TABLE DES MATIÈRES

PRÉFACE

Ce volume explore les liens entre nombres et géométrie, à partir d'objets de nature dynamique. Il montre toute la richesse de ces relations sur l'exemple de la résolution par G. Margulis d'une célèbre conjecture sur les valeurs prises par des polynômes.

Nous tenons à remercier la direction de l'École polytechnique, et tout particulièrement la Direction des Études, pour l'aide matérielle importante qu'elle a apportée à la préparation des journées X-UPS. Nous remercions aussi les Éditions de l'École polytechnique qui ont bien voulu accueillir la série *Journées mathématiques X-UPS* au sein de leurs collections.

Nous remercions enfin les secrétaires du Centre de mathématiques, notamment Claudine Harmide et Michèle Lavallette, pour leur contribution à l'organisation de ces journées.

Nicole Berline, Alain Plagne et Claude Sabbah

INTRODUCTION

Soit $n \geqslant 2$ un entier. Une *forme quadratique* q sur l'espace vectoriel $\mathbb{R}^n$ est une application de $\mathbb{R}^n$ dans $\mathbb{R}$, de la forme

$$q : (X_1, \dots, X_n) \longmapsto \sum_{i,j=1}^{n} a_{ij} X_i X_j$$

où pour $1 \leqslant i, j \leqslant n$, les coefficients a_{ij} sont des nombres réels. Dans cet ouvrage, nous nous intéressons aux valeurs prises par une forme quadratique donnée q sur l'ensemble $\mathbb{Z}^n$ des points de coordonnées entières de $\mathbb{R}^n$, et surtout aux propriétés topologiques du sous-ensemble $q(\mathbb{Z}^n)$ de $\mathbb{R}$.

Par exemple, si les coefficients de q sont des nombres rationnels, alors $q(\mathbb{Z}^n)$ est contenu dans $\frac{1}{p}\mathbb{Z}$ pour un entier $p \geqslant 1$, et en particulier est discret. Plus généralement, si q est *rationnelle*, *i.e.* multiple réel d'une forme quadratique à coefficients entiers, alors $q(\mathbb{Z}^n)$ est contenu dans $a\mathbb{Z}$ pour un $a \in \mathbb{R}$, donc est fermé et discret.

Donnons tout d'abord des motivations historiques à l'étude topologique des valeurs prises par les formes quadratiques sur les points entiers.

Cette problématique semble provenir de questions d'approximation d'un nombre réel par des nombres rationnels.

Une inégalité élémentaire et bien connue de G. Lejeune-Dirichlet (1805–1859) dit (voir plus précisément le théorème 1.1 du texte [Dal][(1)]) qu'étant donné un nombre réel irrationnel θ, il existe une infinité de nombres rationnels a/b (nous supposerons toujours que a et b sont des entiers premiers entre eux,

---

(1) N.d.E. : dans tout le volume, les références au texte de Françoise Dal'Bo sont indiquées par [Dal], celles au texte de Frédéric Paulin par [Pau] et enfin, celles au texte de Gilles Courtois par [Cou]. Chaque texte contient ses propres références bibliographiques et celles-ci sont aussi regroupées à la fin du volume.

avec b non nul) tels que

$$\left|\theta - \frac{a}{b}\right| \leqslant \frac{1}{b^2}.$$

Si θ est un nombre réel irrationnel, on définit alors naturellement sa *constante d'approximation* $\nu(\theta)$ par

$$\nu(\theta) = \liminf_{\substack{b \in \mathbb{Z} \\ b \to +\infty}} \min_{a \in \mathbb{Z}} b^2 \left|\theta - \frac{a}{b}\right|,$$

l'inégalité de Dirichlet disant précisément que $\nu(\theta) \in [0,1]$.

Par une terminologie éclairante, un nombre réel irrationnel θ est dit *mal approchable* par des nombres rationnels si $\nu(\theta) > 0$. On montre, voir le corollaire 1.10 de [Dal], que c'est en particulier le cas des nombres réels irrationnels *quadratiques*, *i.e.* racines de polynômes de degré 2 à coefficients entiers, comme le nombre d'or $(1+\sqrt{5})/2$.

