateurs sont les transformations du couplage et dont les relations sont les relations de cycle et de réflexion.*

Cela provient du fait que les relations de cycle et de réflexion représentent les seuls recouvrements possibles entre $\overline{D_p(\Gamma)}$ et ses translatés. Remarquons que cette présentation est explicite au sens où on dispose de manière calculable de deux isomorphismes réciproques entre Γ et le groupe finiment présenté abstrait G du théorème précédent. Dans un sens, si on a un mot en les générateurs de G, on peut évaluer ce produit dans Γ. Examinons le sens contraire. Lorsqu'on on dispose d'un domaine fondamental, étant donné un point $z \in \mathcal{H}^2$ il est naturel de vouloir calculer un élément de son orbite sous Γ dans le domaine fondamental,

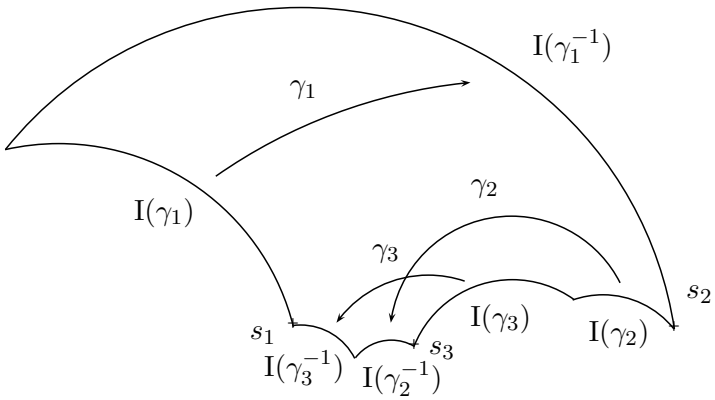

FIGURE 1 – Un cycle dans un domaine de Dirichlet

appelé *réduction de z*. Pour cela, il suffit d'appliquer des transformations du couplage tant que cela réduit la distance à p. Cet algorithme termine car Γ est discret et par définition le point d'arrivée est dans $\overline{D_p(\Gamma)}$. De plus, on obtient la transformation qui envoie z sur sa réduction comme mot en les tranformations du couplage. Enfin, comme p a un stabilisateur trivial dans Γ, l'application orbitale $\gamma \mapsto \gamma \cdot p$ est une bijection, et donc pour $\gamma \in \Gamma$ on peut réduire le point $\gamma \cdot p$, qui se réduira en p car c'est le seul élément de son orbite qui soit dans $\overline{D_p(\Gamma)}$, et donc on aura $w\gamma \cdot p = p$ avec w un mot en les générateurs de G, ce qui donne $\gamma = w^{-1}$.

Il ne reste donc plus qu'à calculer un domaine de Dirichlet pour un groupe $\Gamma = \Gamma(\mathcal{O})$. Pour des raisons de simplicité nous n'étudierons que le cas où $\mathcal{O}$ est un ordre maximal. Le cas général peut se traiter avec une légère modification, mais nous n'entrerons pas dans ces détails. Introduisons, pour toute partie $S \subset \Gamma$, le *domaine de Dirichlet partiel*

$$D_p(S) = \{z \in \mathcal{H}^2 \mid \forall \gamma \in S \setminus \{1\},\ \mathrm{d}(z,p) < \mathrm{d}(\gamma \cdot z, p)\}.$$

On remarque alors que $S \mapsto D_p(S)$ est décroissant, et qu'il existe une partie finie $S \subset \Gamma$ telle que $D_p(S) = D_p(\Gamma)$ (par exemple, prendre pour S l'ensemble des transformations du couplage). Il suffit donc d'énumérer les éléments de Γ, de calculer les domaines de Dirichlet partiels correspondants et de s'arrêter lorsqu'on a atteint le véritable domaine de Dirichlet. On a donc besoin de deux choses : une énumération de Γ et un test d'égalité entre $D_p(S)$ et $D_p(\Gamma)$.

