J.M.E. *de l'ENS de Lyon*
Vol. III, Octobre 2017
p. 3-14

Les spectres de Markov et de Lagrange

Nicolas Rocher

Résumé. *Dans cet article, on étudie deux ensembles de constantes et leurs structures intimement liées. Les premières constantes interviennent dans l'étude des valeurs minimales prises par certaines formes quadratiques sur le réseau $\mathbb{Z}^2$. Les secondes apparaissent dans l'approximation diophantienne des nombres irrationnels. Les résultats présentés nécessiteraient davantage qu'un court article dans le Journal de Maths des Élèves pour être démontrés complètement et en toute rigueur. C'est pourquoi, au lieu de proposer une longue démonstration technique, j'ai préféré construire cet article plutôt sous la forme d'une promenade à la rencontre des différentes notions mises en jeu. Toutes les références nécessaires à une compréhension plus fine des résultats seront données au lecteur souhaitant aller plus loin.*

1. Markov et les formes quadratiques

1.1. **Généralités sur le problème des minima des formes quadratiques.** Trouver les valeurs minimales (en un sens à préciser) prises par une forme quadratique réelle est un problème qui remonte au XIX$^{\text{e}}$ siècle. Plus précisément, étant donnée une forme quadratique $f : \mathbb{R}^n \longrightarrow \mathbb{R}$, on cherche à étudier la quantité

$$\inf\left\{|f(x_1,\dots,x_n)|,\ (x_1,\dots,x_n) \in \mathbb{Z}^n - \{(0,\dots,0)\}\right\}.$$

Ici, on se limitera au problème en dimension 2. On se donne donc à partir de maintenant une forme quadratique $f : (x,y) \mapsto \alpha x^2 + \beta xy + \gamma y^2$ ($\alpha,\beta,\gamma \in \mathbb{R}$) et on note $\mu(f) = \inf\left\{|f(x,y)|,\ (x,y) \in \mathbb{Z}^2 - \{(0,0)\}\right\}$. On appellera **discriminant** de f la quantité $\Delta(f) = \beta^2 - 4\alpha\gamma$.

On peut dès maintenant distinguer deux types de telles formes quadratiques pour lesquels la situation est bien différente.

Définition 1.1. Si $\Delta(f) \leq 0$, f est dite **définie**. Dans le cas contraire $\Delta(f) > 0$, f est dite **indéfinie**.

Cette terminologie est justifiée par la remarque suivante : si $\alpha \neq 0$, on peut écrire $f(x,y)$ sous sa forme canonique

$$f(x,y) = \alpha\left(x + \frac{\beta}{2\alpha}y\right)^2 - \frac{\Delta(f)}{4\alpha}y^2.$$

Si f est définie, alors $f(x,y)$ a toujours le signe de α, tandis que si elle est indéfinie, son signe est … indéfini ! L'étude de $\mu(f)$ dans le cas où f est définie est la plus facile, et a été réalisée en premier par Hermite. Toutefois, on ne s'y attardera pas, et désormais f sera supposée indéfinie. Le lecteur néanmoins intéressé pourra consulter [3]. On peut quand même noter que les deux cas exploitent la même idée de départ, qui consiste comme souvent, à introduire une relation d'équivalence naturelle qui ramène le problème à l'étude et la classification de certaines formes "normales". Ici on introduit une relation

nicolas.rocher@ens-lyon.fr

d'équivalence entre les formes quadratiques qui laissera invariantes les quantités au centre du problème.

Définition 1.2. On dit que f et g sont équivalentes, et on note $f \sim g$, s'il existe $a, b, c, d \in \mathbb{Z}$ avec $ad - bc = \pm 1$ tels que

$$\forall x, y \in \mathbb{R},\ f(ax + by, cx + dy) = g(x, y).$$

On voit que $\sim$ est bien une relation d'équivalence : c'est la relation d'équivalence sous l'action du groupe formé des matrices de déterminant ± 1 de $GL_2(\mathbb{Z})$ en posant

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f = (x, y) \mapsto f(ax + by, cx + dy).$$

En outre, si $f \sim g$, avec les mêmes notations que dans cette définition, l'application linéaire $\mathbb{R}^2 \longrightarrow \mathbb{R}^2$ représentée par la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ a pour déterminant ± 1, donc préserve le réseau $\mathbb{Z}^2$ et est inversible. Il s'ensuit que f et g y prennent les mêmes valeurs : en particulier, on a $\mu(f) = \mu(g)$. Un calcul élémentaire permet également de se convaincre que $\Delta(f) = \Delta(g)$.

Cette relation d'équivalence semble donc pertinente vis-à-vis de la remarque faite plus haut, en laissant invariante la quantité suivante :

Définition 1.3. La **constante de Markov** de f est la quantité $M(f) = \frac{\mu(f)}{\sqrt{\Delta(f)}}$. L'ensemble $M = \{M(f), f \text{ forme quadratique indéfinie}\}$ est appelé **spectre de Markov**.

FIGURE 1. A. Markov

On remarque que si $\lambda > 0$, $\mu(\lambda f) = \lambda \mu(f)$ et $\Delta(\lambda f) = \lambda^2 \Delta(f)$, et donc que $M(\lambda f) = M(f)$. Ainsi, pour l'étude du spectre de Markov, on peut se limiter aux formes quadratiques telles que $\mu(f) = 1$, ce que l'on fera par la suite.

Les travaux de Markov [1] aboutissent à une description complète d'un morceau de ce spectre. Voyons dans les grandes lignes comment il a procédé.

1.2. **L'équation de Markov.** Markov a introduit l'équation diophantienne suivante, qui porte son nom :

$$x^2 + y^2 + z^2 = 3xyz,\ (x, y, z) \in (\mathbb{N}^*)^3.$$

Un peu de vocabulaire :

— Un triplet $(x, y, z) \in (\mathbb{N}^*)^3$ solution est appelé **triplet de Markov**.

