

Journées mathématiques X-UPS

Année 2007

Systèmes dynamiques, groupes de matrices et applications arithmétiques

Françoise DAL'BO

Points de vue sur les valeurs aux entiers des formes quadratiques binaires

Journées mathématiques X-UPS (2007), p. 1-47.
https://doi.org/10.5802/xups.2007-01

Les Éditions de l'École polytechnique
Route de Saclay
F-91128 PALAISEAU CEDEX
https://www.editions.polytechnique.fr

Centre de mathématiques Laurent Schwartz
CMLS, École polytechnique, CNRS,
Institut polytechnique de Paris
F-91128 PALAISEAU CEDEX
https://portail.polytechnique.edu/cmls/

Publication membre du
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org

Journées mathématiques X-UPS
2007, p. 1–47 doi: 10.5802/xups.2007-01

POINTS DE VUE SUR LES VALEURS AUX ENTIERS DES FORMES QUADRATIQUES BINAIRES

par

Françoise Dal'Bo

Table des matières

Le but de ce texte est de motiver la présence de l'hypothèse $n > 2$ dans la conjecture d'Oppenheim. Plus précisément, nous nous proposons, au travers d'exemples explicites, de montrer qu'en dimension 2, l'adhérence de l'ensemble des valeurs prises aux points entiers par une forme quadratique irrationnelle, non dégénérée et indéfinie, peut être

Publication originelle dans Journées X-UPS 2007. Systèmes dynamiques, groupes de matrices et applications arithmétiques. Éditions de l'École polytechnique, 2007.

très variée. Pour mettre en lumière la richesse de ces ensembles, nous développons trois points de vue : le premier est arithmétique (paragraphes 1 et 2) ; le deuxième est dynamique et met en jeu une action du groupe $\mathrm{SL}_2(\mathbb{Z})$ (paragraphe 3) ; quant au troisième, il repose sur un lien entre les formes quadratiques et des trajectoires sur l'espace quotient $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$ (paragraphe 4). L'étude topologique de cet espace sera approfondie dans [Pau]. Ce dernier point de vue sur les trajectoires sera développé dans [Cou] en dimension $n \geqslant 3$ pour démontrer la conjecture d'Oppenheim.

1. Sur le développement en fractions continues

La principale motivation en théorie élémentaire des approximations diophantiennes est de limiter l'erreur entre un réel et ses valeurs approchées. Un des problèmes consiste à chercher la meilleure fonction (au sens du comportement asymptotique) $f : \mathbb{N} \to \mathbb{R}_+^*$ décroissante vers 0, telle que pour tout irrationnel y, dans une classe donnée, il existe une suite de rationnels irréductibles $(p_n/q_n)_{n\in\mathbb{N}}$ vérifiant

$$\left|y - \frac{p_n}{q_n}\right| \leqslant f(|q_n|) \quad \text{et} \quad \lim_{n\to+\infty} |q_n| = +\infty.$$

Depuis les travaux de Gustave Lejeune-Dirichlet, on sait que parmi toutes les suites de rationnels convergeant vers x, celle de *meilleure approximation* est construite à partir d'un algorithme utilisé à l'origine par Euclide pour calculer le plus grand diviseur commun entre deux entiers naturels. Comme nous allons le montrer, cette suite est reliée au *développement en fractions continues* des réels (voir aussi par exemple les livres [HW79, Khi97]). L'objet de ce paragraphe est de démontrer les principaux résultats sur cette approche des nombres et de la relier à l'étude des valeurs prises aux points entiers par une famille de formes quadratiques sur $\mathbb{R}^2$.

Fixons un nombre irrationnel x et posons $x_0 = x$, $n_0 = E(x_0)$, où $E(x)$ désigne la partie entière de x. Pour tout entier $i \geqslant 1$, on définit x_i et n_i par récurrence de la façon suivante :

$$x_i = \frac{1}{(x_{i-1} - n_{i-1})} \quad \text{et} \quad n_i = E(x_i).$$

Remarquons que pour $i \geqslant 1$, le réel x_i est un irrationnel strictement supérieur à 1 et que l'entier n_i est strictement positif. Par exemple, si $x = \sqrt{2}$, on obtient $n_0 = 1$, et $n_i = 2$ quelque soit $i \geqslant 1$. Si x est le *nombre d'or* $\phi = \frac{1+\sqrt{5}}{2}$, alors $n_i = 1$ pour tout $i \geqslant 0$.

Introduisons deux suites d'entiers $(p_k)_{k\geqslant -1}$ et $(q_k)_{k\geqslant -1}$ définies en posant $p_{-1} = 1$, $q_{-1} = 0$, $p_0 = n_0$, $q_0 = 1$ et pour tout entier $k \geqslant 0$,

$$p_{k+1} = n_{k+1}p_k + p_{k-1} \quad \text{et} \quad q_{k+1} = n_{k+1}q_k + q_{k-1}.$$

Cette relation entraîne que la suite $(q_k)_{k\geqslant 0}$ est croissante et strictement positive (et que $(q_k)_{k\geqslant 1}$ est strictement croissante). Si $x > 0$, alors la suite $(p_k)_{k\geqslant 0}$ est positive, croissante (et $(p_k)_{k\geqslant 1}$ est strictement positive, strictement croissante). Si $x < 0$, alors la suite $(p_k)_{k\geqslant 0}$ est négative, décroissante (et $(p_k)_{k\geqslant 2}$ est strictement négative, strictement décroissante).

On vérifie par récurrence que ces deux suites satisfont, pour tout $k \geqslant 0$, la relation

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k-1}.$$

Les suites $(p_k)_{k\geqslant -1}$ et $(q_k)_{k\geqslant -1}$ sont reliées aux coefficients d'une suite d'homographies. Pour le voir, introduisons, pour tout entier naturel i, l'homographie $h_i : \widehat{\mathbb{R}} = \mathbb{R} \cup \{\infty\} \to \widehat{\mathbb{R}}$ définie par $h_i(\infty) = n_i$, $h_i(0) = \infty$ et sinon

$$h_i(y) = \frac{n_i y + 1}{y}.$$

Par construction, on a $x_i = h_i(x_{i+1})$ et donc

$$x = h_0 h_1 \cdots h_i(x_{i+1}).$$

Pour $k \geqslant 0$, posons $g_k = h_0 h_1 \cdots h_k$. On vérifie par récurrence que l'homographie g_k s'écrit sous la forme

$$g_k : y \longmapsto \frac{p_k y + p_{k-1}}{q_k y + q_{k-1}}.$$

Pour obtenir des valeurs approchées rationnelles de x, nous allons nous intéresser à la suite $(p_k/q_k)_{k\geqslant 0}$. Le rationnel $p_k/q_k = g_k(\infty) =$

$h_0h_1\cdots h_k(\infty)$ s'écrit sous la forme

$$\frac{p_k}{q_k} = n_0 + \cfrac{1}{n_1 + \cfrac{1}{n_2 + \ddots + \cfrac{1}{n_{k-1} + \cfrac{1}{n_k}}}}.$$

En utilisant cette écriture, on montre facilement, puisque $n_i > 0$ pour $i \geqslant 1$, que la suite $(p_{2k}/q_{2k})_{k\geqslant 0}$ est croissante, tandis que $(p_{2k+1}/q_{2k+1})_{k\geqslant 0}$ est décroissante. Par ailleurs, $x = g_k(x_{k+1})$ et $x_{k+1} > n_{k+1}$, donc

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_k(q_kn_{k+1} + q_{k-1})} = \frac{1}{q_kq_{k+1}}.$$

On déduit de cette inégalité le théorème suivant qui montre en particulier que la suite $(p_k/q_k)_{k\geqslant 0}$ est adjacente (*i.e.* que les suites extraites paires et impaires sont monotones et convergent vers la même limite).

Théorème 1.1. *La suite $(p_k/q_k)_{k\geqslant 0}$ converge vers x et vérifie l'inégalité de Dirichlet*

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{q_k^2}\,.$$

Cette inégalité joue un rôle important en théorie des nombres. Historiquement, elle permit par exemple à Lagrange d'établir l'existence de solutions pour l'équation de *Pell-Fermat* $X^2 - AY^2 = 1$, où A est un entier positif non nul et non carré parfait (voir par exemple [Ita63]).

Définition 1.2. La suite $(p_k/q_k)_{k\geqslant 0}$ est appelée la *suite de meilleure approximation* de x et la suite $(n_i)_{i\geqslant 0}$ le *développement en fractions continues* de x.

L'inégalité de Dirichlet n'est pas optimale, on peut en effet l'améliorer en montrant par exemple (voir [HW79, Khi97] pour une démonstration) que pour tout $k \geqslant 0$

$$\left|x - \frac{p_k}{q_k}\right| < \frac{1}{2{q_k}^2}. \tag{1.1}$$

Comme le montre la proposition suivante, l'inégalité (1.1) caractérise les rationnels p_k/q_k et motive la terminologie : suite de *meilleure approximation*.

Proposition 1.3. *Soit a/b un rationnel avec a, b premiers entre eux, et $b > 0$. Si*

$$\left|x - \frac{a}{b}\right| < \frac{1}{2b^2},$$

alors a/b est un terme de la suite de meilleure approximation de x.

Démonstration. Soit a/b un rationnel vérifiant les hypothèses de la proposition. Commençons par montrer que si $c/d \neq a/b$ $(d > 0)$ est un rationnel vérifiant

$$|dx - c| \leqslant |bx - a|, \tag{1.2}$$

alors $d > b$.

Supposons donc que l'inégalité (1.2) soit vérifiée. On obtient

$$\left|x - \frac{c}{d}\right| < \frac{1}{2bd}.$$

Par conséquent

$$\left|\frac{c}{d} - \frac{a}{b}\right| \leqslant \left|\frac{c}{d} - x\right| + \left|x - \frac{a}{b}\right| < \frac{b+d}{2b^2d}.$$

Par ailleurs, puisque $c/d \neq a/b$, on a

$$\left|\frac{c}{d} - \frac{a}{b}\right| \geqslant \frac{1}{bd}.$$

donc $d > b$.

Montrons à présent que le rationnel a/b est un terme p_k/q_k de la suite de meilleure approximation de x.

Soit n_0 la partie entière de x, remarquons que $a/b \geqslant n_0$. En effet, si ce n'est pas le cas, on a

$$|x - n_0| < \left|x - \frac{a}{b}\right| \leqslant |bx - a|,$$

ce qui est impossible par (1.2) car $b \geqslant 1$. On en déduit, puisque la suite $(p_k/q_k)_{k\geqslant 0}$ est adjacente, que a/b est soit compris entre deux termes de la forme p_{k-1}/q_{k-1} et p_{k+1}/q_{k+1}, avec $k > 0$, soit strictement supérieur à p_1/q_1. Commençons par le premier cas en supposant

par l'absurde que a/b n'est pas un terme de la suite de meilleure approximation de x. On a

$$\left|\frac{a}{b}-\frac{p_{k-1}}{q_{k-1}}\right| \geqslant \frac{1}{bq_{k-1}},$$

par ailleurs

$$\left|\frac{a}{b}-\frac{p_{k-1}}{q_{k-1}}\right| < \left|\frac{p_k}{q_k}-\frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_kq_{k-1}},$$

donc $b > q_k$.

D'un autre côté, on a

$$\left|x-\frac{a}{b}\right| \geqslant \left|\frac{p_{k+1}}{q_{k+1}}-\frac{a}{b}\right| \geqslant \frac{1}{bq_{k+1}},$$

donc

$$|bx-a| \geqslant \frac{1}{q_{k+1}}.$$

Puisque $|q_kx-p_k| \leqslant 1/q_{k+1}$, on obtient

$$|q_kx-p_k| \leqslant |bx-a|,$$

ce qui est impossible par (1.2) car $b > q_k$.

Il reste le cas $a/b > p_1/q_1$. Sous cette hypothèse on a

$$\left|x-\frac{a}{b}\right| > \left|\frac{p_1}{q_1}-\frac{a}{b}\right| \geqslant \frac{1}{bq_1},$$

donc $|bx-a| > 1/q_1$.

Soit n_1 la partie entière de $1/(x-n_0)$. On a

$$|x-n_0| \leqslant \frac{1}{n_1}.$$

Remarquons que $q_1 = n_1$ donc

$$|bx-a| > |x-n_0|,$$

ce qui par l'inéquation (1.2) est impossible car $1 \leqslant b$. □

L'inégalité de Dirichlet nous conduit naturellement à associer à chaque irrationnel y le nombre réel positif ou nul $\nu(y)$ qui est la borne inférieure des $c > 0$ tels qu'il existe une infinité de rationnels p/q vérifiant

$$\left|y-\frac{p}{q}\right| \leqslant \frac{c}{q^2}.$$

D'après l'inégalité (1.1), on a $0 \leqslant \nu(y) \leqslant 1/2$.

Plus précisément, on peut montrer que la borne supérieure des $\nu(y)$ prise sur les irrationnels y est égale à $1/\sqrt{5}$ et est atteinte par exemple par le nombre d'or $\phi = \frac{1+\sqrt{5}}{2}$ (voir [HW79, Khi97] pour une démonstration).

Définition 1.4. Soit y un irrationnel.

- Si $\nu(y) > 0$, alors y est dit mal approché.
- Si $\nu(y) = 0$, alors y est dit bien approché.

Définition 1.5. Soit y un irrationnel. Si pour tout $\varepsilon > 0$, il existe un rationnel p/q vérifiant

$$y - \frac{p}{q} < 0 \quad (\text{resp. } y - \frac{p}{q} > 0) \quad \text{et} \quad \left|y - \frac{p}{q}\right| \leqslant \frac{\varepsilon}{q^2},$$

alors y est dit supérieurement (resp. inférieurement) bien approché.

Exemple 1.6.

(i) Le nombre $\sqrt{2}$ est mal approché. Plus précisément, pour tous $p \in \mathbb{Z}$ et $q \in \mathbb{N} - \{0\}$, on a

$$|\sqrt{2} - p/q| \geqslant 1/(4q^2).$$

En effet, cette inégalité est clairement vérifiée si $|\sqrt{2}-p/q| \geqslant 1$. Sinon, on a $0 < p/q < \sqrt{2}+1$, donc $0 < \sqrt{2}+p/q < 4$. Par ailleurs, comme $\sqrt{2}$ est irrationnel, on a $|\sqrt{2}-p/q|\,|\sqrt{2}+p/q| > 1/q^2$, ce qui implique l'inégalité recherchée.

(ii) Soit ℓ le *nombre de Liouville* égal à $\sum_{k=1}^{+\infty} 10^{-k!}$. Pour $n \geqslant 1$, posons $q_n = 10^{-n!}$ et $p_n/q_n = \sum_{k=1}^{n} 10^{-k!}$. On a

$$0 < \ell - \frac{p_n}{q_n} \leqslant \frac{1}{{q_n}^n},$$

donc ℓ est inférieurement bien approché.

L'exemple (ii) montre que pour ℓ, la vitesse de convergence de la suite de meilleure approximation $(p_k/q_k)_{k\geqslant 0}$ est bien plus rapide que $1/{q_k}^2$. Ce phénomène a été mis en évidence par Klaus F. Roth dans un cadre général, et est relié à la propriété de transcendance de ℓ (voir [HW79]).