Le test d'égalité est simple : comme $\mathcal{O}$ est maximal, on connait l'aire de $D_p(\Gamma(\mathcal{O}))$ qui est égale à $\mu(\Gamma(\mathcal{O})\backslash\mathcal{H}^2)$. Il suffit donc de savoir calculer l'aire de $D_p(S)$, ce qui se fait simplement en utilisant la

Proposition 7. *Soit $P \subset \mathcal{H}^2$ un polygone à n sommets, et d'angles intérieurs à chaque sommet $\alpha_1, \ldots, \alpha_n$. Alors l'aire de P est donnée par*

$$\mu(P) = (n-2)\pi - (\alpha_1 + \cdots + \alpha_n).$$

Pour énumérer les éléments de $\Gamma(\mathcal{O})$, il suffit d'énumérer les éléments de $\mathcal{O}$ et de sélectionner ceux qui sont de norme 1. On peut par exemple utiliser une $\mathbb{Z}$-base de $\mathcal{O}$ et énumérer les

combinaisons linéaires de ces éléments. Une autre idée, plus efficace en pratique, est d'équiper $\mathcal{O} \subset \mathcal{M}_2(\mathbb{R})$ d'une forme quadratique Q, par exemple le carré de la norme L^2 usuelle, et d'effectuer une énumération par valeurs de Q croissantes à l'aide d'un algorithme de réduction de réseau, par exemple avec l'algorithme de Fincke et Pohst [FP85].

3 Généralisation et problèmes reliés

3.1 Quaternions sur un corps de nombres

La généralisation naturelle de l'étude précédente consiste à considérer une algèbre de quaternions B sur un corps de nombres F de degré n et d'anneau des entiers $\mathbb{Z}_F$. Les structures entières sur une telle algèbre sont les *ordres* : un *ordre* est un $\mathbb{Z}_F$-module de type fini $\mathcal{O} \subset B$ tel que $F\mathcal{O} = B$ qui est également un sous-anneau unitaire. Les algèbres de quaternions sur un corps de nombres admettent encore une fois une classification simple. Soit v une place de F, on dit que v est *ramifiée* (resp. *décomposée*) si $B_v = B \otimes_F F_v$ est une algèbre à division (resp. est isomorphe à $\mathcal{M}_2(F_v)$), où F_v est la complétion de F en v. On a alors le

Théorème 8. *Une algèbre de quaternions B sur un corps de nombres F est ramifiée en un nombre fini, pair de places de F. Pour tout sous-ensemble fini S des places non complexes de F, de cardinal pair, il existe une unique (à isomorphisme près) algèbre de quaternions sur F ramifiée exactement aux places de S.*

Introduisons maintenant la partie géométrique. On note $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{v \in S_\infty} F_v$ et $B_{\mathbb{R}} = B \otimes_{\mathbb{Q}} \mathbb{R} = \prod_{v \in S_\infty} B_v$ où S_∞ est l'ensemble des places infinies de F. Si on considère le plongement diagonal $\iota : B \hookrightarrow B_{\mathbb{R}}$, alors pour tout ordre $\mathcal{O}$, l'image $\iota(\mathcal{O})$ est un réseau. On note encore $\mathcal{O}_1^\times = \{w \in \mathcal{O} \mid \mathrm{nrd}(w) = 1\}$ et $B_{\mathbb{R},1}^\times = \{w \in B_{\mathbb{R}} \mid \mathrm{nrd}(w) = 1\}$ où nrd désigne le prolongement continu $B_{\mathbb{R}} \to F_{\mathbb{R}}$ de la norme réduite $B \to F$. Remarquons qu'on a l'isomorphisme $B_{\mathbb{R},1}^\times \cong \mathrm{SL}_2(\mathbb{R})^d \times (\mathbb{H}_1^\times)^{r-d} \times \mathrm{SL}_2(\mathbb{C})^c$, où r est le nombre de places réelles de F, d le nombre de places réelles décomposées et c le nombre de places complexes (et $n = r + 2c$). On a déjà vu que l'espace sur lequel $\mathrm{SL}_2(\mathbb{R})$ agit naturellement est $\mathcal{H}^2 \cong \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$. Le groupe $\mathbb{H}_1^\times$ est compact. Enfin, on introduit le *demi-espace de Poincaré* $\mathcal{H}^3 = \mathbb{C} + \mathbb{R}_{>0} j \subset \mathbb{H}$ muni de la métrique d induite par l'élément de longueur