— Un entier $x \in \mathbb{N}^*$ est appelé **nombre de Markov** s'il fait partie d'un triplet de Markov.

1. Il s'agit du mathématicien russe Andreï Andreïevitch Markov (1856 - 1922), célèbre probabiliste à l'origine des processus qui portent son nom, à ne pas confondre avec son fils (du même nom !), Andreï Andreïevitch Markov (1903-1979), logicien à l'origine de l'École constructiviste soviétique.

— Un triplet de Markov (x, y, z) est dit **non singulier** si x, y et z sont 2 à 2 distincts, et **singulier** sinon. Par exemple, $(1, 1, 1)$ est un triplet singulier, tandis que $(1, 2, 5)$ est non singulier.

Avant d'établir le lien entre cette équation et le problème initial, nous souhaitons décrire complètement l'ensemble de ses solutions et se familiariser avec quelques propriétés. Commençons par décrire les triplets singuliers :

Proposition 1.1. *Les seuls triplets de Markov singuliers sont* $(1, 1, 1)$ *et* $(1, 1, 2)$.

Démonstration. Soit (x, y, z) un tel triplet. Sans perte de généralité on peut supposer que $y = x$, quitte à échanger l'ordre des éléments, l'équation étant symétrique.

Si $x = z$, on a

$$3x^2 = 3x^3,$$

c'est-à-dire $x = 0$ ou $x = 1$. Comme $x \in \mathbb{N}^*$, $x = 1$ et on vérifie que $(1, 1, 1)$ est bien un triplet de Markov.

Si $x \neq z$, on a

$$2x^2 + z^2 = 3x^2 z.$$

On en déduit que $z^2 = 0 \pmod{x^2}$ et donc que $z = 0 \pmod{x}$, puis l'existence de $m \in \mathbb{N}^*$ tel que $z = mx$. L'équation de Markov devient

$$2x^2 + m^2x^2 = 3mx^3 \Leftrightarrow m(3x - m) = 2.$$

Par suite, m divise 2, i.e $m = 1$ ou $m = 2$. Or $m = 1$ est exclu car $x \neq z$ d'où $m = 2$ i.e. $z = 2x$. L'équation de Markov devient

$$6x^2 = 6x^3 \Leftrightarrow x = 1 \text{ ou } x = 0.$$

Comme précédemment $x \neq 0$ donc $(x, y, z) = (1, 1, 2)$ qui est bien un triplet de Markov. □

Voyons maintenant qu'à partir d'un triplet de Markov (x, y, z), on peut en fabriquer des nouveaux. En effet, on connaît déjà une racine du polynôme $X^2 - 3yzX + y^2 + z^2$ (d'indéterminée X), à savoir x. L'autre, notée x', est, sur la droite réelle, symétrique de x par rapport à $3yz/2$, c'est-à-dire

$$x' = \frac{3yz}{2} + \left(\frac{3yz}{2} - x\right) = 3yz - x.$$

On a donc un nouveau triplet de Markov : $(x', y, z) = (3yz - x, y, z)$. Si au départ on avait $x \leq y \leq z$ ou $y \leq x \leq z$ (cas (1)), alors on peut vérifier facilement que $x' > x$, et si l'on avait $x > y$ et $x > z$ (cas (2)), alors $x' < x$. Ainsi, en appliquant cette méthode en démarrant du triplet $(1, 1, 1)$, on construit une infinité de solutions à l'équation de Markov, qui peuvent être représentées sous la forme d'un arbre binaire appelé **arbre de Markov**. Le procédé appliqué dans le cas (1) permet de "monter" dans une branche supérieure, tandis que le cas (2) permet de "descendre" dans une branche inférieure.

Proposition 1.2. *Chaque triplet de Markov apparaît une unique fois dans l'arbre binaire ci-dessus*

Démonstration. On remarque d'abord que les deux triplets singuliers sont bien présents dans l'arbre et de manière unique car, par construction, tout triplet formé par l'algorithme ci-dessus à partir d'un triplet non singulier est non singulier, et donc en particulier tous les éléments de l'arbre sont non singuliers à partir de $(1, 2, 5)$.

Soit (x, y, z) un triplet de Markov non singulier, avec $x < y < z$. En adaptant la méthode décrite ci-dessus pour construire l'arbre binaire, mais en considérant le polynôme d'indéterminée Z (i.e. cas (2)), on construit un nouveau triplet $(x, y, 3xy - z)$ tel que $\max\{x, y, 3xy - z\} < z$. En répétant cette opération tant que les triplets obtenus sont non singuliers, on construit par récurrence une suite de triplets non singuliers dont la suite des maximums est strictement décroissante. L'algorithme s'arrête lorsque l'on obtient un triplet non singulier (x', y', z') avec $x' < y' < z'$, tel que $(x', y', 3x'y' - z')$ soit singulier,

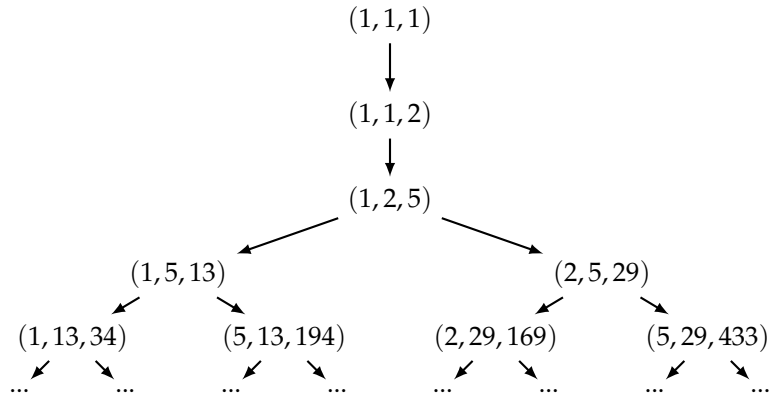

FIGURE 2. Les premiers niveaux de l'arbre de Markov

c'est-à-dire lorsque au moins deux entiers parmi $\{x', y', 3x'y' - z'\}$ sont égaux à 1. Ce sont forcément x' et $3x'y' - z'$. Par suite,

$$3y' - z' = 1 \Rightarrow z' = 3y' - 1,$$

d'où

$$\begin{aligned} 1^2 + y'^2 + (3y' - 1)^2 &= 3y'(3y' - 1) \\ \Leftrightarrow y'^2 - 3y' + 2 &= 0 \\ \Rightarrow y' &= 2. \end{aligned}$$