Remarque 1.7. Soit $h : \widehat{\mathbb{R}} \to \widehat{\mathbb{R}}$ une homographie définie par $h(y) = \frac{ay+b}{cy+d}$, où a, b, c, d sont des entiers vérifiant $ad - bc = \pm 1$. Pour tout irrationnel x, on a

$$\nu(x) = \nu(h(x)).$$

En particulier si x est bien approché, alors $h(x)$ l'est aussi.

Démonstration. Soit $\left(p_n/q_n\right)_{n\geqslant 0}$ une suite de rationnels vérifiant $\lim |q_n| = +\infty$ telle que la suite $\left(q_n^2 \left| x - p_n/q_n \right|\right)_{n\geqslant 0}$ converge vers un réel α. Posons $P_n = ap_n + bq_n$ et $Q_n = cp_n + dq_n$. On peut supposer $Q_n \neq 0$. On a

$$h\Big(\frac{p_n}{q_n}\Big) = \frac{P_n}{Q_n}.$$

On vérifie par un simple calcul la relation suivante

$$\Big|h(x) - \frac{P_n}{Q_n}\Big| = \frac{1}{|cx+d|}\,\frac{1}{|Q_n|}\,\left|q_n x - p_n\right|.$$

Donc

$$Q_n^2\,\Big|h(x) - \frac{P_n}{Q_n}\Big| = \frac{1}{|cx+d|}\,\Big|c\,\frac{p_n}{q_n} + d\Big|q_n\,\left|q_n x - p_n\right|.$$

Par conséquent,

$$\lim_{n\to+\infty} Q_n^2\,\Big|h(x) - \frac{P_n}{Q_n}\Big| = \alpha.$$

Ceci entraîne que $\nu(h(x)) \leqslant \nu(x)$, et donc $\nu(h(x)) = \nu(x)$, en remplaçant x par $h(x)$ et h par h^{-1}. □

Le caractère bien approché d'un irrationnel x se lit sur son développement en fractions continues et sur sa suite de meilleure approximation.

Théorème 1.8. *Soient x un irrationnel, $(n_i)_{i\geqslant 0}$ son développement en fractions continues et $(p_k/q_k)_{k\geqslant 0}$ sa suite de meilleure approximation.*

Les propriétés suivantes sont équivalentes :

(i) *La suite $(n_{2i+1})_{i\geqslant 0}$ (resp. $(n_{2i})_{i\geqslant 0}$) n'est pas bornée.*

(ii) *Le réel 0 est une valeur d'adhérence de la suite*

$$(p_{2i}q_{2i} - xq_{2i}{}^2)_{i\geqslant 0} \quad (\textit{resp. } (p_{2i+1}q_{2i+1} - xq_{2i+1}{}^2)_{i\geqslant 0}).$$

(iii) *Le réel x est inférieurement (resp. supérieurement) bien approché.*

Démonstration. Pour tous les entiers n et m, introduisons la quantité

$$Q(n,m) = nm - xm^2.$$

En utilisant la relation

$$x = \frac{p_k x_{k+1} + p_{k-1}}{q_k x_{k+1} + q_{k-1}},$$

on obtient l'égalité

$$Q(p_k, q_k) = \frac{(-1)^{k+1}}{x_{k+1} + q_{k-1}/q_k}. \tag{1.3}$$

De plus, pour $k \geqslant 1$, on a $n_{k+1} < x_{k+1} < n_{k+1} + 1$ et $0 < q_{k-1} \leqslant q_k$, donc

$$\frac{1}{n_{k+1}+2} < |Q(p_k, q_k)| < \frac{1}{n_{k+1}}. \tag{1.4}$$

L'équivalence des assertions (i) et (ii) se déduit de (1.3) et (1.4).

L'implication (ii) $\Rightarrow$ (iii) découle de la définition 1.5 et de la position de p_k/q_k par rapport à x.

Démontrons que (iii) entraîne (ii). Pour cela, supposons que x soit bien approché par exemple inférieurement. Par hypothèse, il existe une suite non stationnaire de rationnels irréductibles $(p'_n/q'_n)_{n\geqslant 0}$, avec $q'_n > 0$, telle que $(Q(p'_n, q'_n))_{n\geqslant 0}$ converge vers 0 par valeurs négatives. Pour n assez grand, le rationnel p'_n/q'_n vérifie l'inégalité

$$\left| x - \frac{p'_n}{q'_n} \right| < \frac{1}{2{q'_n}^2}.$$

D'après la proposition 1.3, il existe $k_n > 0$ tel que $p'_n/q'_n = p_{k_n}/q_{k_n}$. Par conséquent 0 est la limite de la suite $(Q(p_{k_n}, q_{k_n}))_{n\geqslant 1}$. Cette suite est négative donc d'après l'égalité (1.3), l'entier k_n est pair. □

Parmi les nombres mal approchés, on distingue une famille de réels dont le développement en fractions continues est périodique à partir d'un certain rang. Cette famille se caractérise algébriquement.

Proposition 1.9. *Soient x un irrationnel et $(n_i)_{i\geqslant 0}$ la suite formant son développement en fractions continues.*

Cette suite est périodique à partir d'un certain rang si et seulement s'il existe des entiers a, b, c, avec a non nul, tels que $ax^2 + bx + c = 0$.

Démonstration. Notons encore $(h_i)_{i\in\mathbb{N}}$ et $(g_k)_{k\in\mathbb{N}}$ les suites intervenant dans la construction du développement en fractions continues de x. Supposons que la suite $(n_i)_{i\geqslant 0}$ soit périodique. Dans ce cas la suite $(h_i)_{i\in\mathbb{N}}$ est périodique. Donc il existe une homographie à coefficients entiers $h : \widehat{\mathbb{R}} \to \widehat{\mathbb{R}}$, et une suite extraite $(g_{k_j})_{j\geqslant 0}$ de la suite $(g_k)_{k\in\mathbb{N}}$, telles que $g_{k_j} = h^j$. La suite $(h^j(0))_{j\geqslant 0}(p_{k_j-1}/q_{k_j-1})_{j\geqslant 0}$ converge vers x, donc $h(x) = x$. Ceci entraîne que x est racine d'un polynôme de degré 2 à coefficients entiers, car x est irrationnel.

Si maintenant la suite $(n_i)_{i\geqslant 0}$ est périodique à partir d'un rang $p > 0$, le raisonnement précédent appliqué à la suite $(n_i)_{i\geqslant p}$ montre que le réel $h_{p-1}^{-1}\cdots h_0^{-1}(x)$ est fixé par une homographie à coefficients entiers, donc x l'est aussi.

Avant de démontrer la deuxième partie de l'énoncé, démontrons les résultats suivant.

Fait 1. *Soient x et y deux irrationnels différents, il existe une homographie $\gamma(z) = \frac{az+b}{cz+d}$, où a, b, c, d sont des entiers vérifiant $ad-bc = 1$, telle que $\gamma(x) > 0$ et $\gamma(y) < 0$.*

Démonstration. Notons respectivement $(n_i)_{i\geqslant 0}$ et $(m_i)_{i\geqslant 0}$ les développements en fractions continues de x et y, et $(g_k)_{k\geqslant 0}$ la suite d'homographies (à coefficients entiers et de déterminant ± 1) intervenant dans la construction du développement en fractions continues de x. Comme $x \neq y$, il existe $k \geqslant 0$ tel que $n_k \neq m_k$. Soit $p \geqslant 0$ le plus petit de ces k. Posons $x' = x$ et $y' = y$ si $p = 0$, et $x' = g_{p-1}^{-1}(x)$ et $y' = g_{p-1}^{-1}(y)$ si $p > 0$. Les irrationnels x' et y' ont des parties entières différentes, donc il existe un entier n tel que les signes de $x'' = x' + n$ et $y'' = y' + n$ soient différents. Introduisons les homographies $T(z) = z + 1$, $I(z) = 1/z$, et $S(z) = -1/z$. Si $x'' > 0$, on pose $\gamma = I^m T^n g_{p-1}^{-1}$, avec $m = 0$ si $\det g_{p-1} = 1$, et $m = 1$ si $\det g_{p-1} = -1$. Si $x'' < 0$ on pose $\gamma = SI^m T^n g_{p-1}^{-1}$. L'homographie γ convient. □

La démonstration de l'affirmation suivante est laissée au lecteur.

Fait 2. *Soient x et y deux irrationnels différents, et γ une homographie de la forme $\gamma(z) = \frac{az+b}{cz+d}$, où a, b, c, d sont des entiers vérifiant $ad -$*

$bc = 1$. Si x et y sont racines d'un même polynôme à coefficients entiers de degré 2, alors $\gamma(x)$ et $\gamma(y)$ sont également racine d'un polynôme à coefficients entiers de degré 2. De plus, si le développement en fractions continues de x est périodique à partir d'un certain rang, alors celui de $\gamma(x)$ l'est aussi. □

Revenons à la démonstration de la proposition. Supposons à présent que x soit solution de l'équation diophantienne $ax^2 + bx + c = 0$ ($a \neq 0$). Soit y l'autre solution, qui est aussi irrationnelle.

D'après les deux affirmations ci-dessus, quitte à remplacer x et y par $\gamma(x)$ et $\gamma(y)$, on peut supposer $x > 0$ et $y < 0$, donc $ac < 0$.

On rappelle que $(g_k)_{k\geqslant 0}$ est la suite d'homographies intervenant dans la construction du développement en fractions continues de x.

Soit $k \geqslant 0$, considérons les réels

$$x_{k+1} = g_k^{-1}(x) \quad \text{et} \quad y'_{k+1} = g_k^{-1}(y).$$

On a $x_k > 0$ par le début du paragraphe et $y'_k < 0$ comme le montre le calcul de g_k^{-1} et le fait que les coefficients $p_{k-1}, q_{k-1}, p_k, q_k$ de l'homographie g_k soient positifs. Donc ces deux réels satisfont une équation de la forme

$$a_k x^2 + b_k x + c_k = 0,$$

où a_k, b_k, c_k sont des entiers, et $a_k c_k < 0$.

En utilisant le fait que $x_k = (n_k x_{k+1} + 1)/x_{k+1}$, on montre par récurrence que ces coefficients satisfont la relation

$$b_k^2 - 4a_k c_k = b^2 - 4ac,$$

car

$$a_{k+1} = a_k n_k^2 + b_k n_k + c_k,$$
$$b_{k+1} = b_k + 2n_k a_k$$
et
$$c_{k+1} = a_k.$$

Par conséquent, a_k, b_k, c_k appartiennent à un ensemble fini. Donc il existe $k' > k > 0$ tels que $x_{k'} = x_k$ et $y_{k'} = y'_k$. La suite $(n_i)_{i\geqslant k}$ ne dépend que de x_k, elle est donc égale à la suite $(n_i)_{i\geqslant k'}$. Ainsi, la suite $(n_i)_{i\geqslant k}$ est périodique.

Remarquons pour finir que l'égalité $x_{k'} = x_k$ entraîne

$$g_k g_{k'}^{-1}(x) = x \quad \text{et} \quad g_k g_{k'}^{-1}(y) = y.$$

Donc en posant $h = g_k g_{k'}^{-1}$ ou $(g_k g_{k'}^{-1})^2$ on en déduit que x et y sont fixés par une homographie de la forme $h(z) = \frac{nz+p}{mz+q}$, où n, m, p, q sont des entiers vérifiant $nq - mp = 1$. □

Un irrationnel x satisfaisant une équation de la forme

$$ax^2 + bx + c = 0,$$

où a, b, c sont des entiers avec $a \neq 0$, est dit *quadratique*.

Corollaire 1.10. *Les irrationnels quadratiques sont mal approchés.* □

Des questions ouvertes se posent encore aujourd'hui sur le lien entre les nombres mal approchés et les nombres algébriques. L'une d'elles consiste à savoir si $\sqrt[3]{2}$ est mal approché.

La démonstration de la proposition 1.9 conduit à une autre caractérisation des réels quadratiques.

Remarque 1.11. Deux irrationnels quadratiques $x \neq y$ sont racines d'un même polynôme de degré 2 à coefficients entiers si et seulement s'il existe une homographie, différente de l'identité, $h(z) = \frac{nz+p}{mz+q}$, où n, m, p, q sont des entiers vérifiant $nq - mp = 1$, les fixant.

Comme nous l'avons remarqué dans la démonstration du théorème 1.8, le caractère bien approché d'un irrationnel x peut se formuler à l'aide de la forme quadratique Q_x sur $\mathbb{R}^2$ définie par

$$Q_x(X, Y) = XY - xY^2.$$

Il découle en effet de la définition 1.5 que 0 est une valeur d'adhérence de l'ensemble $Q_x(\mathbb{Z}^2) \cap \mathbb{R}_+^*$ (resp. $Q_x(\mathbb{Z}^2) \cap \mathbb{R}_-^*$) si et seulement si x est supérieurement (resp. inférieurement) bien approché. On déduit alors du théorème 1.8 que 0 est une valeur d'adhérence de l'ensemble $Q_x(\mathbb{Z}^2) \cap \mathbb{R}_+^*$ (resp. $Q_x(\mathbb{Z}^2) \cap \mathbb{R}_-^*$) si et seulement si la suite extraite paire (resp. impaire) du développement en fractions continues de x n'est pas bornée.

L'objet du paragraphe suivant est d'approfondir ce lien entre la nature topologique des ensembles $Q(\mathbb{Z}^2)$, où Q est une forme quadratique binaire, et celle arithmétique de réels « naturellement » associés à Q.

2. Petites valeurs de formes quadratiques binaires et arithmétique

Une *forme quadratique* sur $\mathbb{R}^n$ peut être considérée comme un polynôme homogène de degré 2 à n variables réelles $P = P(X_1, \dots, X_n)$. Pour l'étudier, une méthode consiste à lui associer la matrice symétrique réelle $n \times n$, notée $M_P = (a_{i,j})_{1 \leqslant i,j \leqslant n}$, dont le terme $a_{i,j} = a_{j,i}$ pour $i \neq j$, est la moitié du coefficient du monôme $X_i X_j$, et $a_{i,i}$ est le coefficient de $X_i X_i$. Une telle forme est dite *non dégénérée* si le déterminant de la matrice M_P n'est pas nul, et *indéfinie* si l'ensemble $P(\mathbb{R}^n)$ contient des valeurs strictement positives et des valeurs strictement négatives. Par définition, le déterminant de P, noté $\det P$, est le déterminant de M_P. Remarquons que si g appartient à $\mathrm{SL}_n(\mathbb{R})$, alors $Q = P \circ g$ est une forme quadratique dont la matrice vérifie

$$M_Q = {}^t g \, M_P \, g.$$

En particulier $\det M_Q = \det M_P$.

Dans la suite de cette partie, sauf pour la proposition 2.8 où $n = 3$, nous nous restreignons aux formes quadratiques sur $\mathbb{R}^2$, que nous appelons formes *binaires*. Nous notons $\mathcal{Q}$ (aussi noté $\mathcal{Q}_{1,1}$ dans le paragraphe 2 de [Pau]) l'ensemble des formes binaires non dégénérées et indéfinies.

On vérifie qu'un élément $P \in \mathcal{Q}$ est le produit de deux formes linéaires linéairement indépendantes. Autrement dit, il existe deux vecteurs de $\mathbb{R}^2$ (non uniques), linéairement indépendants, $u = (u_1, u_2)$ et $v = (v_1, v_2)$ tels que

$$P(X, Y) = (u_1 X + u_2 Y)(v_1 X + v_2 Y),$$

Nous notons $P = P_{(u,v)}$.

Nous allons nous intéresser aux petites valeurs de P prises aux points entiers.