$$\mathrm{d}\ell^2 = \frac{\mathrm{d}x^2 + \mathrm{d}y^2 + \mathrm{d}t^2}{t^2}$$

et du volume Vol induit, donné par

$$\mathrm{d}V = \frac{\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}t}{t^3}$$

où $w \in \mathcal{H}^3$, $w = x + yi + tj$ avec $x, y, t \in \mathbb{R}$ et $t > 0$. Les géodésiques pour cette métrique sont les demi-cercles et les droites orthogonaux au plan complexe. L'espace $\mathcal{H}^3$ est complet, simplement connexe et de courbure constante -1. Le groupe $\mathrm{SL}_2(\mathbb{C})$ agit sur $\mathcal{H}^3$ par la formule :

$$g \cdot w = (aw + b)(cw + d)^{-1} \text{ pour tout } w \in \mathcal{H}^3 \text{ et } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}).$$

Cette action induit un isomorphisme entre $\mathrm{PSL}_2(\mathbb{C}) = \mathrm{SL}_2(\mathbb{C})/\{\pm 1\}$ et le groupe des isométries directes de $\mathcal{H}^3$, et on a $\mathcal{H}^3 \cong \mathrm{SL}_2(\mathbb{C})/\mathrm{SU}_2(\mathbb{C})$.

Soit $G = \mathrm{PSL}_2(\mathbb{R})^d \times \mathrm{PSL}_2(\mathbb{C})^c$ qui agit par isométries sur $X = (\mathcal{H}^2)^d \times (\mathcal{H}^3)^c$. Pour tout ordre $\mathcal{O}$ on peut définir le groupe $\Gamma(\mathcal{O}) \subset G$ comme étant l'image de $\mathcal{O}_1^\times$ dans G. Le groupe $\Gamma(\mathcal{O})$ est alors isomorphe à $\mathcal{O}_1^\times/\{\pm 1\}$, et on a le

Théorème 9. *Le groupe $\Gamma(\mathcal{O})$ est discret dans G, de covolume fini dans X. De plus $\Gamma(\mathcal{O})$ est cocompact si et seulement si B est une algèbre à division.*

Pour plus de détails sur l'arithmétique des algèbres de quaternions, on pourra se référer à [Vig80] ; pour une introduction à la géométrie hyperbolique en dimension 3 on pourra consulter par exemple [Mar07].

Il est sans doute possible de déterminer algorithmiquement un domaine fondamental et la structure du groupe $\Gamma(\mathcal{O})$, et d'en déduire la structure de $\mathcal{O}_1^\times$ et $\mathcal{O}^\times$. Cela n'a pour le moment été mis en œuvre que dans des cas particuliers (lorsque toutes les places infinies sont réelles ramifiées, le groupe est fini et une méthode simple d'énumération est connue depuis longtemps ; voir sections 3.3.1 et 3.3.2 pour les autres cas traités), et la conception d'un algorithme dans le cas général pose plusieurs problèmes, par exemple sur le calcul dans X : représentation des hyperplans, calcul d'intersections de demi-espaces, calcul du volume d'un polytope. Même dans les cas déjà réalisés, plusieurs problèmes subsistent : peut-on donner une évaluation a priori du temps de calcul nécessaire (la preuve de terminaison n'est pour le moment pas effective) ? Peut-on choisir de manière intelligente le centre du domaine de Dirichlet calculé (en termes de complexité du polytope calculé, de temps de calcul) ? Peut-on se passer de calculs approchés en gardant un algorithme efficace, ou prédire la précision nécessaire au calcul ? Peut-on améliorer les techniques d'énumération des éléments du groupe ? L'algorithme utilisé en pratique est en fait plus compliqué que celui décrit dans la section 2.3, il exploite l'algorithme de réduction et la structure de couplage afin de trouver plus rapidement les éléments dont les cercles isométriques forment la frontière du domaine de Dirichlet. Évaluer précisément l'apport de cette utilisation à l'algorithme global est également une question ouverte.