Ainsi, $(x', y', z') = (1, 2, 5)$. On conclut avec le procédé inverse, en "remontant" dans l'arbre depuis $(1, 2, 5)$ (et il y a une unique manière de le faire) jusqu'au triplet initial (x, y, z) qui apparaît donc une unique fois dans l'arbre. □

Une dernier résultat qui sera utile dans la suite établit des relations de divisibilité entre les éléments d'un triplet de Markov.

Proposition 1.3. *Les entiers x, y et z d'un triplet de Markov sont deux à deux premiers entre eux.*

Démonstration. Soit d un diviseur commun (positif) de y et z. Il existe donc $k, l \in \mathbb{Z}$ tels que $y = kd$ et $z = ld$. Il vient

$$x^2 = 3xyz - y^2 - z^2 = 3xkld^2 - k^2d^2 - l^2d^2 = (3xkl - k^2 - l^2)d^2.$$

Ainsi d^2 divise x^2 et donc d divise x. En particulier, d divise aussi $3xy - z$, $3xz - y$ et $3yz - x$ i.e. d est un diviseur commun des triplets voisins de (x, y, z) dans l'arbre de Markov. En remontant ainsi de proche en proche, d est un diviseur commun du triplet racine $(1, 1, 1)$ c'est-à-dire $d = 1$. Ainsi $\text{pgcd}(y, z) = 1$. En échangeant leurs rôles dans la démonstration ci-dessus, on conclut que x, y et z sont deux à deux premiers entre eux. □

1.3. **Les formes de Markov.** On a maintenant les outils pour construire, à partir d'un nombre de Markov m, une forme quadratique indéfinie f_m, dite **forme de Markov associée à** m.

Soit m_2, m_3 deux autres entiers tels que (m, m_2, m_3) soit un triplet de Markov. D'après la proposition précédente, m_2 et m sont premiers entre eux donc m_2 est un générateur de $\mathbb{Z}/m\mathbb{Z}$. Il existe donc un entier $u \in \{0, \dots, m-1\}$ tel que $um_2 = m_3 \pmod m$. En outre, comme $m^2 + m_2^2 + m_3^2 = 3mm_2m_3$, on a $m_2^2 + m_3^2 = 0 \pmod m$. Ainsi $u^2m_2^2 = m_3^2 = -m_2^2 \pmod m$. Alors m divise $(u^2 + 1)m_2^2$, puis comme m et m_2 sont premiers entre eux, par deux applications consécutives du lemme de Gauss, on obtient que m divise $u^2 + 1$.

Donc $u^2 = -1 \pmod{m}$ et il existe alors un entier $v \in \{0, \dots, m-1\}$ tel que $u^2 + 1 = mv$. On définit la forme f_m comme suit :

Définition 1.4 (Forme de Markov associée à m)**.** Avec les notations ci-dessus

$$f_m(x, y) = mx^2 + (3m - 2u)xy + (v - 3u)y^2, \ \forall x, y \in \mathbb{R}.$$

On peut facilement calculer le discriminant de f_m. En effet, on a

$$\begin{aligned}\Delta(f_m) &= (3m - 2u)^2 - 4m(v - 3u) \\ &= 9m^2 - 12mu + 4u^2 - 4mv + 12mu \\ &= 9m^2 - 4(mv - u^2) \\ &= 9m^2 - 4.\end{aligned}$$

Calculer $\mu(f_m)$ est plus compliqué. On laisse le lecteur intéressé consulter [3] et se convaincre que $\mu(f_m) = m$. En combinant ces deux résultats, on obtient $M(f_m) = m/\sqrt{9m^2 - 4}$.

1.4. **Lien avec le problème initial.** Les formes de Markov introduites ci-dessus, comme on va le voir, représentent toute une gamme de formes quadratiques indéfinies. Plus précisément, Markov démontre le théorème suivant :

Théorème 1.1 (Markov)**.** *Soit $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ une forme quadratique indéfinie vérifiant les hypothèses $\Delta(f) < 9$ et $\mu(f) = 1$. Alors f est équivalente à une certaine forme de Markov f_m.*

Ce théorème est clairement le point technique et difficile du travail de Markov, et c'est pourquoi nous l'admettrons. Plusieurs démonstrations en ont été données dans [2] et [5], et l'on encourage le lecteur intéressé à les consulter. Ce théorème permet, comme promis, de décrire tout un morceau du spectre de Markov. On procède de la manière suivante.

Soit $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ une forme quadratique indéfinie vérifiant $M(f) > 1/3$ et toujours telle que $\mu(f) = 1$. Dans ce cas, $M(f) = 1/\sqrt{\Delta(f)}$. Comme $M(f) > 1/3$, on en déduit que $\Delta(g) < 9$. On peut donc appliquer le théorème ci-dessus : il existe un nombre de Markov m tel $f \sim f_m$. En particulier on en déduit que $M(f) = M(f_m)$. Par les calculs effectués plus haut, on sait en outre que $M(f_m) = m/\sqrt{9m^2 - 4}$. Comme on l'a vu, se restreindre à $\mu(f) = 1$ n'est qu'un choix de commodité, et le raisonnement ci-dessus s'étend à $\mu(f) > 0$ quelconque, puisque $\mu(\lambda f) = \mu(f)$ pour $\lambda > 0$. On vient d'obtenir le théorème suivant :