Définition 2.1. On dit que P *représente* 0 s'il existe un couple d'entiers $(p,q) \neq (0,0)$ tel que $P(p,q) = 0$.

Remarque 2.2. La forme quadratique $P_{(u,v)}$ représente 0 si et seulement si u ou v est colinéaire à un vecteur de $\mathbb{Q}^2$.

Le théorème suivant établit un lien entre les petites valeurs non nulles de l'ensemble $P_{(u,v)}(\mathbb{Z}^2)$ et la nature arithmétique des vecteurs u et v.

Théorème 2.3. *Le réel* 0 *est une valeur d'adhérence de l'ensemble* $P_{(u,v)}(\mathbb{Z}^2) - \{0\}$ *si et seulement si* u_2/u_1 *ou* v_2/v_1 *sont des irrationnels bien approchés.*

Démonstration. Si u_1, u_2, v_1 ou v_2 est nul, alors le résultat découle de la définition d'irrationnels bien approchés. Nous nous plaçons donc dans le cas où $u_1u_2v_1v_2 \neq 0$.

Supposons que $x = u_2/u_1$ soit un irrationnel bien approché. Posons $v_2/v_1 = y$. La forme binaire P est proportionnelle au polynôme

$$P_0(X,Y) = (X + xY)(X + yY).$$

Considérons une suite $(p_k/q_k)_{k\geqslant 0}$ de rationnels vérifiant

$$\lim_{k\to+\infty} q_k \, |q_k x + p_k| = 0.$$

Quitte à extraire une sous-suite, on peut supposer $P_0(p_k, q_k) \neq 0$. Par ailleurs

$$|P_0(p_k, q_k)| \leqslant |p_k + xq_k| \cdot (|p_k + xq_k| + |q_k| \, |y - x|),$$

donc 0 est une valeur d'adhérence de l'ensemble $P(\mathbb{Z}^2) - \{0\}$.

Réciproquement, supposons qu'il existe une suite $((p_k, q_k))_{k\geqslant 0}$ de couples d'entiers telle que

$$P(p_k, q_k) \neq 0 \quad \text{et} \quad \lim_{k\to+\infty} P(p_k, q_k) = 0.$$

Cela entraîne que l'un au moins des réels u_1, u_2, v_1 ou v_2 n'est pas rationnel. Supposons par exemple que ce soit u_1. Posons $x = u_2/u_1$ et $v_2/v_1 = y \neq x$. On a

$$\lim_{k\to+\infty} q_k^2 \Big(\frac{p_k}{q_k} + x\Big)\Big(\frac{p_k}{q_k} + y\Big) = 0.$$

Donc $\lim_{k\to+\infty} q_k^2 = +\infty$ et la suite $(-p_k/q_k)_{k\geqslant 1}$ converge vers x ou vers y. Par conséquent, x ou y est un irrationnel bien approché. □

Remarquons que si q est un entier non nul, alors le signe de la quantité $P_0(p,q)$ est celui de $(\frac{p}{q}+x)(\frac{p}{q}+y)$. Donc si $\lim_{k\to+\infty} p_k/q_k = -x$ (resp. $\lim_{k\to+\infty} p_k/q_k = -y$), alors pour k grand, le signe de $P_0(p_k,q_k)$ est celui de $(\frac{p_k}{q_k}+x)(-x+y)$ (resp. $(\frac{p_k}{q_k}+y)(x-y)$). Cette remarque, ajoutée à la démonstration du théorème 2.3, permet d'énoncer le résultat plus précis suivant :

Corollaire 2.4. *Soient x et y des irrationnels distincts. Notons ε le signe de $(-x+y)$ et P la forme quadratique*

$$P(X,Y) = (X+xY)(X+yY).$$

Le réel 0 est une valeur d'adhérence de l'ensemble $P(\mathbb{Z}^2)\cap\mathbb{R}^*_\varepsilon$ si et seulement si x est inférieurement bien approché ou y est supérieurement bien approché. □

La présence de petites valeurs prises par une forme $P\in\mathcal{Q}$ en des points entiers a de fortes répercussions sur l'ensemble $P(\mathbb{Z}^2)$.

Proposition 2.5. *Soit $P\in\mathcal{Q}$. Si 0 est une valeur d'adhérence de l'ensemble $P(\mathbb{Z}^2)\cap\mathbb{R}^*_+$ (resp. $P(\mathbb{Z}^2)\cap\mathbb{R}^*_-$)), alors $\mathbb{R}_+$ (resp. $\mathbb{R}_-$) est inclus dans $P(\mathbb{Z}^2)$.*

Démonstration. Supposons qu'il existe une suite $((p_k,q_k))_{k\geqslant 0}$ de couples d'entiers telle que

$$P(p_k,q_k)>0 \quad\text{et}\quad \lim_{k\to+\infty} P(p_k,q_k)=0.$$

Soit x un réel strictement positif. Posons $a=\sqrt{x}$. Pour tout $k\geqslant 0$, il existe un entier naturel n_k tel que

$$n_k \leqslant \frac{a}{\sqrt{P(p_k,q_k)}} < n_k+1.$$

Donc

$$0\leqslant a-\sqrt{P(p_k,q_k)}\,n_k < \sqrt{P(p_k,q_k)}.$$

Par conséquent $\lim_{k\to+\infty}\sqrt{P(p_k,q_k)}\,n_k = a$. D'où

$$\lim_{k\to+\infty} P(n_kp_k,n_kq_k)=x.$$

Le cas où la suite $(P(p_k, q_k))_{k\geqslant 1}$ est négative se traite de façon analogue. □

On déduit de ce résultat et du corollaire 2.4, une caractérisation des formes $P_{(u,v)}$ pour lesquelles l'ensemble $P_{(u,v)}(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$, portant sur le couple (u, v).

Corollaire 2.6. *L'ensemble $P_{(u,v)}(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$ si et seulement si l'une des deux conditions est satisfaite :*

(i) *u_2/u_1 ou v_2/v_1 est un irrationnel supérieurement et inférieurement bien approché.*

(ii) *u_2/u_1 est un irrationnel supérieurement (resp. inférieurement) bien approché, et v_2/v_1 est un irrationnel inférieurement (resp. supérieurement) bien approché.* □

Donnons des exemples de formes quadratiques $Q \in \mathcal{Q}$ pour lesquelles l'ensemble $Q(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$.

Exemple 2.7.

(i) Notons x le « nombre univers » dont la suite de meilleure approximation $(p_k/q_k)_{k\geqslant 1}$ est définie par

$$\frac{p_k}{q_k} = \cfrac{1}{1+\cfrac{1}{2+\ddots+\cfrac{1}{k-1+\cfrac{1}{k}}}},$$

et considérons la forme quadratique $Q(X, Y) = Y(X + xY)$.

D'après le théorème 1.8, le nombre x est supérieurement et inférieurement bien approché, donc on a $\overline{Q(\mathbb{Z}^2)} = \mathbb{R}$.

(ii) Soient ℓ le nombre de Liouville $\sum_{k=1}^{+\infty} 10^{-k!}$ (voir l'exemple 1.6) et $P \in \mathcal{Q}$ défini par

$$P(X, Y) = (X + \ell Y)(X - \ell Y).$$

Le nombre ℓ est bien approché donc $u_2/u_1 = \ell$ et $v_2/v_1 = -\ell$ vérifient la condition (ii) du corollaire 2.6, ce qui entraîne $\overline{P(\mathbb{Z}^2)} = \mathbb{R}$.

Cette distinction entre petites valeurs positives ou négatives d'une forme quadratique binaire disparaît en dimension plus grande que 2. Démontrons-le pour les formes quadratiques non dégénérées et indéfinies de $\mathbb{R}^3$, ce qui servira dans [Cou].

Proposition 2.8. *Soit Q une forme quadratique non dégénérée et indéfinie sur $\mathbb{R}^3$. Si 0 est une valeur d'adhérence de l'ensemble $Q(\mathbb{Z}^3)-\{0\}$, alors cet ensemble est dense dans $\mathbb{R}$.*

Démonstration. Cette démonstration repose sur deux résultats intermédiaires.

Fait 1. *Si P est une forme quadratique binaire non dégénérée indéfinie ou définie positive, alors il existe (X,Y) dans $\mathbb{Z}^2$ tel que*

$$0 < P(X,Y) \leqslant 2\sqrt{|\det P|}.$$

Démonstration. On peut supposer $|\det P| = 1$. Il s'agit donc de montrer qu'il existe (X,Y) dans $\mathbb{Z}^2$ tel que $0 < P(X,Y) \leqslant 2$.

Soit m la borne inférieure de l'ensemble des $P(X,Y) > 0$, avec (X,Y) dans $\mathbb{Z}^2$. Si m est strictement inférieure à 2, ou encore si $m = 2$ et si cette borne est atteinte, alors cette propriété est claire.

Sinon, il existe $U = (u_1, u_2) \in \mathbb{Z}^2$, avec u_1 et u_2 premiers entre eux, vérifiant les quatre inégalités

$$P(U) > 0, \qquad \frac{P(U)}{4} + \frac{1}{P(U)} < m,$$
$$\frac{P(U)}{4} - \frac{1}{P(U)} > 0 \qquad P(U) - \frac{1}{P(U)} < m.$$

Soit $V = (v_1, v_2) \in \mathbb{Z}^2$ tel que $u_1v_2 - u_2v_1 = 1$. Le couple (U,V) est une base directe de $\mathbb{Z}^2$. Considérons M la matrice 2×2 à coefficients dans $\mathbb{Z}$ telle que $M(e_1) = U$ et $M(e_2) = V$, où (e_1, e_2) est la base canonique de $\mathbb{R}^2$. Cette matrice appartient au groupe $\mathrm{SL}_2(\mathbb{Z})$.

Posons $P' = P \circ M$. On a $P(\mathbb{Z}^2) = P'(\mathbb{Z}^2)$ et $\det P = \det P'$. Le polynôme P' s'écrit

$$P'(X,Y) = aX^2 + bY^2 + cXY,$$

avec $|ab - c^2/4| = 1$. Par définition de P', on a $a = P(U)$ donc $a \neq 0$ et l'on peut écrire

$$P'(X,Y) = a\Big(X + \frac{c}{2a}Y\Big)^2 + \frac{Y^2}{a}\Big(ba - \frac{c^2}{4}\Big).$$

Posons $\alpha = c/2a$ et $\beta = ba - c^2/4$. On a $|\beta| = 1$ et

$$P'(X,Y) = P(U)(X + \alpha Y)^2 + \beta\frac{1}{P(U)}Y^2.$$

Commençons par le cas $\beta = 1$ et considérons l'entier E tel que $0 \leqslant |E + \alpha| \leqslant 1/2$. On a

$$0 < P'(E,1) \leqslant \frac{P(U)}{4} + \frac{1}{P(U)}.$$

Donc $P'(E,1) < m$, ce qui est impossible.

Il reste le cas où $\beta = -1$. Introduisons l'entier E' tel que $1/2 \leqslant |E' + \alpha| \leqslant 1$. On a

$$\frac{P(U)}{4} - \frac{1}{P(U)} \leqslant P'(E',1) \leqslant P(U) - \frac{1}{P(U)}$$

donc $0 < P'(E',1) < m$, ce qui est impossible. □

Démontrons maintenant le second résultat.

Fait 2. *Soit Q une forme quadratique non dégénérée et indéfinie sur $\mathbb{R}^3$. Si U appartient à $\mathbb{Z}^3$ et vérifie $Q(U) > 0$, alors il existe U' dans $\mathbb{Z}^3$ tel que*

$$Q(U') < 0 \quad \textit{et} \quad Q(U')^2 \leqslant 8\sqrt{Q(U)}\sqrt{|\det Q|}.$$

Démonstration. On peut supposer que les coordonnées de $U = (u_1, u_2, u_3)$ sont premières entre elles, autrement dit qu'il existe des entiers n_1, n_2, n_3 tels que $n_1u_1 + n_2u_2 + n_3u_3 = 1$. En utilisant cette relation, on construit une matrice $M \in \mathrm{SL}_3(\mathbb{Z})$ telle que $Me_1 = U$ (voir l'exercice corrigé 1.6 de [Pau]), où (e_1, e_2, e_3) est la base canonique de $\mathbb{R}^3$. Par construction, les vecteurs $(U, M(e_2) = V, M(e_3) = W)$ forment une base directe de $\mathbb{Z}^3$.

Posons $Q' = Q \circ M$. On a $Q'(\mathbb{Z}^3) = Q(\mathbb{Z}^3)$ et $\det Q' = \det Q$. La forme Q' s'écrit

$$Q'(X,Y,Z) = a(X + \alpha Y + \beta Z)^2 - Q_0(Y,Z),$$

où $a = Q(U)$, α, β sont des réels, et Q_0 est une forme binaire non dégénérée, indéfinie ou définie positive, dont le déterminant vérifie la relation

$$-a \det Q_0 = \det Q.$$

D'après le Fait 1, il existe (Y_0, Z_0) dans $\mathbb{Z}^2$ tel que

$$0 < Q_0(Y_0, Z_0) \leqslant 2\sqrt{|\det Q_0|}.$$

En posant $c = Q_0(Y_0, Z_0)$, on obtient

$$0 < c \leqslant 2\sqrt{\frac{|\det Q|}{a}}\,.$$

Considérons la forme binaire $P(X, T) = -Q'(X, TY_0, TZ_0)$. Cette forme est non dégénérée, indéfinie et $\det P = -ac$. Toujours d'après le Fait 1, il existe (X', T') dans $\mathbb{Z}^2$ tel que

$$0 < P(X', T') \leqslant 2\sqrt{ac}.$$

Posons $U' = (X', T'Y_0, T'Z_0)$, on a

$$Q'(U') < 0 \quad \text{et} \quad 0 < Q'(U')^2 \leqslant 8\sqrt{a}\,\sqrt{|\det Q|}.$$

Par conséquent, il existe $U'' \in \mathbb{Z}^3$ tel que

$$Q(U'') < 0 \quad \text{et} \quad Q(U'')^2 \leqslant 8\sqrt{Q(U)}\,\sqrt{|\det Q|}. \qquad \square$$

À présent, montrons que si 0 est une valeur d'adhérence de l'ensemble $Q(\mathbb{Z}^3) - \{0\}$, alors cet ensemble est dense dans $\mathbb{R}$.

En utilisant le Fait 2 et en remplaçant Q par $-Q$, on obtient que s'il existe une suite $((p_k, q_k))_{k\geqslant 0}$ de couples d'entiers telle que la suite de terme général $Q(p_k, q_k)$ soit strictement positive (respectivement négative) et converge vers 0, alors il existe une suite $((p'_k, q'_k))_{k\geqslant 0}$ de couples d'entiers telle que la suite de terme général $Q(p'_k, q'_k)$ soit strictement négative (respectivement positive) et converge aussi vers 0. On conclut alors en reprenant le même raisonnement que celui utilisé pour démontrer la proposition 2.5. $\square$

La proposition que nous venons de démontrer est valable en dimension $n \geqslant 3$ (voir par exemple [BM00, Bre00]). Démontrer la conjecture d'Oppenheim pour une forme quadratique non dégénérée et indéfinie sur $\mathbb{R}^3$ revient donc à démontrer la présence de valeurs non nulles

arbitrairement petites dans l'ensemble $Q(\mathbb{Z}^3)$. Ce fait sera fortement utilisé dans [Cou].