Par ailleurs, la résolution d'une équation de Pell-Fermat généralisée n'est pas la seule motivation de cette étude. Nous allons présenter maintenant quelques autres problèmes en rapport avec les groupes $\Gamma(\mathcal{O})$.

3.2 Cohomologie et opérateurs de Hecke

Soit $\mathcal{O}$ un ordre dans une algèbre de quaternions B sur un corps de nombres, et M un $\mathcal{O}_1^\times$-module. On peut alors construire les espaces de cohomologie des groupes $H^k(\mathcal{O}_1^\times, M)$. Ces espaces sont très intéressants. Ils sont munis d'*opérateurs de Hecke* de la manière suivante. Soit $\Gamma \subset \mathcal{O}_1^\times$ un sous-groupe d'indice fini $[\mathcal{O}_1^\times : \Gamma]$. On a alors une application de restriction induite par l'inclusion $\mathrm{res} : H^k(\mathcal{O}_1^\times, M) \to H^k(\Gamma, M)$, et dans l'autre sens une application de transfert $\mathrm{tr} : H^k(\Gamma, M) \to H^k(\mathcal{O}_1^\times, M)$ telle que la composée $\mathrm{tr} \circ \mathrm{res}$ est la multiplication par $[\mathcal{O}_1^\times : \Gamma]$ sur $H^k(\mathcal{O}_1^\times, M)$. Soit $\delta \in B$, alors $\mathcal{O}_1^\times \cap \delta\mathcal{O}_1^\times\delta^{-1}$ est d'indice fini dans $\mathcal{O}_1^\times$, et la conjugaison par δ induit un isomorphisme

$$\tilde{\delta} : H^k(\mathcal{O}_1^\times \cap \delta\mathcal{O}_1^\times\delta^{-1}, M) \to H^k(\delta^{-1}\mathcal{O}_1^\times\delta \cap \mathcal{O}_1^\times, M).$$

L'*opérateur de Hecke* T_δ associé à δ est alors défini par le diagramme commutatif :

$$\begin{array}{ccc} H^k(\mathcal{O}_1^\times, M) & \xrightarrow{T_\delta} & H^k(\mathcal{O}_1^\times, M) \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\uparrow{\scriptstyle \mathrm{tr}} \\ H^k(\mathcal{O}_1^\times \cap \delta\mathcal{O}_1^\times\delta^{-1}, M) & \xrightarrow[\tilde{\delta}]{} & H^k(\delta^{-1}\mathcal{O}_1^\times\delta \cap \mathcal{O}_1^\times, M) \end{array}$$

Ces opérateurs de Hecke ont les propriétés suivantes :
- Chaque T_δ est diagonalisable avec des valeurs propres réelles et un polynôme caractéristique à coefficients entiers ;
- L'opérateur T_δ ne dépend que de la double classe $\mathcal{O}_1^\times \delta \mathcal{O}_1^\times$;
- Les opérateurs T_δ commutent lorsque $\mathcal{O}$ est maximal.