Théorème 1.2 (Spectre de Markov au-dessus de $1/3$)**.** *Le spectre de Markov est entièrement connu au-dessus de la valeur $1/3$:*

$$M \cap]1/3, +\infty[= \left\{ \frac{m}{\sqrt{9m^2 - 4}}, \ m \text{ nombre de Markov} \right\}.$$

2. L'approximation diophantienne

La densité de $\mathbb{Q}$ dans $\mathbb{R}$ nous informe que l'on peut approcher un réel par des rationnels avec une précision illimitée. Cependant, on veut en outre pouvoir mesurer la "qualité" d'une telle approximation, et obtenir la meilleure possible. C'est tout l'enjeu de l'approximation diophantienne. Le but de cette deuxième partie est d'introduire quelques notions de cette branche de la théorie des nombres et d'utiliser les résultats obtenus dans la première partie pour décrire des constantes qui interviennent dans l'approximation de certains irrationnels.

2.1. **Ordre d'approximation, premiers résultats et constantes de meilleure approximation.** Afin de formaliser la notion de "qualité" d'approximation, on introduit une première définition.

Définition 2.1. Soient $\alpha \in \mathbb{R}$ et $s > 0$. On dit que α est approchable à l'ordre s s'il existe une infinité de rationnels $\frac{p}{q}$ ($p \in \mathbb{Z}, q \in \mathbb{N}^*$) et de constantes $A > 0$ tels que :

$$\left|\alpha - \frac{p}{q}\right| < \frac{A}{q^s}.$$

Moralement, on demande que le dénominateur ne devienne pas trop grand, et une bonne approximation cherchera à la fois à maximiser l'ordre s, et minimiser la constante A.

Si α est lui-même rationnel, (i.e. $\alpha = \frac{a}{b}, a \in \mathbb{Z}, b \in \mathbb{N}^*$), il est approchable au mieux à l'ordre 1 : en effet, pour tout $\frac{p}{q} \in \mathbb{Q}$ tel que $\frac{p}{q} \neq \frac{a}{b}$, on a

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}.$$

Les rationnels sont donc "mal approchables" par des rationnels, et par la suite, on considérera uniquement le cas où α est irrationnel.

Le premier résultat important en approximation diophantienne est le suivant, démontré par Dirichlet.

Théorème 2.1 (Dirichlet)**.** *Tout irrationnel α est approchable à l'ordre* 2*.*

Démonstration. Soit $N \in \mathbb{N}^*$. Considérons une subdivision de $[0,1[$ en N intervalles de même longueur $1/N$, i.e.

$$[0,1[= \left[0, \frac{1}{N}\right[\cup \left[\frac{1}{N}, \frac{2}{N}\right[\cup \ldots \cup \left[\frac{N-1}{N}, 1\right[.$$

D'après le principe des tiroirs[2] appliqué à la famille $(k\alpha - [k\alpha])_{0 \leq k \leq N}$ où $[\ ]$ désigne la partie entière, il existe deux entiers $l, k \in [\![0, N]\!]$ avec $l < k$ tels que

$$|(k\alpha - [k\alpha]) - (l\alpha - [l\alpha])| < \frac{1}{N}.$$

En posant $q = k - l \in]\!]0, N]\!]$ et $p = [k\alpha] - [l\alpha] \in \mathbb{Z}$, il vient

$$|q\alpha - p| < \frac{1}{N} \Rightarrow \left|\alpha - \frac{p}{q}\right| < \frac{1}{Nq}.$$

Comme $q \leq N$, on a $\frac{1}{N} \leq \frac{1}{q}$, et finalement

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

□

L'ordre 2 est-il toutefois optimal ? Cette question a demandé plus de travail. Un théorème de Liouville apporte un premier élément de réponse pour le cas des irrationnels algébriques[3] : il affirme qu'un tel irrationnel de degré d est approchable au maximum à l'ordre d. La démonstration de ce théorème est simple et repose sur l'inégalité des accroissements finis. Cependant le théorème de Liouville n'est pas optimal et il a connu des améliorations successives jusqu'au théorème de Roth qui a valu à son auteur la médaille Fields en 1958 : si un irrationnel est approchable à un ordre $s > 2$, alors il n'est pas algébrique.

Dans ce contexte, plutôt que de chercher à optimiser l'ordre d'approximation, qui est de toute façon optimal pour les irrationnels algébriques, on cherchera à optimiser la constante $A > 0$ qui intervient dans la définition. On donne alors la définition suivante :

2. Ce principe est d'une simplicité quotidienne ! Si l'on range $n+1$ chaussettes dans une commode composée de n tiroirs, alors au moins un des tiroirs contiendra 2 chaussettes.

3. On rappelle qu'un réel est dit algébrique s'il est racine d'un polynôme non nul à coefficients entiers, et son degré est par définition le degré minimal d'un tel polynôme annulateur.

Définition 2.2 (Constante de Lagrange)**.** Soit α irrationnel. On appelle constante de Lagrange ou constante de meilleure approximation de α, le réel

$$L(\alpha) = \inf\left\{ A \mid \left|\alpha - \frac{p}{q}\right| < \frac{A}{q^2} \text{ admet une infinité de solutions } \frac{p}{q} \in \mathbb{Q} \right\}.$$

L'ensemble $L = \{L(\alpha), \alpha \in \mathbb{R} - \mathbb{Q}\}$ est appelé spectre de Lagrange.

Remarque 2.1. En vertu du théorème de Dirichlet démontré plus haut, cette constante $L(\alpha)$ existe bien (α irrationnel). Toutefois, rien n'assure a priori, que cette constante soit non nulle. Par exemple si α est approchable à l'ordre 3, $L(\alpha) = 0$. En revanche, d'après le théorème de Roth, la constante de Lagrange de tout irrationnel algébrique est non nulle.