Nous revenons à présent (et jusqu'à la fin de cette partie) aux formes binaires. Nous avons donné des exemples de formes quadratiques $Q \in \mathcal{Q}$ pour lesquelles $Q(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$. À l'opposé, nous allons montrer que ce sous-ensemble de $\mathbb{R}$ peut être discret (pour la topologie induite) et non fermé.

3. Actions de $\mathbf{SL_2}(\mathbb{Z})$ et applications aux formes quadratiques binaires

Le fil conducteur de ce paragraphe consiste à étudier la topologie de l'ensemble des valeurs prises aux points entiers par une forme quadratique binaire en utilisant des propriétés dynamiques du groupe $\mathrm{SL}_2(\mathbb{Z})$. Ce point de vue est développé dans un article de Dani-Nogueira [DN02].

Soient u et v deux vecteurs linéairement indépendants de $\mathbb{R}^2$. Nous rappelons que la forme quadratique $P_{(u,v)} \in \mathcal{Q}$ est définie pour tout $w \in \mathbb{R}^2$ par

$$P_{(u,v)}(w) = \langle u, w\rangle\langle v, w\rangle,$$

où $\langle u, w\rangle$ est le produit scalaire usuel entre u et w.

Posons $G = \mathrm{SL}_2(\mathbb{R})$ et $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. On associe à $g \in G$ et à $P_{(u,v)}$ la forme $gP_{(u,v)} \in \mathcal{Q}$ définie par

$$gP_{(u,v)} = P_{(g(u),g(v))}.$$

Remarquons que pour tout $w \in \mathbb{R}^2$, on a

$$gP_{(u,v)}(w) = P_{(u,v)}({}^t g w).$$

Si γ appartient au sous-groupe Γ, puisque ${}^t\gamma(\mathbb{Z}^2) = \mathbb{Z}^2$, on a

$$P_{(\gamma(u),\gamma(v))}(\mathbb{Z}^2) = P_{(u,v)}(\mathbb{Z}^2).$$

En particulier, s'il existe une suite $(\gamma_n)_{n\geqslant 0}$ de Γ et une forme $Q \in \mathcal{Q}$ telles que pour tout $w \in \mathbb{R}^2$

$$\lim_{n\to+\infty} P_{(\gamma_n(u),\gamma_n(v))}(w) = Q(w),$$

alors

$$Q(\mathbb{Z}^2) \subset \overline{P_{(u,v)}(\mathbb{Z}^2)}.$$

La nature topologique de l'ensemble $P_{(u,v)}(\mathbb{Z}^2)$ est donc liée à la dynamique de Γ sur $\mathcal{Q}$, ou encore, comme le montre la proposition suivante, à l'action de Γ sur le produit de la droite projective par elle-même.

Proposition 3.1. *Soit $P_{(u,v)}$ un élément de $\mathcal{Q}$. Supposons qu'il existe une suite $(\gamma_n)_{n\geqslant 0}$ dans Γ, et deux suites de réels non nuls $(a_n)_{n\geqslant 0}, (b_n)_{n\geqslant 0}$ telles que le couple de vecteurs $((\gamma_n(a_n u), \gamma_n(b_n v)))$ converge vers un couple (u', v') de vecteurs linéairement indépendants. Alors*

$$\frac{\det(u,v)}{\det(u',v')}\, P_{(u',v')}(\mathbb{Z}^2) \subset \overline{P_{(u,v)}(\mathbb{Z}^2)}.$$

Démonstration. Puisque la suite $((\gamma_n(a_n u), \gamma_n(b_n v)))_{n\geqslant 0}$ converge vers le couple (u', v'), par passage au déterminant, on obtient que la suite réelle $(a_n b_n)_{n\geqslant 0}$ converge vers $\det(u', v')/\det(u, v)$.

Soit $w \in \mathbb{Z}^2$, pour tout $n \geqslant 0$, le vecteur $w_n = {}^t\gamma_n(w)$ appartient à $\mathbb{Z}^2$. Par définition

$$P_{(\gamma_n(a_n u), \gamma_n(b_n v))}(w) = a_n b_n P_{(u,v)}(w_n).$$

Donc

$$P_{(u,v)}(w_n) = \frac{1}{a_n b_n} \langle \gamma_n(u), w\rangle \langle \gamma_n(v), w\rangle.$$

Par conséquent

$$\lim_{n\to+\infty} P_{(u,v)}(w_n) = \frac{\det(u,v)}{\det(u',v')}\, P_{(u',v')}(w).$$

Ceci entraîne

$$\frac{\det(u,v)}{\det(u',v')}\, P_{(u',v')}(\mathbb{Z}^2) \subset \overline{P_{(u,v)}(\mathbb{Z}^2)}. \qquad \square$$

Nous allons appliquer ce théorème à des situations particulières et privilégier une famille d'éléments de Γ.

Définition 3.2. Un élément de Γ, différent de l'identité et de son opposé, est dit *hyperbolique* s'il est diagonalisable sur $\mathbb{R}$.

Un tel élément γ admet deux valeurs propres réelles λ et λ^{-1} différentes de 1 et -1. Nous supposons $|\lambda| > 1$. Soient u^+ (resp. u^-)

un vecteur propre (non nul) *attractif* (resp. *répulsif*) associé à λ (resp. λ^{-1}).

Considérons le vecteur $v = u^- + u^+$ et intéressons-nous à la forme quadratique $P_{(u^-,v)}$. On a

$$\gamma^n(u^-) = \lambda^{-n}u^- \quad \text{et} \quad \gamma^n(v) = \lambda^{-n}u^- + \lambda^n u^+.$$

Donc la suite $((\lambda^n\gamma^n(u^-), \lambda^{-n}\gamma^n(v)))_{n\geqslant 0}$ converge vers (u^-, u^+).

En utilisant la proposition 3.1, et en remarquant que pour tous w tel que $\langle u^-, w\rangle \neq 0$ et $n \neq 0$, on a

$$\langle u^-, w\rangle\langle \lambda^{-2n}u^- + u^+, w\rangle \neq \langle u^-, w\rangle\langle u^- + u^+, w\rangle,$$

on obtient le résultat suivant.

Corollaire 3.3. *Soient u^- et u^+ deux vecteurs propres respectivement répulsif et attractif d'un élément hyperbolique γ de Γ. Si $v = u^- + u^+$, alors l'ensemble $P_{(u^-,v)}(\mathbb{Z}^2)$ n'est pas fermé dans $\mathbb{R}$ et on a*

$$P_{(u^-,u^+)}(\mathbb{Z}^2) \subset \overline{P_{(u^-,v)}(\mathbb{Z}^2)}. \qquad \square$$

Étudions la forme $P_{(u^-,u^+)}$. Pour cela posons

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

Les coefficients de γ sont des entiers et γ est hyperbolique, donc b n'est pas nul et les vecteurs u^- et u^+ sont de la forme

$$u^- = \alpha^-(1, \theta^-) \quad \text{et} \quad u^- = \alpha^+(1, \theta^+),$$

où α^- et α^+ sont des réels non nuls, et (en utilisant le fait que u^-, u^+ sont des vecteurs propres de γ), les réels θ^- et θ^+ sont des irrationnels quadratiques vérifiant l'équation

$$bx^2 + (a-d)x - c = 0.$$

On a $\theta^- + \theta^+ = (d-a)/b$ et $\theta^-\theta^+ = -c/b$.

Pour tout $(X, Y) \in \mathbb{R}^2$, la forme quadratique $P_{(u^-,u^+)}$ évaluée en (X, Y) s'écrit

$$P_{(u^-,u^+)}(X, Y) = \alpha^-\alpha^+(X + \theta^- Y)(X + \theta^+ Y).$$

Cette forme est donc proportionnelle à la forme quadratique

$$Q(X, Y) = bX^2 + (d-a)XY - cY^2.$$

En résumé, nous venons de démontrer la proposition suivante.

Proposition 3.4. *Soient* $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *un élément hyperbolique de* Γ *et* Q *la forme quadratique*

$$Q(X,Y) = bX^2 + (d-a)XY - cY^2.$$

Si u^-, u^+ *sont des vecteurs propres respectivement répulsif et attractif de* γ, *alors la forme quadratique* $P_{(u^-,u^+)}$ *est proportionnelle à* Q. □

Une forme quadratique qui est proportionnelle à une forme dont les coefficients sont des entiers est dite *rationnelle* (voir l'introduction). Sous les hypothèses de la proposition 3.4, la forme quadratique $P_{(u^-,u^+)}$ est rationnelle.

Proposition 3.5. *Une forme quadratique* $P_{(u,v)} \in \mathcal{Q}$ *est rationnelle si et seulement si l'une des conditions suivantes est vérifiée :*

(i) *les vecteurs* u *et* v *sont colinéaires à des vecteurs de* $\mathbb{Z}^2$;

(ii) *les vecteurs* u *et* v *sont des vecteurs propres d'un même élément hyperbolique de* Γ.

Démonstration. Si l'une des conditions (i) ou (ii) est vérifiée, alors nous avons déjà montré que $P_{(u,v)}$ est rationnel.

Supposons que $P_{(u,v)}$ soit rationnel et que la condition (i) ne soit pas satisfaite. Sous ces hypothèses, on a $u_1 \neq 0$ et $v_1 \neq 0$.

Montrons que les vecteurs u et v vérifient la condition (ii). Posons $x = u_2/u_1$ et $y = v_2/v_1$. La forme $P(X,Y) = (X + xY)(X + yY)$ est rationnelle, donc x et y sont racines d'un polynôme de degré deux à coefficients entiers. D'après la remarque 1.11, les irrationnels x et y sont fixés par une homographie non triviale $h(z) = \frac{az+b}{cz+d}$, où a, b, c, d sont des entiers et $ad - bc = 1$.

Posons $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Cet élément appartient à Γ et est différent de l'identité et de son opposé. Par ailleurs γ est diagonalisable car $(x, 1)$ et $(y, 1)$ sont deux vecteurs propres non colinéaires de γ, donc γ est hyperbolique. Par conséquent u et v sont des vecteurs propres d'un élément hyperbolique de Γ. □

Nous allons à présent nous intéresser au cas particulier où γ est la matrice hyperbolique définie par

$$\gamma = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

On rappelle que ϕ désigne le nombre d'or $\frac{1+\sqrt{5}}{2}$ et qu'il vérifie l'équation

$$X^2 - X - 1 = 0.$$

Un petit calcul montrer que les vecteurs $u^- = (1, -\phi)$ et $u^+ = (1, 1/\phi)$ sont deux vecteurs propres respectivement répulsif et attractif de γ.

Posons $v = (1, \phi)$, $\alpha^- = (1 - \phi^2)/(1 + \phi^2)$ et $\alpha^+ = 2\phi^2/(1 + \phi^2)$. On a la décomposition

$$v = \alpha^- u^- + \alpha^+ u^+.$$

Considérons la forme quadratique de *Pell-Fermat* $F_\phi \in \mathcal{Q}$ définie par

$$F_\phi = P_{(u^-, v)}.$$

On a

$$F_\phi(X, Y) = X^2 - \phi^2 Y^2.$$

Les réels ϕ^2 et ϕ sont irrationnels, donc la forme F_ϕ n'est pas rationnelle et ne représente pas 0.

D'après le corollaire 1.10, le nombre ϕ est mal approché, donc d'après le théorème 2.3, l'ensemble $\overline{F_\phi(\mathbb{Z}^2) - \{0\}}$ ne contient pas 0. Par conséquent, l'ensemble $F_\phi(\mathbb{Z}^2)$ n'est pas dense dans $\mathbb{R}$. Par ailleurs, d'après la proposition 3.3, cet ensemble n'est pas fermé. Nous allons décrire sa frontière

$$\mathcal{F} = \overline{F_\phi(\mathbb{Z}^2)} - F_\phi(\mathbb{Z}^2).$$

Proposition 3.6. *Soit Q la forme quadratique définie par*

$$Q(X, Y) = \frac{2\phi^2}{1 + \phi^2}(X^2 - XY - Y^2).$$

(i) *L'ensemble $F_\phi(\mathbb{Z}^2)$ est discret.*
(ii) $\mathcal{F} = Q(\mathbb{Z}^2) - \{0\}$.

Démonstration. Commençons par montrer deux affirmations. La première se vérifie facilement.

Fait 1. *Les formes quadratiques F_ϕ et Q sont liées par la relation*

$$(Q - F_\phi)(X, Y) = \frac{\phi^2 - 1}{\phi^2 + 1}(X - \phi Y)^2. \qquad \square$$

Fait 2. $(Q(\mathbb{Z}^2) - \{0\}) \cap F_\phi(\mathbb{Z}^2) = \varnothing$.

Pour démontrer cette affirmation, il suffit de supposer qu'il existe $(n, m) \neq (0, 0)$ dans $\mathbb{Z}^2$ et $(p, q) \in \mathbb{Z}^2$ tels que

$$n^2 - \phi^2 m^2 = \frac{2\phi^2}{1 + \phi^2}(p^2 - pq - q^2),$$

et de constater que ceci est impossible car $\frac{2\phi^2}{1+\phi^2} = \frac{1}{\sqrt{5}}$, $\phi^2 = \frac{3+\sqrt{5}}{2}$, et $\sqrt{5}$ n'est pas rationnel.

Revenons à la démonstration de la proposition.

(i) Montrons que l'ensemble $F_\phi(\mathbb{Z}^2)$ est discret (pour la topologie induite).

Soit $(F_\phi(X_n, Y_n))_{n\geqslant 0}$ une suite non stationnaire de l'ensemble $F_\phi(\mathbb{Z}^2)$ convergeant vers un réel r. On peut supposer $X_n > 0$ et $Y_n > 0$. Sous ces hypothèses, on a

$$\lim_{n\to+\infty} Y_n = +\infty \quad \text{et} \quad \lim_{n\to+\infty} X_n - \phi Y_n = 0.$$

Donc, d'après le Fait 1,

$$\lim_{n\to+\infty} Q(X_n, Y_n) = r.$$

Or $Q(\mathbb{Z}^2) \subset \frac{2\phi^2}{1+\phi^2}\,\mathbb{Z}$, donc $r \in Q(\mathbb{Z}^2)$. Le réel r n'est pas nul, donc d'après le Fait 2

$$r \notin F_\phi(\mathbb{Z}^2).$$

On déduit de ce raisonnement que chaque point de l'ensemble $F_\phi(\mathbb{Z}^2)$ est isolé et que

$$\mathcal{F} \subset Q(\mathbb{Z}^2).$$

(ii) Puisque $\alpha^- u^-$ et $\alpha^+ u^+$ sont des vecteurs propres non colinéaires de γ, dont la somme est égale à v, d'après la proposition 3.3, on a

$$P_{(\alpha^- u^-, \alpha^+ u^+)}(\mathbb{Z}^2) \subset \overline{P_{(\alpha^- u^-, v)}(\mathbb{Z}^2)}.$$

Par ailleurs

$$P_{(\alpha^- u^-, \alpha^+ u^+)}(X, Y) = \alpha^- \alpha^+ (X^2 - XY - Y^2).$$

Donc, comme $P_{(\alpha^- u^-, v)} = \alpha^- P_{(u^-, v)} = \alpha^- F_\phi$, on a

$$Q(\mathbb{Z}^2) \subset \overline{F_\phi(\mathbb{Z}^2)}.$$

Plus précisément, d'après le Fait 2, on a

$$Q(\mathbb{Z}^2) - \{0\} \subset \mathcal{F}. \qquad \square$$

L'étude de l'ensemble $F_\phi(\mathbb{Z}^2)$ se généralise aux formes quadratiques de *Pell-Fermat* $F_\theta = X^2 - \theta^2 Y^2$, où θ est un irrationnel quadratique, et θ^2 est irrationnel (voir [TV01]).