Ces espaces de cohomologies posent de nombreuses questions, par exemple leur rang ou la taille de leur partie de torsion. On pourra trouver ce type d'études par exemple dans [FGT10] ou [BV10]. Ils sont également au cœur de nombreuses conjectures :
- Conjectures de modularité : d'après la philosophie de Langlands, à certaines représentations continues $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to G$ (où G est un groupe relié à $\mathcal{O}_1^\times$ en un sens qu'on ne précisera pas) on devrait pouvoir associer un $\mathcal{O}_1^\times$-module M_ρ et une classe de cohomologie $x \in H^*(\mathcal{O}_1^\times, M_\rho)$ propre pour les opérateurs de Hecke, et dont les valeurs propres sont compatibles avec les valeurs propres de $\rho(\varphi)$ pour certains éléments particuliers $\varphi \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (les « éléments de Frobénius »). On pourra par exemple trouver une formulation précise d'une conjecture de ce type dans [BV10] ;
- Construction d'unités dans des corps de classe et de points rationnels sur des courbes elliptiques : des constructions cohomologiques ont été proposées pour généraliser les conjectures de Stark (pour les unités) et de Darmon (pour les points rationnels). Ainsi il est conjecturé que certaines classes (explicites) dans la cohomologie de groupes particuliers $\mathcal{O}_1^\times$ sur un corps totalement réel F fournissent dans certains cas le logarithme d'une unité dans un corps de classe de certaines extensions quadratiques de F (voir par exemple [CD08]), dans d'autres cas un point sur une courbe elliptique sur F, défini à nouveau sur un corps de classe d'une certaine extension quadratique de F (voir par exemple [Gre09]).

3.3 Cas particuliers

3.3.1 Cas fuchsien

Un cas intéressant, où un algorithme calculant un domaine fondamental pour $\Gamma(\mathcal{O})$ a été réalisé par John Voight [Voi09], est le cas où le corps de base est totalement réel et l'algèbre de quaternions est ramifiée à toutes les places réelles sauf une. Dans ce cas, $\Gamma(\mathcal{O})$ est un groupe fuchsien et les méthodes décrites en section 2.3 s'appliquent presque inchangées. Outre le fait que c'est un cas relativement simple, il présente un grand intérêt puisque les (premiers) espaces de cohomologie décrits à la section 3.2, pour des modules bien choisis, sont isomorphes en tant que Hecke-modules à des espaces de formes modulaires de Hilbert, via une correspondance de Jacquet-Langlands. Cet isomorphisme a été exploité par John Voight et

Matthew Greenberg [GV10] pour calculer des systèmes de valeurs propres de Hecke de formes modulaires de Hilbert, complétant ainsi le travail de Dembélé et Donnely [DD08].

3.3.2 Cas kleinéen

Le dernier cas où un algorithme calculant un domaine fondamental pour $\Gamma(\mathcal{O})$ a été réalisé est celui où le corps de base possède une unique place complexe et l'algèbre de quaternions est ramifiée à toutes les places réelles. Dans ce cas, $\Gamma(\mathcal{O})$ est un sous-groupe discret de $\mathrm{PSL}_2(\mathbb{C})$, un *groupe kleinéen*. Cette réalisation était l'objet de mon mémoire de master [Pag10] sous la direction de John Voight, et nécessitait certaines modifications par rapport au cas de la dimension deux. Des algorithmes existaient déjà pour le cas où B est l'algèbre des matrices sur un corps quadratique imaginaire $\mathcal{M}_2(\mathbb{Q}(\sqrt{-d}))$, par exemple les méthodes de Swan [Swa71] ou Yasaki [Yas09], et un calcul dans une algèbre à division avait été effectué par Corrales, Jespers, Leal, Ángel del Río [CJLdR04].

Ce second cas particulier a également un intérêt supplémentaire, plutôt dans la direction de la géométrie cette fois-ci : il permet de calculer des groupes kleinéens, et donc des variétés (ou plus précisément des « orbifolds ») hyperboliques de dimension 3. Or ces variétés ne sont pas aussi bien comprises que celles de dimension 2, il est donc intéressant d'exploiter des calculs explicites pour les approcher expérimentalement. Pour plus de détails sur l'arithmétique des variétés hyperboliques de dimension 3 on pourra se référer à [MR03].