Cette définition, naturelle du point de vue de l'intuition, est difficilement utilisable en pratique, et on lui préférera une autre formulation équivalente. Aboutir à cette formulation plus commode est l'objet du prochain paragraphe.

2.2. **Les fractions continues donnent les meilleures approximations d'ordre 2.** Pour étudier en pratique le spectre de Lagrange et de manière générale les approximations d'ordre 2, on utilise la théorie des fractions continues, dont on rappelle ici certains éléments. Comme il n'est pas l'objet de cet article de présenter une construction rigoureuse des fractions continues, les notions qui suivent seront admises et le lecteur qui n'est pas (plus ?) au fait de ces énoncés pourra rafraîchir sa mémoire à l'aide de [4].

Quelques notations usuelles :

— On utilise le symbole $[.]$ pour représenter les fractions continues : si $a_0, \dots, a_n \in \mathbb{Z}^*$,

$$[a_0, \dots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{\dots a_n}}.$$

— Si $a_0, a_1, \dots$ sont les coefficients du développement de α en fraction continue ($a_0 \in \mathbb{Z}^*, a_n \geq 1$ *pour* $n \geq 1$), le n-ième quotient partiel est noté $\frac{p_n}{q_n}$ et le n-ième reste est noté α_n. Ainsi,

$$\forall n \in \mathbb{N}, \frac{p_n}{q_n} = [a_0, \dots, a_n] \text{ et } \alpha = [a_0, \dots, a_{n-1}, \alpha_n].$$

En particulier $\frac{p_n}{q_n} \to \alpha$ et $\alpha_n \to 0$.

On rappelle ici les propriétés du développement en fraction continue, nécessaires à la suite de l'article.

Proposition 2.1. *Soit α irrationnel. Avec les notations ci-dessus :*

(i) $\forall n \in \mathbb{N}, p_{n+1} = a_{n+1}p_n + p_{n-1}, q_{n+1} = a_{n+1}q_n + q_{n-1}$ *et* $p_0 = a_0, p_{-1} = 1, q_0 = 1, q_{-1} = 0$.

(ii) $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \ldots < \frac{p_3}{q_3} < \frac{p_1}{q_1}$.

(iii) $\forall n \in \mathbb{N}, \alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}$.

(iv) $\forall n \in \mathbb{N}, p_n q_{n-1} - q_n p_{n-1} = (-1)^{n+1}$.

(v) Les quotients partiels $\frac{p_n}{q_n}$ sont des fractions de meilleure approximation, i.e. elles vérifient $|q\alpha - p| < |q_n\alpha - p_n| \Rightarrow q > q_n$. C'est ce qui leur vaut communément leur nom de réduite (cf [4]).

(vi) Ce sont en plus les seules (théorème de Legendre) : si $\frac{p}{q} \in \mathbb{Q}$ vérifie $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, alors $\frac{p}{q} = \frac{p_n}{q_n}$ pour un certain $n \in \mathbb{N}$.

Le premier résultat concernant le spectre de Lagrange et utilisant la théorie des fractions continues est dû à Hurwitz.

Théorème 2.2 (Hurwitz)**.** *Soit α irrationnel. Alors $L(\alpha) \leq \frac{1}{\sqrt{5}}$.*

Démonstration. Soit $n \in \mathbb{N}^*$. Avec les notations introduites, montrons qu'au moins une des fractions $\frac{p_{n-1}}{q_{n-1}}$, $\frac{p_n}{q_n}$, $\frac{p_{n+1}}{q_{n+1}}$ vérifie l'inéquation d'Hurwitz $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$. Supposons que cela ne soit pas le cas. En particulier on a :

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{\sqrt{5}q_{n-1}^2} + \frac{1}{\sqrt{5}q_n^2}.$$

D'autre part, d'après le point (ii) de la proposition 2.1, α est entre $\frac{p_{n-1}}{q_{n-1}}$ et $\frac{p_n}{q_n}$ donc

$$\left|\alpha - \frac{p_{n-1}}{q_{n-1}}\right| + \left|\alpha - \frac{p_n}{q_n}\right| = \left|\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n-1}q_n - p_nq_{n-1}}{q_{n-1}q_n}\right| \overset{(iv)}{=} \frac{1}{q_{n-1}q_n}.$$

D'où

$$\frac{1}{q_{n-1}q_n} > \frac{1}{\sqrt{5}q_{n-1}^2} + \frac{1}{\sqrt{5}q_n^2}.$$

En multipliant l'inégalité par $\sqrt{5}q_{n-1}^2 > 0$, on a

$$0 > (\frac{q_{n-1}}{q_n})^2 - \sqrt{5}(\frac{q_{n-1}}{q_n}) + 1.$$

Le polynôme $X^2 - \sqrt{5}X + 1$ ayant pour racines, $\frac{\sqrt{5}+1}{2}$ et $\frac{\sqrt{5}-1}{2}$, l'inégalité ci-dessus implique que

$$\frac{\sqrt{5}-1}{2} < \frac{q_{n-1}}{q_n}.$$

Avec le même raisonnement en utilisant les fractions $\frac{p_n}{q_n}$ et $\frac{p_{n+1}}{q_{n+1}}$, on obtient

$$\frac{q_{n+1}}{q_n} < \frac{\sqrt{5}+1}{2}.$$

D'après (i), $q_{n+1} = a_{n+1}q_n + q_{n-1}$, d'où $\frac{q_{n+1}}{q_n} = a_{n+1} + \frac{q_{n-1}}{q_n} \geq 1 + \frac{q_{n-1}}{q_n}$ (car $a_k \geq 1$ pour $k \geq 1$). Finalement :

$$\frac{\sqrt{5}+1}{2} = \frac{\sqrt{5}-1}{2} + 1 < \frac{q_{n-1}}{q_n} + 1 \leq \frac{q_{n+1}}{q_n} < \frac{\sqrt{5}+1}{2}.$$

C'est absurde. □

Résumons un peu la situation. Le point (v) de la proposition 2.1 nous informe que les fractions continues sont les meilleures approximations lorsque l'on contraint le dénominateur à ne pas être trop grand. Quant au point (vi) (théorème de Legendre), il montre l'unicité de telles approximations lorsque leurs constantes sont inférieures à $1/2$, ce qui est le cas de toutes les approximations qui nous intéressent comme l'assure le théorème d'Hurwitz ($1/\sqrt{5} < 1/2$). Les quotients partiels sont donc **les** fractions de meilleure approximation.