4. Formes quadratiques binaires et trajectoires du sous-groupe diagonal de $\mathbf{SL_2}(\mathbb{R})$ sur $\mathbf{SL_2}(\mathbb{R})/\mathbf{SL_2}(\mathbb{Z})$

Nous établissons ici une relation entre les formes quadratiques binaires $Q \in \mathcal{Q}$ et les orbites, encore appelées *trajectoires*, du groupe à un paramètre

$$H = \left\{ \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix} : t \in]0, +\infty[\right\},$$

(aussi noté **A** dans [Pau]) agissant par translations à gauche sur l'espace topologique quotient G/Γ, où $G = \mathrm{SL}_2(\mathbb{R})$ et $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Comme nous allons le voir, la diversité de l'adhérence des ensembles $Q(\mathbb{Z}^2)$, mise en évidence dans les paragraphes précédents, se reflète sur la topologie des orbites de H (et vice versa !), qui peuvent être denses, compactes, fermées, non fermées, non denses... (voir par exemple [Dal07]).

Topologie de $\mathrm{SL}_2(\mathbb{R})/\mathrm{SL}_2(\mathbb{Z})$ et demi-plan supérieur

Avant d'étudier ce lien, nous allons nous intéresser aux propriétés topologiques de l'espace topologique quotient G/Γ en nous appuyant sur des résultats démontrés dans un cadre plus général dans [Pau]. Nous notons π la projection canonique de G sur G/Γ. Par définition de la topologie quotient, une partie U de G/Γ est un ouvert si et seulement si $\pi^{-1}(U)$ est un ouvert de G. L'espace G/Γ est séparé donc localement compact, et π est un homéomorphisme local (voir la proposition 2.2 de [Pau]).

Proposition 4.1. *L'espace topologique quotient G/Γ n'est pas compact.*

Démonstration. Si G/Γ est compact, alors il existe $g_1, g_2, \dots g_k$ dans G et des voisinages compacts $V_1, V_2, \dots, V_k$ de ces points tels que $\pi(V_1), \pi(V_2), \dots, \pi(V_k)$ recouvrent G/Γ. Notons C la réunion finie des V_i. Cet ensemble est un compact de G qui vérifie $G = C\Gamma$. En particulier pour tout entier $n > 0$, il existe $\gamma_n \in \Gamma$ tel que

$$\begin{pmatrix} n & 0 \\ 0 & 1/n \end{pmatrix} \gamma_n \in C,$$

ce qui est impossible, car si $\gamma_n = \left(\begin{smallmatrix} a_n & b_n \\ c_n & d_n \end{smallmatrix}\right)$ avec $a_n, b_n, c_n, d_n \in \mathbb{Z}$, alors les suites $(na_n)_{n\geqslant 1}$ et $(nb_n)_{n\geqslant 1}$ sont bornées, donc il existe $N > 0$ tel que $a_n = b_n = 0$ pour tout $n > N$, ce qui contredit le fait que γ_n soit inversible. □

Introduisons le sous-groupe compact $\mathbf{K}$ de G des rotations vectorielles, défini par

$$\mathbf{K} = \left\{ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} : \theta \in \mathbb{R}/2\pi\mathbb{Z} \right\}.$$

L'espace topologique quotient $G/\mathbf{K}$ est séparé donc localement compact. Nous allons en donner une interprétation géométrique. Pour cela introduisons le demi-plan ouvert supérieur

$$\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}.$$

Si $z \in \mathbb{C}$ et si a, b, c, d sont des réels tels que $ad - bc = 1$, alors $\operatorname{Im}\left(\frac{az+b}{cz+d}\right) = (\operatorname{Im} z)/|cz + d|^2$. Donc, l'application $G \times \mathbb{H} \to \mathbb{H}$ définie

par

$$\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), z\right) \longmapsto \frac{az+b}{cz+d}$$

est bien définie. Il est facile de vérifier que c'est une action continue de G sur $\mathbb{H}$. Elle est appelée l'*action de G par homographies sur* $\mathbb{H}$.

Remarquons que le sous-groupe $\mathbf{N} = \left\{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) : t \in \mathbb{R}\right\}$ agit par translations

$$\left(\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right), z\right) \longmapsto z + t,$$

et que H agit par homothéties (de rapport strictement positif)

$$\left(\left(\begin{smallmatrix} t & 0 \\ 0 & 1/t \end{smallmatrix}\right), z\right) \longmapsto t^2 z.$$

Le noyau de cette action de G sur $\mathbb{H}$ est égal à $\{\pm \mathrm{id}\}$. Cette action induit donc une action fidèle du groupe $\mathrm{PSL}_2(\mathbb{R}) = G/\{\pm \mathrm{id}\}$ sur $\mathbb{H}$.

***Exercice 4.2* (voir** [Pau, § 2]**, *Action par homographies sur le demi-plan*)**

(i) Démontrer que l'action de $\mathrm{PSL}_2(\mathbb{R})$ sur $\mathbb{H}$ est transitive : pour tout z dans $\mathbb{H}$, il existe un élément de $\mathrm{PSL}_2(\mathbb{R})$ qui envoie i sur z.

(ii) Démontrer que le stabilisateur du point i dans $\mathrm{PSL}_2(\mathbb{R})$ est le groupe $\mathbf{K}/\{\pm \mathrm{id}\}$.

Le résultat suivant est une conséquence de l'exercice 4.2 ci-dessus, et de la proposition 2.3 de [Pau].

Proposition 4.3. *La bijection canonique $\Theta_i : G/\mathbf{K} \to \mathbb{H}$ induite par l'application de G dans $\mathbb{H}$ qui à la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ associe le nombre complexe $\frac{ai+b}{ci+d}$, est un homéomorphisme G-équivariant :*

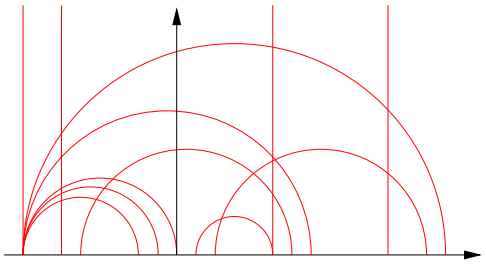
$$\forall\, g, g' \in G, \quad \Theta_i(g'g\mathbf{K}) g'(\Theta_i(g\mathbf{K})). \qquad \square$$

L'action de $\mathrm{PSL}_2(\mathbb{R})$ sur $\mathbb{H}$ s'étend continûment au compactifié d'Alexandrov du demi-plan supérieur fermé $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{R} \cup \{\infty\}$. Sa restriction à $\widehat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ est l'action projective de G sur la droite projective réelle donnée par l'application $G \times \widehat{\mathbb{R}} \to \widehat{\mathbb{R}}$ définie par

$$\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), x\right) \longmapsto \frac{ax+b}{cx+d},$$

avec la convention usuelle que $\frac{a\infty+b}{c\infty+d} = \infty$ si $c = 0$, et si $c \neq 0$, $\frac{a\infty+b}{c\infty+d} = a/c$ et $\frac{a(-d/c)+b}{c(-d/c)+d} = \infty$ (voir le paragraphe 2 de [Pau]).

L'action de $\mathrm{PSL}_2(\mathbb{R})$ sur les triplets de points distincts cycliquement ordonnés de $\widehat{\mathbb{R}}$ est simplement transitive : pour tous x, y, z dans $\widehat{\mathbb{R}}$ dans cet ordre cyclique, il existe un unique élément de $\mathrm{PSL}_2(\mathbb{R})$ qui envoie $0, 1, \infty$ sur respectivement x, y, z. En effet, par translation (qui fixe ∞), on peut envoyer tout point de $\widehat{\mathbb{R}}$ sur 0 et $z \mapsto -1/z$ échange 0 et ∞, donc $\mathrm{PSL}_2(\mathbb{R})$ agit transitivement sur les couples de points de $\widehat{\mathbb{R}}$. Les seules homographies qui fixent 0 et ∞ sont les homothéties $z \mapsto \lambda z$ avec $\lambda > 0$. Celles-ci agissent simplement transitivement sur les points de $]0, +\infty[$, ce qui montre le résultat.

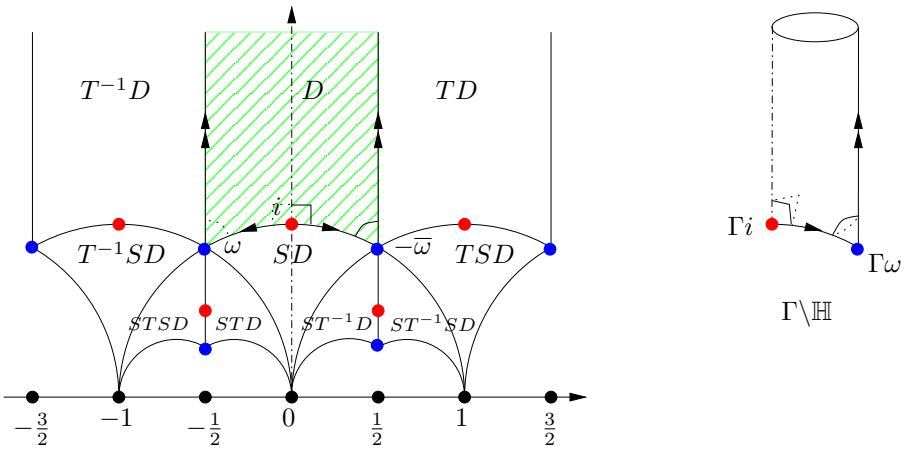


Géodésiques du demi-plan supérieur

Une *géodésique* de $\mathbb{H}$ est ou bien une demi-droite (ouverte) verticale d'origine dans $\mathbb{R}$ contenue dans $\mathbb{H}$ ou bien un demi-cercle (ouvert) euclidien contenu dans $\mathbb{H}$ et perpendiculaire à $\mathbb{R}$ en ses deux extrémités. Pour comprendre cette terminologie, il faut savoir que le demi-plan ouvert supérieur peut être muni d'une distance pour laquelle le plus court chemin joignant deux points z et z' de $\mathbb{H}$ est précisément le segment euclidien d'extrémités ces deux points s'ils ont la même partie réelle ou sinon, l'arc d'extrémités z et z' porté dans le demi-cercle perpendiculaire à $\mathbb{R}$ passant par ces deux points ([Kat92, Dal07]).

Exercice 4.4 **(voir** [Pau, § 2]**,** ***Action par homographies sur le demi-plan*****)**
Démontrer que l'action par homographies de G sur $\mathbb{H}$ préserve l'ensemble des géodésiques et qu'elle est transitive sur cet ensemble.

Intéressons-nous à présent à l'action par homographies de $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ sur $\mathbb{H}$. Pour cela, introduisons le sous-ensemble D de $\mathbb{H}$ formé



Domaine fondamental de Γ sur $\mathbb{H}$

des points z tels que $|z| \geqslant 1$ et $|\operatorname{Re} z| \leqslant 1/2$. Dans [Pau], on démontrera que cet ensemble est un *domaine fondamental* pour l'action de Γ sur $\mathbb{H}$, *i.e.* D est l'adhérence de son intérieur, $\mathbb{H} = \bigcup_{\gamma\in\Gamma} \gamma D$ (c'est-à-dire que $\mathbb{H}$ est la réunion des images de D par les éléments de Γ), et ces images sont d'intérieurs deux à deux disjoints (modulo $\{\pm \mathrm{id}\}$). Donnons dans la proposition 4.5 l'énoncé précis des propriétés de l'action de Γ sur $\mathbb{H}$, qui seront démontrées dans [Pau] (proposition 2.4).

Proposition 4.5. (1) *Pour tout z dans $\mathbb{H}$, il existe $g \in \Gamma$ tel que $gz \in D$.*

(2) *Si deux points distincts z, z' de D sont dans la même orbite par Γ, alors ou bien $\operatorname{Re} z = \pm 1/2$, $|z| > 1$ et $z = z' \pm 1$, ou bien $|z| = 1$ et $z' = -1/z$.*

(3) *Posons $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $\omega = e^{2i\pi/3}$.*

Si $z \in D$, alors le stabilisateur Γ_z de z dans Γ est $\{\pm \mathrm{id}\}$, sauf si $z = i$ où $\Gamma_z = \{\pm \mathrm{id}, \pm S\}$, $z = \omega$ où $\Gamma_z = \{\pm \mathrm{id}, \pm ST, \pm (ST)^2 = \pm (ST)^{-1}\}$ et $z = -\overline{\omega}$ où $\Gamma_z = \{\pm \mathrm{id}, \pm TS, \pm (TS)^2 = \pm (TS)^{-1}\}$.

(4) *Le groupe Γ est engendré par S et T.* □

Remarque 4.6. L'action de Γ sur $\widehat{\mathbb{R}}$ est transitive sur $\mathbb{Q} \cup \{\infty\}$.

Démonstration. Si p/q est un élément de $\mathbb{Q}$ avec p, q des entiers premiers entre eux, alors par le théorème de Bézout, il existe des entiers r, s tels que $ps - qr = 1$, et donc l'élément $g_{p,q} = \left(\begin{smallmatrix} p & r \\ q & s \end{smallmatrix}\right)$ de G envoie ∞ sur p/q. □

L'espace topologique quotient $\Gamma\backslash\mathbb{H}$ est appelé la *surface modulaire*. On peut la « visualiser » à partir du domaine D. Pour cela, considérons la relation d'équivalence $\mathcal{R}$ sur D définie par $z \mathcal{R} z'$ si et seulement s'il existe $\gamma \in \Gamma$ tel que $z' = \gamma z$.

L'application de l'espace topologique quotient $D/\mathcal{R}$ sur $\Gamma\backslash\mathbb{H}$, qui à la classe de z modulo $\mathcal{R}$ associe sa classe modulo Γ, est un homéomorphisme (voir par exemple [Kat92, Dal07]). Donc $\Gamma\backslash\mathbb{H}$ est homéomorphe à l'espace obtenu en identifiant les deux côtés verticaux de D par la translation T, et les arcs de cercles d'extrémités respectives ω, i d'une part, et $-\overline{\omega}$, i d'autre part, par la transformation S. Cette surface est homéomorphe à une sphère privée d'un point (correspondant au point $\infty \in \overline{\mathbb{H}}$), en particulier elle n'est pas compacte.

Les espaces topologiques quotients $\Gamma\backslash G/\mathbf{K}$ et $\Gamma\backslash\mathbb{H}$ sont homéomorphes. En effet, l'homéomorphisme G-équivariant Θ_i de $G/\mathbf{K}$ dans $\mathbb{H}$, qui à gK associe gi, induit, par passage au quotient par Γ, un homéomorphisme Φ entre $\Gamma\backslash G/\mathbf{K}$ et $\Gamma\backslash\mathbb{H}$ défini par

$$\Phi(\Gamma g\mathbf{K}) = \Gamma\Theta_i(g\mathbf{K}).$$

Cet homéomorphisme Φ nous permet de caractériser géométriquement les sous-ensembles non bornés de G/Γ.