Une forme quadratique *binaire* est une forme quadratique sur $\mathbb{R}^2$. Pour tout nombre réel irrationnel θ, considérons la forme quadratique binaire q_θ définie par

$$q_\theta(X,Y) = XY - \theta Y^2.$$

Ainsi, par définition, un nombre réel irrationnel θ est mal approchable si et seulement si l'adhérence dans $\mathbb{R}$ de l'ensemble $q_\theta(\mathbb{Z}^2) - \{0\}$ ne contient pas 0. Cette reformulation met en lumière un lien entre la topologie du sous-ensemble $q(\mathbb{Z}^2)$ de $\mathbb{R}$ et la nature arithmétique des coefficients d'une forme quadratique binaire q. Remarquons aussi que ceci implique en particulier que si θ est le nombre d'or $(1+\sqrt{5})/2$, alors $q_\theta(\mathbb{Z}^2)$ n'est pas dense dans $\mathbb{R}$.

Faisons quelques remarques sur la nature de la forme quadratique q_θ ci-dessus. Une forme quadratique q sur $\mathbb{R}^n$ est dite

- *non dégénérée* si le seul élément x dans $\mathbb{R}^n$ tel que, pour tout y dans $\mathbb{R}^n$, on ait $q(x+y) = q(x) + q(y)$ est l'élément nul 0 ;
- *indéfinie* si elle n'est ni à valeurs toutes positives, ni à valeurs toutes négatives ;
- *irrationnelle* si elle n'est pas rationnelle.

Il est immédiat que si θ est un nombre réel irrationnel, alors q_θ est non dégénérée, indéfinie et irrationnelle.

Fixons donc une forme quadratique q sur $\mathbb{R}^n$, non dégénérée, indéfinie et irrationnelle. Existe-t-il toujours un lien entre la topologie de $q(\mathbb{Z}^n)$ et l'arithmétique des coefficients de q ? La réponse à cette question est bien différente selon que l'on suppose $n = 2$ ou $n \geqslant 3$. Le but de ce texte est d'en expliquer les raisons, en utilisant uniquement des arguments élémentaires de topologie et d'actions de groupes linéaires

En dimension $n = 2$, ce lien existe bien, et il est exposé dans [Dal] (voir aussi [Dal2] pour une introduction illustrée). En particulier, nous donnons un critère de nature arithmétique (via le développement en fraction continue de nombre réels) sur les coefficients d'une forme quadratique binaire q pour que $q(\mathbb{Z}^2)$ soit dense dans $\mathbb{R}$ (voir le corollaire 2.6 du texte [Dal]). En appliquant ce critère, nous montrons par exemple que si

$$\theta = 1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{4 + \ddots}}},$$

alors $q_\theta(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$.

Le texte [Dal] montre aussi (en en expliquant les raisons arithmétiques) qu'entre le cas où $q(\mathbb{Z}^2)$ est fermé discret dans $\mathbb{R}$ et le cas où $q(\mathbb{Z}^2)$ est dense dans $\mathbb{R}$ se trouve un large éventail de possibilités d'ensembles $q(\mathbb{Z}^2)$, ni denses, ni fermés, dont la topologie peut être complexe.

En dimension $n \geqslant 3$, la situation est radicalement différente, comme le montre le résultat suivant démontré en 1987 par G. Margulis [Mar1, Mar2]

***Théorème* (Margulis).** *Soient $n \geqslant 3$ un entier et q une forme quadratique sur $\mathbb{R}^n$ non dégénérée, indéfinie et irrationnelle. Alors $q(\mathbb{Z}^n)$ est dense dans $\mathbb{R}$.*

Cet énoncé (ou celui a priori plus faible que 0 n'est pas un point isolé de $q(\mathbb{Z}^n)$ dans $\mathbb{R}$) a été conjecturée par A. Oppenheim (1903-1997) en 1929 (voir [Opp1, Opp2]) pour $n \geqslant 5$ (voir [Ser, page 77] pour comprendre une telle restriction sur n). Cette conjecture a été étendue plus généralement à $n \geqslant 3$ par H. Davenport (1907-1969), qui avec des collaborateurs [DH, BD, DR] la montre dans des cas particuliers, par des méthodes de théorie analytique des nombres. C'est finalement par des méthodes géométriques, reposant sur un lien entre la topologie des ensembles $q(\mathbb{Z}^n)$ et la dynamique topologique de groupes linéaires, qu'elle sera résolue par G. Margulis. Le but du texte [Cou] est d'exposer cette démonstration, en suivant les arguments élémentaires donnés par S. Dani et G. Margulis (voir [Dan] simplifiant encore [DM]). Nous recommandons aussi le livre [BM], le mémoire [Bre] et l'excellent survol [Mar4] pour un historique et la genèse de la preuve.

Voici en quelques lignes le fil conducteur de cette démonstration.