On désire alors réécrire une définition équivalente et plus concrète de la constante de Lagrange d'un irrationnel α, utilisant les quotients partiels de α. Intuitivement, on a par ce qui précède, pour une infinité de n, $\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{L(\alpha)}{q_n^2}$. Ceci nous encourage à évaluer, pour $n \in \mathbb{N}, n \geq 1$, la quantité $\left|\alpha - \frac{p_n}{q_n}\right|$, ce que nous faisons maintenant.

$$\left|\alpha - \frac{p_n}{q_n}\right| = \left|[a_0, \ldots, a_n, \alpha_{n+1}] - \frac{p_n}{q_n}\right| = \left|\frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n}\right|.$$

Après mise au même dénominateur et utilisation du point (iv) :

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n(\alpha_{n+1}q_n + q_{n-1})} = \frac{1}{q_n^2(\alpha_{n+1} + \frac{q_{n-1}}{q_n})}.$$

Posons $\lambda_n(\alpha) = \left(\alpha_{n+1} + \frac{q_{n-1}}{q_n}\right)^{-1}$. On a :

$$|q_n\alpha - p_n| = \frac{\lambda_n(\alpha)}{q_n^2}.$$

On montre facilement par récurrence que

$$\lambda_n(\alpha)^{-1} = [a_{n+1}, a_{n+2}, \ldots] + [0, a_n, a_{n+1}, \ldots, a_1],$$

ce qui fournit au passage un moyen simple de calculer la suite des $\lambda_n(\alpha)$, ce qu'on fera par la suite sur un exemple.

Proposition 2.2 (Nouvelle expression de la constante de Lagrange)**.** *Soit α un irrationnel. Avec la notation introduite ci-dessus*

$$L(\alpha) = \liminf_{n\to+\infty} \lambda_n(\alpha).$$

Démonstration. On note $L'(\alpha) = \liminf_{n\to+\infty} \lambda_n(\alpha)$.
Si A est un réel vérifiant $A > L'(\alpha)$. Alors par définition, il existe une infinité de $n \in \mathbb{N}$ tels que $A > \lambda_n(\alpha)$ et donc tels que $\frac{A}{q_n^2} > \frac{\lambda_n(\alpha)}{q_n^2}$. Par le calcul ci-dessus, ceci implique que pour de tels n, $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{A}{q_n^2}$ et donc que $A \geq L(\alpha)$. Ceci étant vrai quel que soit le réel A choisi, on a $L'(\alpha) \geq L(\alpha)$.

Soit maintenant A un réel, $A \leq \frac{1}{\sqrt{5}}$ tel que $\left|\alpha - \frac{p}{q}\right| < \frac{A}{q^2}$ pour infinité de p et q. En réalité, cette infinité de p et q sont des p_n et q_n (d'après (vi) de la proposition 2.1). Toujours par le calcul ci-dessus, cela implique que pour de tels n, $\lambda_n(\alpha) < A$ et donc que $L'(\alpha) < A$. En prenant la borne inférieure sur de tels A, on obtient que $L'(\alpha) \leq L(\alpha)$. Finalement on a bien $L(\alpha) = L'(\alpha)$.

□

3. Quand approximation diophantienne et minima des formes quadratiques se rejoignent

Utilisons la nouvelle définition de la constante de Lagrange d'un irrationnel pour voir un peu ce qu'elle apporte en pratique à travers l'exemple du nombre d'or $\phi = \frac{1+\sqrt{5}}{2}$ qui joue un rôle important en approximation diophantienne. ϕ est racine du polynôme $X^2 - X - 1$. Il vérifie donc $\phi = 1 + \frac{1}{\phi}$ et on en déduit aisément son développement en fraction continue : $\phi = [1, 1, 1, \ldots]$. On calcule donc

$$\forall n \in \mathbb{N}, \lambda_n(\phi)^{-1} = \underbrace{[1, 1, \ldots, 1]}_{\text{de taille } n} + [0, 1, 1, \ldots] = \underbrace{[1, 1, \ldots, 1]}_{\text{de taille } n} + \frac{1}{[1, 1, \ldots]}.$$

La suite $(\lambda_n(\phi))_n$ converge donc vers $\left(\phi + \frac{1}{\phi}\right)^{-1}$, et on en déduit que

$$L(\alpha) = \liminf_{n\to+\infty} \lambda_n(\alpha) = \left(\phi + \frac{1}{\phi}\right)^{-1} = \frac{1}{\sqrt{5}}.$$

Pour ϕ, le théorème d'Hurwitz est donc optimal [4] et pour l'améliorer, il faudra renforcer ses hypothèses. Cependant, cette optimalité n'est pas réservée à ϕ : elle l'est pour toute une infinité d'irrationnels qui se comportent comme ϕ vis à vis de l'approximation diophantienne.