Proposition 4.7. *Soient A une partie de G et A^{-1} l'ensemble des inverses de A. Les assertions suivantes sont équivalentes :*

(i) *L'ensemble $A\Gamma \subset G/\Gamma$ n' est pas borné.*

(ii) *L'ensemble $\Phi(\Gamma A^{-1}\mathbf{K}) \subset \Gamma\backslash\mathbb{H}$ n'est pas borné.*

(iii) *Il existe une suite $(a_n)_{n\geqslant 0}$ de A et une suite $(\gamma_n)_{n\geqslant 0}$ de Γ telles que les points $z_n\Theta_i(\gamma_n {a_n}^{-1}\mathbf{K})$ vérifient $\lim_{n\to+\infty} \operatorname{Im} z_n = +\infty$.*

Démonstration. L'équivalence entre (i) et (ii) repose sur le fait que l'application de G dans G qui à g associe g^{-1} induit un homéomorphisme entre les espaces $\Gamma\backslash G$ et G/Γ, et que $\mathbf{K}$ est compact (voir le lemme 2.1 de [Pau]).

L'équivalence entre (ii) et (iii) se démontre en utilisant l'application Φ, la proposition 4.5 démontrée dans [Pau], et le fait que l'injection canonique de D dans $\mathbb{H}$ est propre. □

Après cette introduction géométrique, revenons aux formes quadratiques binaires.

Formes quadratiques binaires et trajectoires non bornées

Posons $e_1 = (1, 0)$, $e_2 = (0, 1)$ et $Q_0 = P_{(e_1,e_2)}$. On a

$$Q_0(X, Y) = XY.$$

Le groupe diagonal H, introduit au début de ce paragraphe, est la composante connexe de l'identité dans le groupe orthogonal $O(Q_0)$ de Q_0, défini par

$$O(Q_0) = \{g \in G : \forall\, w \in \mathbb{R}^2,\ Q_0(gw) = Q_0(w)\}.$$

Nous notons $\mathcal{Q}^1$ l'ensemble des éléments $P_{(u,v)}$ de $\mathcal{Q}$ tels que $\det(u, v) = 1$. Pour tout $P_{(u,v)} \in \mathcal{Q}^1$, il existe un unique $g' \in G$ tel que

$${}^t g'(e_1) = u \quad \text{et} \quad {}^t g'(e_2) = v.$$

On a donc, pour tout $w \in \mathbb{R}^2$,

$$P_{(u,v)}(w) = Q_0(g'w).$$

Grâce à cette relation, on peut relier l'ensemble $P_{(u,v)}(\mathbb{Z}^2)$ à l'orbite de $g'\Gamma \in G/\Gamma$ sous l'action par translations à gauche du groupe H sur G/Γ.

Théorème 4.8. *Soient $x < y$ deux irrationnels. Notons P la forme quadratique $P(X, Y) = (X + xY)(X + yY)$, et $g \in G$ la matrice définie par*

$$g = \frac{1}{\sqrt{y - x}} \begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}.$$

Les propriétés suivantes sont équivalentes.

(i) *Le sous-ensemble $Hg\Gamma$ de G/Γ n'est pas borné.*
(ii) *Le réel 0 appartient à l'ensemble $\overline{P(\mathbb{Z}^2) - \{0\}}$.*
(iii) *Le réel x ou y est bien approché.*

De plus, si l'une de ces conditions est vérifiée, alors il existe une suite non bornée $(h_n)_{n\geqslant 0}$ dans H pour laquelle la suite $(h_n g\Gamma)_{n\geqslant 0}$ converge dans G/Γ.

Démonstration. L'équivalence entre les propriétés (ii) et (iii) a été déjà démontrée (voir le théorème 2.3).

Remarquons que pour tout $w \in \mathbb{R}^2$ on a

$$P(w) = (y-x)Q_0(gw).$$

Démontrons que (i) entraîne (ii). Supposons que la partie $Hg\Gamma$ de G/Γ ne soit pas bornée. D'après la proposition 4.7, il existe des suites $(h_n)_{n\geqslant 0}$ dans H et $(\gamma_n)_{n\geqslant 0}$ dans Γ telles que les points $z_n = \Theta_i(\gamma_n(h_n g)^{-1}\mathbf{K})$ vérifient $\lim_{n\to+\infty} \operatorname{Im} z_n = +\infty$. Posons

$$\gamma_n(h_n g)^{-1} = \begin{pmatrix} A_n & B_n \\ C_n & D_n \end{pmatrix}.$$

On a $\operatorname{Im} z_n = 1/(C_n^2 + D_n^2)$, donc $\lim_{n\to+\infty} C_n = \lim_{n\to+\infty} D_n = 0$. Par ailleurs, $h_n g {\gamma_n}^{-1}$ est une matrice de la forme

$$\begin{pmatrix} t_n(a_n + xc_n) & t_n(b_n + xd_n) \\ \frac{1}{t_n}(a_n + yc_n) & \frac{1}{t_n}(b_n + yc_n) \end{pmatrix},$$

où a_n, b_n, c_n, d_n sont des entiers vérifiant $a_n d_n - b_n c_n = 1$, et t_n est un réel strictement positif. On a

$$D_n = t_n(a_n + xc_n) \quad \text{et} \quad -C_n = \frac{1}{t_n}(a_n + yc_n),$$

donc

$$\lim_{n\to+\infty} t_n(a_n + xc_n) = \lim_{n\to+\infty} \frac{1}{t_n}(a_n + yc_n) = 0.$$

Par ailleurs D_n et C_n ne sont pas nuls donc $(P(a_n, c_n))_{n\geqslant 0}$ est une suite de $P(\mathbb{Z}^2) - \{0\}$ qui converge vers 0, ce qui démontre (ii).

Démontrons que (iii) entraîne (i). Supposons par exemple que x soit bien approché. D'après la proposition 4.7, démontrer (i) revient à démontrer que $\Phi(\Gamma g^{-1} H)$ n'est pas borné dans $\Gamma\backslash\mathbb{H}$. Posons $g' = g^{-1}$. On a

$$g' = \frac{1}{\sqrt{y-x}} \begin{pmatrix} y & -x \\ -1 & 1 \end{pmatrix}.$$

Raisonnons sur le demi-plan ouvert $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. L'ensemble $\Theta_i(g'H\mathbf{K})$ est l'image par g' du demi-axe imaginaire $\Theta_i(H\mathbf{K})$, c'est donc le demi-cercle dont le diamètre est le segment d'extrémités $g'(\infty) = -y$ et $g'(0) = -x$. Soit γ un élément de Γ tel que $x' = \gamma(-x) > 0$ et $y' = \gamma(-y) < 0$ (l'existence d'un tel élément est garantie par le Fait 1 démontré au cours de la démonstration de la proposition 1.9). Le réel x' est également bien approché (voir la remarque 1.7). Donc, d'après le théorème 1.8, son développement en fractions continues $(n_i)_{i\geqslant 0}$ n'est pas borné. Introduisons la translation $T(z) = z+1$ et l'homographie $F(z) = z/(1+z)$. On a $F^n(z) = \frac{1}{n+1/z}$, donc

$$x' = \lim_{k\to+\infty} T^{n_0}F^{n_1}T^{n_2}\cdots T^{n_{2k}}F^{n_{2k+1}}(x'_{2k+2}),$$

où x'_{2k+2} est un irrationnel strictement supérieur à 1. Soit $(n_{k_p})_{p\geqslant 0}$ une suite extraite strictement croissante. On peut supposer que les k_p sont tous pairs ou tous impairs.

Dans le premier cas, posons

$$\gamma_p = T^{n_0}F^{n_1}T^{n_2}\cdots T^{n_{k_p-2}}F^{n_{k_p-1}}.$$

Par construction, ${\gamma_p}^{-1}(x') > n_{k_p}$, donc

$$\lim_{p\to+\infty} {\gamma_p}^{-1}(x') = +\infty.$$

Pour $p \geqslant 2$, les coefficients de γ_p sont des entiers naturels strictement positifs et le déterminant de γ_p est égal à 1, donc la matrice associée à γ_p, que nous notons encore γ_p, appartient au groupe Γ.

Le réel y' est strictement négatif et les coefficients de γ_p sont strictement positifs donc ${\gamma_p}^{-1}(y')$ est un réel négatif. Par conséquent, l'ensemble $\Theta_i({\gamma_p}^{-1}\gamma g'H\mathbf{K})$ est un demi-cercle. Puisque l'une de ses extrémités est négative et l'autre est positive et tend vers $+\infty$, pour p grand, ce demi-cercle rencontre le domaine fondamental D de Γ (introduit avant la proposition 4.5) en des points z_p qui vérifient

$$\lim_{p\to+\infty} \operatorname{Im} z_p = +\infty. \tag{4.1}$$

D'après la proposition 4.7, l'ensemble $Hg\Gamma$ n'est pas borné dans G/Γ.

Si l'on suppose que les k_p sont tous impairs, on pose alors

$$\gamma_p = T^{n_0}F^{n_1}T^{n_2}\cdots T^{n_{k_p-1}}S,$$

avec $S(z) = -1/z$. Cet élément appartient à Γ. Par construction, ${\gamma_p}^{-1}(x')$ est un irrationnel négatif strictement inférieur à $-n_{k_p}$, donc

$$\lim_{p\to+\infty} {\gamma_p}^{-1}(x') = -\infty.$$

Pour tout p, le réel ${\gamma_p}^{-1}(y')$ est strictement positif, donc l'ensemble $\Theta_i({\gamma_p}^{-1}\gamma g' H\mathbf{K})$ est un demi-cercle qui, pour p grand, rencontre le domaine D en des points z_p qui vérifient également la condition (4.1).

Montrons à présent que sous l'hypothèse (iii), il existe une suite non bornée $(h_n)_{n\geqslant 0} \subset H$ telle que $(h_n g\Gamma)_{n\geqslant 0}$ converge dans G/Γ. Pour cela il suffit de revenir à la démonstration précédente. En effet, nous avons mis en évidence une suite de demi-cercles de la forme $\gamma_n g^{-1} H(i)$, où $(\gamma_n)_{n\geqslant 0}$ est une suite non bornée de Γ, qui rencontre le domaine D en des points z_n vérifiant $\lim_{n\to+\infty} \operatorname{Im} z_n = +\infty$. Pour n assez grand, chaque demi-cercle contient nécessairement un point z'_n tel que $\operatorname{Im} z'_n = 1$.

Pour chaque z'_n, il existe un entier p_n tel que $T^{p_n}(z'_n) \in D$. Donc la suite $(T^{p_n}(z'_n))_{n\geqslant N}$ est incluse dans un compact de $\mathbb{H}$. Soit $h_n \in H$ tel que $z'_n = \gamma_n g^{-1} h_n(i)$, cette suite n'est pas bornée et la suite $(\Gamma g^{-1} h_n)_{n\geqslant N}$ est incluse dans un compact de $\Gamma\backslash\mathbb{H}$, donc quitte à extraire une sous-suite, $(h_n^{-1} g\Gamma)_{n\geqslant N}$ converge dans G/Γ. □

Nous allons maintenant donner une caractérisation arithmétique des sous-ensembles fermés de la forme $Hg\Gamma \subset G/\Gamma$, en commençant par ceux qui sont compacts.

Formes quadratiques binaires et trajectoires compactes

Proposition 4.9. *Soit $g \in G$. Les assertions suivantes sont équivalentes.*

(i) *Il existe $h \in H$ différent de l'identité, tel que $g^{-1}hg \in \Gamma$.*
(ii) *Le sous-ensemble $Hg\Gamma \subset G/\Gamma$ est compact.*

Démonstration. Supposons (i). Il existe donc $h \in H - \{\mathrm{id}\}$ et $\gamma \in \Gamma$ tels que $g^{-1}hg = \gamma$. Cette hypothèse entraîne l'égalité suivante sur G/Γ

$$hg\Gamma = g\Gamma.$$

Posons

$$h = \begin{pmatrix} t_0 & 0 \\ 0 & 1/t_0 \end{pmatrix}.$$

Quitte à remplacer h par h^{-1}, on peut supposer $t_0 > 1$. Soit C le compact de H défini par

$$C = \Big\{ \begin{pmatrix} t & 0 \\ 0 & 1/t \end{pmatrix} : 1 \leqslant t \leqslant t_0 \Big\}.$$

Pour tout $h' \in H$, il existe $k \in C$ et $n \in \mathbb{Z}$, tels que $h' = kh^n$. Donc

$$Hg\Gamma = Cg\Gamma.$$

L'application π_g de H dans G/Γ qui à h' associe $h'g\Gamma$ étant continue, l'ensemble $Cg\Gamma$ est compact.

Réciproquement si l'ensemble $Hg\Gamma$ est compact, alors l'application π_g n'est pas injective. Il existe donc $h \in H$ différent de l'identité tel que $hg\Gamma = g\Gamma$. Par conséquent, il existe $\gamma \in \Gamma$ tel que $g^{-1}hg = \gamma$. □

Grâce à cette proposition, on obtient le lien suivant entre les ensembles compacts $Hg\Gamma \subset G/\Gamma$ et les formes quadratiques binaires.

Corollaire 4.10. *Soient $x < y$ deux irrationnels. Notons P la forme quadratique définie par $P(X,Y) = (X + xY)(X + yY)$ et $g \in G$ la matrice définie par*

$$g = \frac{1}{\sqrt{y-x}} \begin{pmatrix} 1 & x \\ 1 & y \end{pmatrix}.$$

Les propriétés suivantes sont équivalentes.

(i) *Le sous-ensemble $Hg\Gamma \subset G/\Gamma$ est compact.*

(ii) *Les irrationnels x et y sont solutions d'un même polynôme de degré 2 à coefficients entiers.*

(iii) *La forme quadratique P est rationnelle.*

Démonstration. L'équivalence entre (ii) et (iii) est claire.

L'implication (i) entraîne (ii) est une conséquence de la proposition 4.9. En effet, si le sous-ensemble $Hg\Gamma$ est compact, alors il existe $h \in H$ tel que $g^{-1}hg \in \Gamma$. Donc il existe $t > 0$ tel que les réels $yt - x/t$, $txy - xy/t$, $-t + 1/t$ et $-tx + y/t$ soient des entiers. Ceci entraîne que les réels xy et $x + y$ sont des rationnels, et donc que la condition (ii) est satisfaite.

Il reste à démontrer (ii) entraîne (i). Pour cela considérons la matrice g^{-1}. On a

$$g^{-1} = \frac{1}{\sqrt{y-x}} \begin{pmatrix} y & -x \\ -1 & 1 \end{pmatrix}.$$

Posons, $U = (y, -1)$ et $V = (-x, 1)$. Par hypothèse, les réels $-y$ et $-x$ sont solutions d'un polynôme de degré 2 à coefficients entiers. D'après la remarque 1.11, il existe une homographie différente de l'identité $h'(z) = \frac{nz+p}{mz+q}$, où n, m, p, q sont des entiers vérifiant $nq - mp = 1$, les fixant. Autrement dit, il existe $\gamma \in \Gamma$ différent de l'identité, et $\lambda \neq 0$ tels que $\gamma(U) = \lambda U$ et $\gamma(V) = \frac{1}{\lambda}V$. Par conséquent $g\gamma g^{-1}(e_1) = \lambda e_1$ et $g\gamma g^{-1}(e_2)\frac{1}{\lambda}e_2$. Il existe donc $h \in H$ différent de l'identité tel que $g\gamma g^{-1} = h$, ce qui montre, d'après la proposition 4.9, que l'ensemble $Hg\Gamma$ est compact. □

Formes quadratiques binaires et trajectoires fermées non bornées

Intéressons-nous maintenant aux sous-ensembles fermés non bornés de la forme $Hg\Gamma \subset G/\Gamma$.