Donnons un exemple : la conjecture « virtuellement Haken. » Une variété hyperbolique de dimension 3 est *Haken* si elle est irréductible et si elle contient une surface immergée incompressible. Nous ne préciserons pas ces termes techniques ici, le fait essentiel est qu'une variété Haken peut être décomposée le long de sa surface immergée pour donner des variétés Haken plus simples, ce qui permet des arguments de récurrence pour ces variétés. Cependant, on peut observer qu'elles sont rares parmi toutes les variétés, mais une variété non Haken M peut avoir un revêtement fini qui soit Haken, permettant d'obtenir de l'information sur M. Une variété est *virtuellement Haken* si elle admet un revêtement fini qui est Haken. La conjecture « virtuellement Haken » affirme que toute variété irréductible de groupe fondamental infini est virtuellement Haken. Cette conjecture peut être testée algorithmiquement pour une variété dont on dispose du groupe fondamental, ce qui est le cas pour les variétés (dites *arithmétiques*) construites comme précédemment à partir d'algèbres de quaternions : en effet, pour que $M = \Gamma\backslash\mathcal{H}^3$ soit Haken, il suffit que $H^1(M,\mathbb{Z}) = H^1(\Gamma,\mathbb{Z})$ soit de rang non nul. Pour plus de détails sur cette conjecture et sa vérification expérimentale, on pourra consulter [DT03].

Références

[BV10] N. Bergeron and A. Venkatesh. The asymptotic growth of torsion homology for arithmetic groups. *preprint*, 2010.

[CD08] P. Charollois and H. Darmon. Arguments des unités de Stark et périodes de séries d'Eisenstein. *Algebra Number Theory*, 2 :655–688, 2008.

[CJLdR04] C. Corrales, E. Jespers, G. Leal, and Á. del Río. Presentations of the unit group of an order in a non-split quaternion algebra* 1. *Advances in Mathematics*, 186(2) :498–524, 2004.

[DD08] L. Dembélé and S. Donnelly. Computing Hilbert modular forms over fields with nontrivial class group. In *Proceedings of the 8th international conference on Algorithmic number theory*, pages 371–386. Springer-Verlag, 2008.

[DT03] N.M. Dunfield and W.P. Thurston. The virtual Haken conjecture : Experiments and examples. *Geometry and Topology*, 7(1) :399–441, 2003.

[FGT10] T. Finis, F. Grunewald, and P. Tirao. The Cohomology of Lattices in $\mathrm{SL}(2,\mathbb{C})$. *Experimental Mathematics*, 19(1) :29–63, 2010.

[FP85] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Mathematics of computation*, 44(170) :463–471, 1985.

[Gre09] M. Greenberg. Stark–Heegner points and the cohomology of quaternionic Shimura varieties. *Duke Math. J*, 147(3) :541–575, 2009.

[GV10] M. Greenberg and J. Voight. Computing systems of Hecke eigenvalues associated to Hilbert modular forms. *Arxiv preprint math.NT/0904.3908*, 2010.

[Hin08] M. Hindry. Arithmétique. *Tableau Noir. Calvage & Mounet*, 2008.

[Kat92] S. Katok. *Fuchsian groups*. University of Chicago Press, 1992.

[Mar07] A. Marden. *Outer Circles : An introduction to hyperbolic 3-manifolds*. Cambridge Univ Pr, 2007.

[MR03] C. Maclachlan and A.W. Reid. *The arithmetic of hyperbolic 3-manifolds*. Springer Verlag, 2003.

[Pag10] A. Page. Computing fundamental domains for arithmetic Kleinian groups. Master's thesis, Université Paris Diderot, 2010.

[Swa71] R.G. Swan. Generators and relations for certain special linear groups. *Advances in Math*, 6(1-77) :1971, 1971.

[Vig80] M.F. Vignéras. *Arithmétique des algèbres de quaternions*. Springer, 1980.

[Voi09] J. Voight. Computing fundamental domains for Fuchsian groups. *Journal de théorie des nombres de Bordeaux*, 21(2) :467–489, 2009.

[Yas09] D. Yasaki. Hyperbolic tessellations associated to Bianchi groups. *Arxiv preprint arXiv :0908.1762*, 2009.