4. C'est la raison pour laquelle on dit souvent que le nombre d'or est le plus irrationnel de tous les irrationnels.

Définition 3.1 (Nombres équivalents)**.** Soient $\alpha, \beta \in \mathbb{R}$. On dit que α et β sont équivalents, et on note $\alpha \sim \beta$ si

$$\alpha = \frac{a\beta + b}{c\beta + d} \text{ où } a, b, c, d \in \mathbb{Z} \text{ et } ad - bc = \pm 1.$$

Proposition 3.1. *Soient α, β deux irrationnels. Si $\alpha \sim \beta$, alors $L(\alpha) = L(\beta)$.*

Démonstration. Soient α et β comme dans la définition, et notons $\varepsilon = ad - bc \in \{-1, 1\}$. Soit $A > 0$ un réel et $p \in \mathbb{Z}, q \in \mathbb{N}^*$ des entiers tels que $\left|\alpha - \frac{p}{q}\right| < \frac{A}{q^2}$, c'est-à-dire $q|q\alpha - p| < A$. On veut construire un rationnel à partir de $\frac{p}{q}$ qui approche au mieux β. On a

$$q\alpha - p = \frac{q'\beta - p'}{c\beta + d},$$

où l'on a posé $q' = aq - cp$ et $p' = pd - bq$. Examinons $q'\beta - p'$. Après un calcul élémentaire,

$$q'\beta - \varepsilon p' = \frac{q\alpha - p}{a - c\alpha}.$$

En remarquant que $q' = aq - cp = q(a - c\alpha) + c(q\alpha - p)$, on a finalement

$$q'|q'\beta - \varepsilon p'| \leq q|q\alpha - p| + \frac{|c|}{|a - c\alpha|}|q\alpha - p|^2 \leq A + \frac{|c|}{|a - c\alpha|}\frac{A}{q^2}.$$

Le deuxième terme du membre de droite de l'inégalité peut être rendu aussi petit qu'on veut si q peut être choisi arbitrairement grand. Ainsi, si au départ, $A > L(\alpha)$, alors pour tout $A' > A$, on peut trouver une infinité de p, q vérifiant $q|q\alpha - p| < A$ avec q assez grand pour que les p', q' ainsi construits vérifient $q'|q'\beta - \varepsilon p'| < A'$ et par là on voit que $L(\beta) \leq A'$. Ceci étant valable pour tous $A' > A > L(\alpha)$, on en déduit que $L(\beta) \leq L(\alpha)$. En échangeant dans le raisonnement les rôles de α et β, on a l'inégalité inverse. Finalement $L(\alpha) = L(\beta)$. □

On peut maintenant affiner le résultat concernant l'optimalité du théorème d'Hurwitz pour ϕ.

Corollaire 3.1. *Si $\alpha \in \mathbb{R}$ est irrationnel, alors $L(\alpha) \leq \frac{1}{\sqrt{5}}$ et le résultat est optimal pour tous les réels équivalents au nombre d'or ϕ.*

Mais qu'en est-il si $\alpha \in \mathbb{R}$ n'est pas équivalent à ϕ ? Le théorème d'Hurwitz a été amélioré "à la main" à de nombreuses reprises : si $\alpha \not\sim \phi$, alors $L(\alpha) \leq \frac{1}{2\sqrt{2}}$ et il existe un irrationnel ψ pour lequel le résultat est optimal, ainsi que tous les irrationnels qui lui sont équivalents.

Le lecteur perspicace aura vu avec $\frac{1}{\sqrt{5}}$ et $\frac{1}{2\sqrt{2}}$ apparaître les nombres $\frac{m}{\sqrt{9m^2-4}}$ pour $m = 1$ et $m = 2$ et entrevu un lien avec la première partie. En effet, le spectre de Markov et celui de Lagrange sont intimement liés. Voyons dans quel sens.

Prenons un nombre quadratique θ, c'est-à-dire tel qu'il existe une forme quadratique non nulle f à coefficients rationnels vérifiant $f(\theta, 1) = 0$. Par exemple $\sqrt{2}$ est quadratique : en effet $f(\sqrt{2}, 1) = 0$ où par exemple $f(x, y) = x^2 - 2y$. Si $f \sim g$, alors il existe $a, b, c, d \in \mathbb{Z}$ tels que $ad - bc = \pm 1$ et $\forall x, y,\ f(x, y) = g(ax + by, cx + dy)$. On a alors $\theta \sim \frac{a\theta+b}{c\theta+d}$ et $0 = f(\theta, 1) = g(a\theta + b, c\theta + d)$ ce qui implique que $g(\frac{a\theta+b}{c\theta+d}, 1) = 0$. La constante $L(\theta)$ peut donc être calculée en se ramenant au calcul de $L(\psi)$ où les ψ est une racine du polynôme $g(X, 1)$ où g est une forme quadratique équivalente à f. Puisque les formes de Markov représentent toute une gamme de formes quadratiques comme on l'a vu dans la première partie, il est donc naturel d'étudier les constantes de Lagrange des racines de $f_m(X, 1)$ où m est un nombre de Markov. On démontre d'abord un lemme facile qui ne concerne pas seulement les formes de Markov mais n'importe quelle forme quadratique.

Lemme 3.1. *Soit f une forme quadratique et θ une racine irrationnelle de $f(X,1)$. Alors $L(\theta) \geq M(f)$.*

Démonstration. On note θ et ψ les racines de $f(X,1)$. On peut alors écrire

$$\forall x, y,\ f(x,y) = a(x-\theta y)(x-\psi y),$$

d'où

$$f(x,y) = a(\theta-\psi)y(x-\theta y) + a(x-\theta y)^2.$$

Soit $A > L(\theta)$. En appliquant l'égalité ci-dessus à $(x,y) = (p,q) \in \mathbb{Z} \times \mathbb{N}^*$ tels que $q|q\theta - p| \leq A$ (donnés par la définition de $L(\alpha)$), et en remarquant que $a|\theta - \psi| = \sqrt{\Delta(f)}$, on a

$$|f(p,q)| \leq \sqrt{\Delta(f)}A + a\frac{A}{q^2}.$$

Comme q peut être choisi arbitrairement grand, on en déduit que $\mu(f) \leq \sqrt{\Delta(f)}A$ c'est-à-dire que $M(f) \leq A$. Comme ceci est valable pour tout $A > L(\theta)$, on a $L(\theta) \geq M(f)$. □

Corollaire 3.2. *Soit m un nombre de Markov et f_m la forme de Markov associée. Alors les racines de $f_m(X,1)$ ont pour constante de Lagrange $m/\sqrt{9m^2-4}$.*