Proposition 4.11. *Soit $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$. Les assertions suivantes sont équivalentes.*

(i) *Les vecteurs (a, b) et (c, d) sont colinéaires à des vecteurs de $\mathbb{Q}^2$.*
(ii) *Le sous-ensemble $Hg\Gamma$ est fermé et non borné dans G/Γ.*

Démonstration. Démontrons que (i) entraîne (ii). Supposons que les vecteurs (a, b) et (c, d) soient colinéaires à des vecteurs de $\mathbb{Q}^2$ et écrivons g sous la forme $g = h_0 g_0$, où h_0 est une matrice diagonale et g_0 est à coefficients entiers. En utilisant cette écriture et le fait qu'une suite d'entiers convergeant vers 0 est stationnaire, on montre que le sous-ensemble $Hg\Gamma$ est fermé dans G. Par ailleurs il est invariant à droite par Γ, donc sa projection sur l'espace G/Γ est fermée. Posons $g' = g^{-1}$. Pour montrer que $Hg\Gamma$ n'est pas borné, nous allons montrer, en nous appuyant sur la proposition 4.7, que l'ensemble $\Theta_i(\Gamma g' H\mathbf{K})$ n'est pas borné dans le quotient $\Gamma\backslash\mathbb{H}$. Par hypothèse, l'ensemble $\Theta_i(g' H\mathbf{K})$ est une demi-droite ou un demi-cercle dont les extrémités sont rationnelles.

Dans le premier cas, il existe une translation entière $T^m(z)=z+m$ telle que l'ensemble $\Theta_i(T^m g' H\mathbf{K})$ soit une demi-droite verticale rencontrant le domaine fondamental D de Γ en une demi-droite. Ceci entraîne, par la proposition 4.7, que l'ensemble $Hg\Gamma$ n'est pas borné dans G/Γ.

Le deuxième cas se ramène au premier en utilisant la remarque 4.6.

Démontrons (ii) entraîne (i). Supposons que l'ensemble $Hg\Gamma$ soit fermé et non borné dans G/Γ. Considérons l'action à droite de Γ sur le quotient $H\backslash G$, qui est un espace localement compact car H est fermé (voir le paragraphe 2 de [Pau]). L'ensemble $Hg\Gamma$ est fermé dans $H\backslash G$, car il est fermé dans G (par définition de la topologie quotient) et est invariant à droite par H.

Si (a,b) et (c,d) ne sont pas colinéaires à des vecteurs de $\mathbb{Q}^2$, alors d'après le théorème 4.8, dont l'hypothèse est vérifiée car $Hg\Gamma$ n'est pas borné, il existe une suite non stationnaire $(Hg\gamma_n)_{n\geqslant 0}$ qui converge vers Hg dans $H\backslash G$. Chaque voisinage de Hg dans l'espace topologique $Hg\Gamma$ rencontre donc la suite $(Hg\gamma_n)_{n\geqslant 0}$, ce qui montre que $\{Hg\}$ est un fermé d'intérieur vide de l'espace topologique $Hg\Gamma$. Par ailleurs, pour tout $\gamma\in\Gamma$, la suite $(Hg\gamma_n\gamma)_{n\geqslant 0}$ converge vers $Hg\gamma$, donc cet espace est une union dénombrable de fermés d'intérieur vide. Ceci est impossible car par le théorème de Baire, son intérieur serait vide.

Sinon, supposons par exemple que (c,d) appartienne à $\mathbb{Q}^2$. Posons $g'=g^{-1}$. Quitte à remplacer g' par $\gamma g'$, avec $\gamma\in\Gamma$, on peut supposer que g' est de la forme

$$g'=\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

avec $b'd'>0$. En effet, si $c=0$, il suffit de prendre un entier $n>b/a$ et de poser

$$\gamma=\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Sinon, introduisons des entiers p,q,u,v tels que $-d/c=p/q$ et $pu+qv=1$ et posons

$$\gamma_1=\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \quad \text{et} \quad \gamma_2=\begin{pmatrix} u & v \\ -q & p \end{pmatrix}.$$

Pour un entier $n > 0$ suffisamment grand, l'élément $\gamma = \gamma_1\gamma_2$ convient.

Intéressons-nous à présent à la géodésique $\Theta_i(g'H\mathbf{K})$. Par hypothèse, c'est une demi-droite verticale de $\mathbb{H}$ d'extrémité $x = b'/d' > 0$. Supposons que x soit un irrationnel. Considérons la suite d'homographies $(g_k)_{k\geqslant 0}$ intervenant dans son développement en fractions continues. On a $g_k^{-1}(x) = x_{k+1} > 1$ et $g_k^{-1}(\infty) < 0$, donc la droite horizontale d'équation $\operatorname{Im} z = 1/2$ dans $\mathbb{H}$ est rencontrée par tous les demi-cercles $\Theta_i(g_k^{-1}g'H\mathbf{K})$. Notons z_k un point d'intersection de ces deux courbes et $h_k \in H$ tel que $\Theta_i(g_k^{-1}g'h_k\mathbf{K}) = z_k$. Remarquons que la suite $(h_k)_{k\geqslant 0}$ n'est pas bornée, car les g_k^{-1} sont des éléments tous différents de Γ et $\operatorname{Im} z_k = 1/2$. Il existe une suite d'entiers naturels p_k telle que la suite $(T^{p_k}(z_k))_{k\geqslant 2}$ soit bornée. La sous-suite impaire extraite de $(T^{p_k}g_k^{-1}g'h_k)_{k\geqslant 0}$ appartient à G, car $\det g_k = (-1)^{k-1}$. On a $g_k^{-1}g'h_k(i) = z_k$. Posons $T^{p_k}g_k^{-1}g'h_k(i) = (a_ki + b_k)/(c_ki + d_k)$, avec $a_kd_k - b_kc_k = 1$. Quitte à extraire une sous-suite, on peut supposer que la sous-suite impaire extraite de $\big((a_ki + b_k)/(c_ki + d_k)\big)_{k\geqslant 0}$ converge vers un point de $\mathbb{H}$, ce qui entraîne que les sous-suites impaires extraites de $(a_k)_{k\geqslant 0}$, $(b_k)_{k\geqslant 0}$, $(c_k)_{k\geqslant 0}$ et $(d_k)_{k\geqslant 0}$ convergent. Autrement dit, on peut supposer que la sous-suite impaire extraite de $(T^{p_k}g_k^{-1}g'h_k)_{k\geqslant 0}$ converge dans G, et donc, par passage à l'inverse, que celle extraite de $(h_k^{-1}gg_kT^{-p_k})_{k\geqslant 0}$ converge aussi. On obtient ainsi une sous-suite non stationnaire de la suite $(Hgg_kT^{-p_k})_{k\geqslant 0}$, qui est incluse dans $H\backslash G$ et qui converge vers un élément de $Hg\Gamma$, puisque cet ensemble est fermé. On en déduit que, pour tout $\gamma \in \Gamma$, le singleton $\{Hg\gamma\}$ est un fermé d'intérieur vide dans l'ensemble $Hg\Gamma \subset H\backslash G$ muni de la topologie induite. Par le théorème de Baire, l'intérieur de cet ensemble est vide, ce qui est impossible.

En conclusion, les vecteurs (a, b) et (c, d) appartiennent à $\mathbb{Q}^2$. □

On déduit de ces résultats et de la proposition 3.4 les équivalences suivantes

Corollaire 4.12. *Soient $P \in \mathcal{Q}^1$ et $g \in G$ tels que $P = Q_0 \circ g$. Les assertions suivantes sont équivalentes.*

(i) *Le sous-espace $Hg\Gamma \subset G/\Gamma$ est fermé.*

(ii) *La forme P est rationnelle.*

De plus, $Hg\Gamma$ est compact si et seulement si la forme P est rationnelle et ne représente pas 0.

Démonstration. Posons

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

On a $P(X,Y) = (aX + bY)(cX + dY)$.

Si a (ou c) est nul, alors P est rationnel si et seulement si d/c (ou b/a) est rationnel et donc, d'après la proposition 4.11, si et seulement si $Hg\Gamma$ est fermé et non borné. Supposons que a et c ne soient pas nuls.

Montrons que (ii) entraîne (i). Posons

$$Q(X,Y) = (X + (b/a)Y)(X + (d/c)Y).$$

On a $P(X,Y) = acQ(X,Y)$. Si P est rationnel, alors Q l'est aussi et donc, d'après la proposition 3.5, ou bien les réels b/a et d/c sont rationnels, ou bien $u = (a,b)$ et $v = (c,d)$ sont des vecteurs propres d'un même élément hyperbolique γ de Γ. Dans le premier cas, on obtient, en utilisant la proposition 4.11, que l'ensemble $Hg\Gamma$ est fermé et non borné. Dans le second cas, on a ${}^tg^{-1}\gamma {}^tg \in H$. Donc $g^{-1}hg \in \Gamma$, ce qui, d'après la proposition 4.9, entraîne que le sous-ensemble $Hg\Gamma \subset G/\Gamma$ est compact.

Montrons que (i) entraîne (ii). Supposons que $Hg\Gamma$ soit fermé. Si cet ensemble n'est pas borné, d'après la proposition 4.11, $u = (a,b)$ et $v = (c,d)$ sont colinéaires à des vecteurs de $\mathbb{Q}^2$, donc P est rationnel. Sinon, d'après la proposition 4.9, il existe $h \in H$ non trivial tel que $g^{-1}hg$ appartienne à Γ. Cette propriété entraîne que le vecteur $(ac, ad+bc, bd) \in \mathbb{R}^3$ est colinéaire à un vecteur de $\mathbb{Q}^3$, et donc que P est rationnel. □

Formes quadratiques binaires et trajectoires denses

À l'opposé des sous-ensembles fermés $Hg\Gamma \subset G/\Gamma$ se trouvent les sous-ensembles denses. De tels sous-ensembles peuvent être construits en utilisant la théorie des approximations diophantiennes (voir

[Dal07, DN02]). On peut en effet montrer que si y est un irrationnel positif et si g est la matrice définie par

$$g = \frac{1}{\sqrt{y}} \begin{pmatrix} 1 & 0 \\ 1 & y \end{pmatrix},$$

alors $Hg\Gamma$ est dense dans G/Γ si et seulement si toute suite finie de $\mathbb{N}$ est une sous-suite du développement en fractions continues de y ([DN02, Cor. 4.5] ou [Dal07, Ch. II & IV]).

Remarquons que s'il existe une suite $(h_n)_{n\geqslant 0}$ de H et une suite $(\gamma_n)_{n\geqslant 0}$ dans Γ telles que $(h_n g \gamma_n)_{n\geqslant 0}$ converge vers $g' \in G$, alors pour tout $w \in \mathbb{R}^2$,

$$\lim_{n\to+\infty} Q_0(g\gamma_n(w)) = Q_0(g'w).$$

Donc

$$Q_0(g'\mathbb{Z}^2) \subset \overline{Q_0(g\mathbb{Z}^2)}.$$

Par conséquent, on peut énoncer la proposition suivante.

Proposition 4.13. *Soient $P \in \mathcal{Q}^1$ et $g \in G$ tels que $P = Q_0 \circ g$. Si l'ensemble $Hg\Gamma$ est dense dans G/Γ, alors*

$$\overline{P(\mathbb{Z}^2)} = \mathbb{R}. \qquad \square$$

La réciproque de la proposition ci-dessus est fausse. Il suffit par exemple de considérer le réel y dont le développement en fractions continues est la suite $(n_i)_{i\geqslant 0}$ définie par $n_i = 2^i$ et la matrice

$$g = \frac{1}{\sqrt{y}} \begin{pmatrix} 1 & 0 \\ 1 & y \end{pmatrix}.$$

D'après [DN02, Cor. 4.5] ou [Dal07, Ch. II & IV], l'ensemble $Hg\Gamma$ n'est pas dense dans G/Γ. Considérons maintenant la forme quadratique $P = Q_0 \circ g$, qui s'écrit encore $P(X, Y) = \frac{X}{y}(X + yY)$. Le réel y étant supérieurement et inférieurement bien approché, d'après le corollaire 2.6, on a $\overline{P(\mathbb{Z}^2)} = \mathbb{R}$.

Formes quadratiques binaires et trajectoires bornées non fermées

Avant de terminer ce texte, nous allons étudier un cas intermédiaire d'orbite sous H, c'est-à-dire un sous-ensemble $Hg\Gamma$ borné et

non fermé dans G/Γ, en nous appuyant sur l'étude de la forme quadratique

$$F_\phi(X,Y) = X^2 - \phi^2 Y^2,$$

avec $\phi = (1+\sqrt{5})/2$, faite dans le paragraphe précédent.

Proposition 4.14. *Soit g la matrice de G définie par*

$$g = \frac{1}{\sqrt{2\phi}} \begin{pmatrix} 1 & -\phi \\ 1 & \phi \end{pmatrix}.$$

L'ensemble $Hg\Gamma$ n'est pas fermé et est borné dans G/Γ. De plus $\overline{Hg\Gamma} - Hg\Gamma$ est la réunion d'un nombre fini d'orbites compactes.

Démonstration. La matrice g et la forme F_ϕ sont liées par la relation

$$F_\phi(w) = 2\phi Q_0(gw),$$

pour tout $w \in \mathbb{R}^2$.

Le fait que l'ensemble $Hg\Gamma \subset G/\Gamma$ ne soit pas fermé et soit borné est une conséquence directe du corollaire 4.12, car F_ϕ n'est pas rationnel, et du théorème 4.8, car ϕ est un réel mal approché.

Intéressons-nous à l'adhérence de $Hg\Gamma$. Soit $g' \in \overline{Hg\Gamma} - Hg\Gamma$, il existe une suite $(h_n)_{n\geqslant 0}$ non bornée dans H et $(\gamma_n)_{n\geqslant 0}$ dans Γ telles que $\lim_{n\to+\infty} h_n g \gamma_n = g'$. Pour tout $w \in \mathbb{R}^2$, on a donc $\lim_{n\to+\infty} Q_0(h_n g \gamma_n(w)) = Q_0(g'(w))$, ce qui entraîne l'inclusion

$$2\phi Q_0(g'(\mathbb{Z}^2)) \subset \overline{F_\phi(\mathbb{Z}^2)}.$$

Rappelons que, d'après la proposition 3.6, l'ensemble $F_\phi(\mathbb{Z}^2)$ est discret (pour la topologie induite) et que

$$\overline{F_\phi(\mathbb{Z}^2)} - F_\phi(\mathbb{Z}^2) = Q(\mathbb{Z}^2) - \{0\},$$

où Q désigne la forme quadratique rationnelle définie par

$$Q(X,Y) = \frac{2\phi^2}{1+\phi^2}(X^2 - XY - Y^2).$$

Soit $w \in \mathbb{Z}^2$. Posons $w_n = \gamma_n(w)$. La suite $(F_\phi(w_n))_{n\geqslant 0}$ converge vers $2\phi Q_0(g'(w))$. Montrons que cette limite appartient à l'ensemble $Q(\mathbb{Z}^2)$. Si ce n'est pas le cas, puisque $F_\phi(\mathbb{Z}^2)$ est un ensemble discret, cette suite est stationnaire à partir d'un certain rang, autrement dit, si l'on pose $w_n = (x_n, y_n)$, alors la quantité ${x_n}^2 - \phi^2 {y_n}^2$ est constante

à partir d'un rang N. Puisque ϕ^2 est un irrationnel, quitte à extraire une sous-suite, on peut supposer que la suite $(w_n)_{n\geqslant 0}$ est constante et donc que l'on a $h_n g(w_n) = h_n g(w_0)$, ce qui est impossible car la suite $(h_n g(w_0))_{n\geqslant 0}$ converge, et la suite $(h_n)_{n\geqslant 0}$ n'est pas bornée. Par conséquent, on a l'inclusion

$$2\phi Q_0(g'\mathbb{Z}^2)) \subset Q(\mathbb{Z}^2).$$

Or

$$Q(X,Y) = \frac{2\phi^2}{1+\phi^2}(X^2 - XY - Y^2),$$

ce qui montre que la forme quadratique $Q_0 \circ g'$ est rationnelle. En appliquant le corollaire 4.12, on obtient que le sous-ensemble $Hg'\Gamma \subset G/\Gamma$ est fermé. Par ailleurs cet ensemble est borné, car il est inclus dans $\overline{Hg\Gamma}$, donc $Hg'\Gamma$ est compact.

En conclusion, si $Hg'\Gamma$ est inclus dans $\overline{Hg\Gamma}$, alors ou bien $Hg'\Gamma = Hg\Gamma$, ou bien $Hg'\Gamma$ est compact dans G/Γ.

Montrons à présent que l'ensemble $\overline{Hg\Gamma} \subset G/\Gamma$ ne contient qu'un nombre fini d'orbites compactes sous l'action de H. Nous allons nous appuyer sur deux résultats intermédiaires.

Plaçons-nous dans le demi-plan ouvert supérieur $\mathbb{H}$ et considérons l'action de Γ par homographies. On rappelle (voir la proposition 4.5), que le sous-ensemble D de $\mathbb{H}$ formé des points z tels que $|z| \geqslant 1$ et $|\operatorname{Re} z| \leqslant 1/2$ est un domaine fondamental pour cette action et que les homographies $T(z) = z+1$ et $S(z) = 1/-z$ engendrent Γ.

Fait 1. *Soit C un demi-cercle inclus dans $\mathbb{H}$, centré en un réel. Si l'une des extrémités de C est irrationnelle, alors il existe un élément γ de Γ, tel que le demi-cercle γC rencontre le domaine D et le domaine $S(D)$.*

Démonstration. Quitte à remplacer C par γC, avec $\gamma \in \Gamma$, on peut supposer que C rencontre l'intérieur de D. Soient z un point appartenant à l'intérieur de D et à C, et x une extrémité irrationnelle de C. Le point ∞ est l'intersection de l'adhérence du domaine D dans $\overline{\mathbb{H}} = \mathbb{H} \cup \widehat{\mathbb{R}}$ et de $\widehat{\mathbb{R}}$. Par ailleurs, l'image de ce point par le groupe Γ est égal à $\mathbb{Q} \cup \{\infty\}$, donc, puisque x est irrationnel, l'arc C' d'origine z, d'extrémité x et porté par C, est recouvert par une infinité de domaines successifs de la forme $D, a_1 D, a_1 a_2 D, a_1 a_2 a_3 D, \ldots,$

avec $a_i \in \{T, T^{-1}, S\}$ et ${a_i}^{-1} \neq a_{i+1}$. Puisque C' n'est pas une demi-droite horizontale, l'un des a_i est égal à S. Posons $g_i = \mathrm{id}$ si $i = 1$, et $g_i = a_1 \cdots a_{i-1}$ si $i > 1$. Le demi-cercle ${g_i}^{-1}C$ rencontre D et $S(D)$. □

Fait 2. *Il existe un sous-ensemble fini $F \subset \mathbb{R}^+$ tel que si $Hg'\Gamma$ est un compact inclus dans $\overline{Hg\Gamma}$ et si le demi-cercle ${g'}^{-1}H(i)$, d'extrémités $x = {g'}^{-1}(0)$ et $y = {g'}^{-1}(\infty)$, rencontre D, alors $|x - y|$ appartient à F.*

Démonstration. Puisque $\overline{Hg\Gamma}$ est un compact de G/Γ, l'ensemble $\overline{\Gamma g^{-1}H(i)}$ est un compact de $\Gamma\backslash\mathbb{H}$. Donc d'après la proposition 4.7, il existe $A > 0$ tel que pour tout γ dans Γ, le demi-cercle $\gamma g^{-1}H(i)$ soit inclus dans l'ensemble $\{z \in \mathbb{C} : 0 < \operatorname{Im} z < A\}$. Remarquons que les extrémités du demi-cercle $\gamma g^{-1}H(i)$ sont $\gamma(-\phi)$ et $\gamma(\phi)$. Donc il existe $A' > 0$ tel que si γ est dans Γ, alors $0 < |\gamma(-\phi) - \gamma(\phi)| \leqslant A'$.

Soit $Hg'\Gamma$ une orbite compacte incluse dans $\overline{Hg\Gamma}$. On suppose que le demi-cercle ${g'}^{-1}H(i)$, d'extrémités $x = {g'}^{-1}(0)$ et $y = {g'}^{-1}(\infty)$, rencontre D. Ces extrémités sont les limites de suites de la forme $(\gamma_n(-\phi))_{n\geqslant 0}$ et $(\gamma_n(\phi))_{n\geqslant 0}$, donc

$$|x - y| \leqslant A'.$$

Par ailleurs, il existe $B > 0$ tel que si x' et y' sont les extrémités d'un demi-cercle centré en un réel rencontrant D, alors $B \leqslant |x' - y'|$. Puisque ${g'}^{-1}H(i)$ rencontre D, on a

$$B \leqslant |x - y|.$$

Par hypothèse, il existe des suites $(\gamma_n)_{n\geqslant 0}$ dans Γ et $(h_n)_{n\geqslant 0}$, non bornée, dans H telles que $(\gamma_n g^{-1} h_n)_{n\geqslant 0}$ converge vers g'.

Posons

$$\gamma_n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix},$$

où a_n, b_n, c_n, d_n sont des entiers vérifiant $a_n d_n - c_n b_n = 1$. On a

$$(\gamma_n(\phi) - \gamma_n(-\phi))^2 = \frac{1}{(-c_n\phi + d_n)^2} \frac{1}{(c_n\phi + d_n)^2} (2\phi)^2.$$

Donc

$$(\gamma_n(\phi) - \gamma_n(-\phi))^2 \frac{1}{(F_\phi(d_n, c_n))^2}(2\phi)^2.$$

La suite $(F_\phi(d_n, c_n))_{n\geqslant 0}$ n'est pas stationnaire, car $(h_n)_{n\geqslant 0}$ n'est pas bornée. Donc il existe des entiers N et M tels que

$$(x-y)^2 = \frac{1}{(Q(N,M))^2}(2\phi)^2.$$

L'ensemble $Q(\mathbb{Z}^2)$ est inclus dans un ensemble de la forme $\lambda\mathbb{Z}$ et $B \leqslant |x-y| \leqslant A'$, donc il existe $E > 0$ et $E' > 0$ tels que pour tout g' satisfaisant les conditions du Fait 2, le réel $|x-y|^2$ appartienne à l'ensemble fini $\{r > 0 : r \in (2\phi)^2/Q(\mathbb{Z}^2) \text{ et } E' < r < E\}$. □

Démontrons à présent que $\overline{Hg\Gamma} \subset G/\Gamma$ ne contient qu'un nombre fini d'ensembles compacts de la forme $Hg'\Gamma$.

Soit $Hg'\Gamma$ un tel ensemble. Les extrémités $x = g'^{-1}(0)$ et $y = g'^{-1}(\infty)$ du demi-cercle $g'^{-1}H(i)$ sont irrationnelles. En effet, $Hg'\Gamma$ étant une orbite compacte, il existe $\gamma \in \Gamma$, non trivial, et $h \in H$ tels que $hg' = g'\gamma$, ce qui entraîne que x et y sont fixés par l'homographie associée à γ, donc que x et y sont des irrationnels (quadratiques). D'après le Fait 1, quitte à remplacer g' par $g'\gamma'$, avec $\gamma' \in \Gamma$, on peut supposer que $g'^{-1}H(i)$ rencontre les domaines D et $S(D)$. En appliquant le Fait 2 à g' et à $g'S$, on obtient que les réels $|x-y|$ et $|\frac{-1}{x} - \frac{-1}{y}|$ appartiennent à F. Par conséquent il existe un sous-ensemble fini $F' \subset \mathbb{R}^+$, indépendant de g', tel que $|x-y|$ et $|xy|$ appartiennent à F'. Ceci montre que l'ensemble des points $g'^{-1}(0)$ et $g'^{-1}(\infty)$ est fini. On conclut en remarquant que si deux éléments g' et g'' de G vérifient $g'^{-1}(0) = g''^{-1}(0)$ et $g'^{-1}(\infty)g''^{-1}(\infty)$, alors il existe $h \in H$ tel que $g'' = hg'$. □

Une étude plus poussée, s'appuyant sur le développement en fractions continues de ϕ et de $-\phi$, et sur la dynamique de l'application de décalage sur des suites bilatères (voir [Dal07, Chap. II & IV]), permet de montrer que $\overline{Hg\Gamma}$ contient exactement deux ensembles compacts, $Hg_2\Gamma$ et $Hg_1\Gamma$, dont voici la description.

Introduisons les matrices suivantes de G.

$$\gamma_1 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},\ g_1 = \sqrt{\frac{1}{10\phi}} \begin{pmatrix} \frac{1}{\phi} + \phi & -2 - \phi \\ 2\phi & 2 \end{pmatrix} \text{ et } h_1 = \begin{pmatrix} \frac{1}{1+\phi} & 0 \\ 0 & 1 + \phi \end{pmatrix}.$$

La matrice γ_1 appartient à Γ et elle est hyperbolique. Remarquons que les matrices h_1, γ_1 et g_1 sont liées par une relation de conjugaison

$$g_1{}^{-1} h_1 g_1 = \gamma_1,$$

donc d'après la proposition 4.9, l'ensemble $Hg_1\Gamma$ est compact.

Par ailleurs, un simple calcul conduit à l'égalité suivante

$$h_1{}^{-n} g \gamma_1{}^n = \lambda_n{}^{-1} \begin{pmatrix} \frac{1}{\phi} + \phi & -2 - \phi \\ 2\phi - \frac{1}{t^{2n}} & 2 + \frac{\phi}{t^{2n}} \end{pmatrix},$$

où $t = 1 + \phi$ et $\lambda_n = \det \begin{pmatrix} \frac{1}{\phi} + \phi & -2 - \phi \\ 2\phi - \frac{1}{t^{2n}} & 2 + \frac{\phi}{t^{2n}} \end{pmatrix}$.

Donc $\lim_{n\to+\infty} h_1{}^{-n} g \gamma_1{}^n = g_1$, ce qui montre que $Hg_1\Gamma$ est inclus dans $\overline{Hg\Gamma}$.

En suivant la même démarche mais en remplaçant γ_1, g_1, h_1 respectivement par

$$\gamma_2 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},\ g_2 = \frac{1}{\sqrt{10\phi}} \begin{pmatrix} 2\phi & -2 \\ \frac{1}{\phi} + \phi & 1 + \phi^2 \end{pmatrix} \text{ et } h_2 = \begin{pmatrix} \frac{1}{-\phi+2} & 0 \\ 0 & -\phi + 2 \end{pmatrix},$$

on obtient que l'ensemble $Hg_2\Gamma$ est compact et est inclus dans $\overline{Hg\Gamma}$.

Comme nous le verrons dans [Cou], en dimension $n \geqslant 3$, il existe également un lien entre l'adhérence des ensembles $Q(\mathbb{Z}^n)$, où Q est une forme quadratique sur $\mathbb{R}^n$, et celle des orbites d'un sous-groupe de $\mathrm{SL}_n(\mathbb{R})$, qui sera encore noté H. Contrairement au cas $n = 2$, ce groupe n'est plus diagonal et est engendré par des matrices dites *unipotentes* dont les valeurs propres sont réelles et toutes égales à 1. Depuis les années 1970, l'étude des adhérences des orbites d'un tel groupe dans l'espace des réseaux $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$ a fait l'objet de nombreux travaux, tous motivés par la conjecture de Raghunathan (voir l'introduction générale). Dans les années 1990, M. Ratner a donné une caractérisation de ces adhérences (voir [Rat95]). Cette propriété de régularité des orbites de H qui, comme nous l'avons vu, est

loin d'être vérifiée en dimension $n = 2$, joue un rôle essentiel dans la démonstration de la conjecture d'Oppenheim.

Références

[BM00] M. B. Bekka & M. Mayer – *Ergodic theory and topological dynamics of group actions on homogeneous spaces*, London Math. Soc. Lect. Note Series, vol. 269, Cambridge University Press, Cambridge, 2000.

[Bre00] E. Breuillard – « La conjecture d'Oppenheim et sa version quantitative », Mémoire de DEA, Université Paris VI, 2000, `http://www.math.polytechnique.fr/~breuilla/Opp4.ps`.

[Cou] G. Courtois – « Sur les valeurs aux entiers des formes quadratiques réelles », in *Systèmes dynamiques, groupes de matrices et applications arithmétiques*, Journées X-UPS, Les Éditions de l'École polytechnique, Palaiseau, 2007, ce volume.

[Dal07] F. Dal'Bo – *Trajectoires géodésiques et horocycliques*, Savoirs Actuels, CNRS Éditions & EDP Sciences, Paris, 2007.

[DN02] S. G. Dani & A. Nogueira – « On orbits of $\mathrm{SL}(2,\mathbb{Z})_+$ and values of binary quadratic forms on positive integral pairs », *J. Number Theory* **95** (2002), no. 2, p. 313–328.

[HW79] G. H. Hardy & E. M. Wright – *An introduction to the theory of numbers*, 5e éd., The Clarendon Press Oxford University Press, New York, 1979, Trad. française : Vuibert, Paris, 2007.

[Ita63] J. Itard – *Arithmétique et théorie des nombres*, Que sais-je ?, vol. 1093, Presses Universitaires de France, Paris, 1963.

[Kat92] S. Katok – *Fuchsian groups*, Chicago Lectures in Math., University of Chicago Press, Chicago, IL, 1992.

[Khi97] A. Y. Khinchin – *Continued fractions*, Dover Publications Inc., Mineola, NY, 1997.

[Pau] F. Paulin – « De la géométrie et de la dynamique de $\mathrm{SL}_n\mathbb{R}$ et $\mathrm{SL}_n\mathbb{Z}$ », in *Systèmes dynamiques, groupes de matrices et applications arithmétiques*, Journées X-UPS, Les Éditions de l'École polytechnique, Palaiseau, 2007, ce volume.

[Rat95] M. Ratner – « Interactions between ergodic theory, Lie groups, and number theory », in *Proceedings of the International Congress of Mathematicians, (Zürich, 1994)*, Birkhäuser, Basel, 1995, p. 157–182.

[TV01] G. Troessaert & A. Valette – « On values at integer points of some irrational, binary quadratic forms », in *Essays on geometry and related topics*, Monogr. Enseign. Math., vol. 38, Enseignement Math., Genève, 2001, p. 597–610.

Françoise Dal'Bo, Institut de Recherche Mathématique de Rennes, UMR 6625 CNRS, Campus de Beaulieu, Université Rennes 1, 35042 Rennes Cedex, France
E-mail : `francoise.dalbo@univ-rennes1.fr`