Démonstration. On donne seulement des éléments de démonstration. Grâce au lemme précédent, il ne reste qu'à établir l'inégalité $L(\theta) \leq M(f_m)$. On aura ainsi

$$L(\theta) = M(f_m) = \frac{m}{\sqrt{9m^2-4}}.$$

On note (m, m_1, m_2) un triplet de Markov contenant m et on considère u, u_1, v, v_1 les entiers définis comme lors de la construction des formes de Markov, c'est-à-dire tels que $u^2+1 = mv$ et $u_1^2+1 = m_1v_1$. On a alors

$$f_m(u,m) = m \text{ et } f_m(u_1,m_1) = -m.$$

L'ensemble $\{f_m(p,q), p \in \mathbb{Z}, q \in \mathbb{N}^*\}$ contient donc $\mu(f_m)$ et $-\mu(f_m)$. Grâce aux fractions continues, on peut alors montrer que les (p,q) vérifiant $f_m(p,q) = \pm\mu(f_m)$ peuvent être choisis avec q arbitrairement grand. Ce résultat est d'après S. Perrine, un cas particulier de ce qui porte souvent le nom de "théorème d'isolation" (on peut en apprendre plus dans sa thèse [5], ou dans l'ouvrage classique [2] de J. Cassels). En reprenant la démonstration du lemme précédent, on a alors, pour de tels (p,q),

$$\begin{aligned}\mu(f_m) = |f_m(p,q)| &= |a(\theta-\psi)q(q\theta-p) + a(p-q\theta)^2| \\ &\geq \sqrt{\Delta(f_m)}q|p-\theta q| - a|p-\theta q|^2.\end{aligned}$$

Pour tout $\varepsilon > 0$, (p,q) peuvent être choisis tels que $a|q-\theta p|^2 \leq \varepsilon$ et il vient pour cette infinité de (p,q),

$$\sqrt{\Delta(f_m)}q|q-\theta p| \leq \mu(f_m) + \varepsilon,$$

ce qui implique que

$$L(\theta) \leq M(f_m) + \frac{\varepsilon}{\sqrt{\Delta(f_m)}}.$$

Comme ε peut être pris aussi petit que l'on veut, on conclut que $L(\theta) \leq M(f_m)$. □

Grâce à ces derniers faits, on peut conclure notre étude et établir un résultat intéressant. Soit θ un irrationnel quadratique, racine de $f(X,1)$ où f est une forme quadratique vérifiant $M(f) > \frac{1}{3}$. Alors d'après le théorème de Markov sur les formes quadratiques, $f \sim f_m$ où f_m est une forme de Markov. Donc θ est équivalent à une racine de f_m et donc $L(\theta) = m/\sqrt{9m^2-4}$. On vient de décrire une petite partie du spectre de Lagrange. Ce résultat est incomplet, et Markov en a donné une version bien plus forte : il n'est pas nécessaire que θ soit quadratique pour conclure. Il suffit de demander $L(\theta) > \frac{1}{3}$.

Théorème 3.1 (Spectre de Lagrange au-dessus de 1/3)**.** *Le spectre de Lagrange est entièrement connu au-dessus de la valeur 1/3 :*

$$L \cap]1/3, +\infty[= \left\{ \frac{m}{\sqrt{9m^2-4}},\ m \text{ nombre de Markov} \right\}.$$

Conclusion - Pistes vers des aspects non abordés de la théorie de Markov

On sait maintenant que le spectre de Lagrange et de Markov coïncident sur $I =]1/3, +\infty[$. Plus précisément, l'ensemble $L \cap I = M \cap I$ est discret dénombrable, constitué des constantes $\{m/\sqrt{9m^2-4}, m \text{ nombre de Markov}\}$ qui s'accumulent vers $1/3$. Qu'en est-il au delà de l'intervalle I ? Les connaissances à ce sujet sont aujourd'hui encore largement lacunaires. Parmi les résultats obtenus, l'un établit l'existence d'un trou dans le spectre de Lagrange : $L \cap]1/\sqrt{13}, 1/\sqrt{12}[= \emptyset$.
On peut également se demander si la proposition 3.1 admet une réciproque. Cette question est toujours ouverte et elle porte le nom de conjecture d'unicité. Cette terminologie fait référence à une conjecture formulée par Frobenius à propos des nombres de Markov : *tout nombre de Markov apparaît dans l'arbre de Markov une unique fois comme maximum d'un triplet*. Il se trouve que cette affirmation est équivalente à cette éventuelle réciproque de la proposition 3.1. La question a été attaquée par différentes approches, toutes infructueuses, et laissant place systématiquement à de faux espoirs si bien que Richard Guy dans l'une de ses publications a déclaré "Don't try to solve it !". Cette conjecture a de multiples formulations (on vient d'en donner deux) dont une en termes de géodésiques sur des surfaces obtenues à partir de recollement de polygones hyperboliques. C'est un joli sujet pour un éventuel article dans un prochain numéro du Journal de Maths des Élèves, qui sait.

Remerciements et référence. Je conseille vivement le livre [1] de M. Aigner, qui aborde différents points de vue sur l'approximation diophantienne et la théorie de Markov. Je remercie mon professeur de Spé, Romain Krust, qui me l'a recommandé, et à qui je dédie ce premier article dans le Journal de Maths des Élèves.

Références.

[1] M. Aigner. *Markov's theorem and 100 years of the Uniqueness Conjecture*. Springer, 2013.
[2] J. Cassels. *An introduction to diophantine approximation*. Cambridge University Press, 1957.
[3] J. Cassels. *An introduction to the geometry of numbers*. Springer, 1959.
[4] R. Descombes. *Éléments de théorie des nombres*. Presses universitaires, 1986.
[5] S. Perrine. "Approximations diophantiennes (Théorie de Markov)". Thèse de doct. Université de Metz, 1988.