Il est naturel de considérer le groupe des transformations préservant q, plus précisément le groupe spécial orthogonal de q défini par

$$\mathrm{SO}(q) = \{g \in \mathrm{SL}_n(\mathbb{R}) : q \circ g = q\}.$$

Pour $g \in \mathrm{SL}_n(\mathbb{R})$, l'ensemble $g(\mathbb{Z}^n)$ est un *réseau* de $\mathbb{R}^n$, *i.e.* un sous-groupe discret, qui engendre $\mathbb{R}^n$ comme espace vectoriel réel. Comme g est de déterminant égal à 1, ce réseau $g(\mathbb{Z}^n)$ est *unitaire*, *i.e.* ses parallélotopes fondamentaux sont de volume 1 (voir le paragraphe 1 de [Pau]). L'ensemble des réseaux unitaires est naturellement muni d'une topologie (deux réseaux sont proches s'ils admettent des parallélotopes fondamentaux proches, voir [Pau]). La nature topologique de l'orbite

$$\mathrm{SO}(q) \cdot \mathbb{Z}^n = \{g(\mathbb{Z}^n) : g \in \mathrm{SO}(q)\}$$

dans cet espace est reliée à celle de l'ensemble $q(\mathbb{Z}^n)$: par exemple, comme tout vecteur non nul de $\mathbb{R}^2$ est élément d'un réseau unitaire (car $n \geqslant 2$), comme q est continue et $q(\mathbb{Z}^n) = q(g(\mathbb{Z}^n))$ pour tout g dans $\mathrm{SO}(q)$, si l'orbite $\mathrm{SO}(q) \cdot \mathbb{Z}^n$ est dense dans l'espace des réseaux unitaires, alors $q(\mathbb{Z}^n)$ est dense dans $q(\mathbb{R}^n) = \mathbb{R}$ (car q est indéfinie).

C'est cette passerelle entre arithmétique et dynamique que va emprunter G. Margulis pour démontrer la conjecture d'Oppenheim. Sous forme implicite, l'idée d'utiliser des techniques de géométrie des nombres (*i.e.* l'étude des réseaux et des orbites de groupes linéaires comme $\mathrm{SL}_n(\mathbb{R})$ et $\mathrm{SL}_n(\mathbb{Z})$) remonte à J. Cassels et P. Swinnerton-Dyer [CSD]. Mais c'est M. Raghunathan qui a formellement établi un lien entre cette conjecture et l'étude de l'adhérence d'orbites de sous-groupes du groupe linéaire.

Le but du texte [Pau] est d'introduire et d'étudier les outils nécessaires pour le texte [Cou]. Il est donc essentiellement axé sur une étude des groupes $\mathrm{SL}_n(\mathbb{R})$ et $\mathrm{SL}_n(\mathbb{Z})$, de leurs sous-groupes, et de leurs principales actions. Deux sous-groupes y sont privilégiés, le sous-groupe $\mathbf{A}$ des matrices diagonales de $\mathrm{SL}_n(\mathbb{R})$ à coefficients diagonaux strictement positifs et le sous-groupe $\mathbf{N}$ des matrices triangulaires supérieures à coefficients diagonaux égaux à 1. Ces groupes agissent naturellement sur l'espace topologique quotient $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$, qui par ailleurs s'identifie à l'espace des réseaux unitaires de $\mathbb{R}^n$ (voir le paragraphe 2 de [Pau]). Leur dynamique sur l'espace quotient $\mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$ est bien différente : celle des sous-groupes de $\mathbf{A}$ est nettement plus compliquée que celle des sous-groupes de $\mathbf{N}$ (voir [Rat2, Ghy, Mar5] et le paragraphe 5 de [Pau] pour des raisons, ainsi que le paragraphe 4 de [Dal] pour les phénomènes remarquables lorsque $n = 2$). Ces deux groupes $\mathbf{A}$ et $\mathbf{N}$ sont reliés au groupe $\mathrm{SO}(q)$. Plus précisément, si $n = 2$, alors un sous-groupe d'indice 2 du groupe $\mathrm{SO}(q)$ est conjugué à $\mathbf{A}$ (voir le paragraphe 4 de [Dal]) ; en revanche si $n \geqslant 3$, alors le groupe $\mathrm{SO}(q)$ est engendré par des sous-groupes *unipotents* (*i.e.* conjugués à des sous-groupes de $\mathbf{N}$) de $\mathrm{SL}_n(\mathbb{R})$. Cette différence se reporte sur la topologie des ensembles $q(\mathbb{Z}^n)$.

Vers les années 1970, M. Raghunathan énonce une conjecture sur la « régularité topologique » des adhérences des orbites de sous-groupes unipotents sur $\mathrm{SL}_n(\mathbb{R})/\,\mathrm{SL}_n(\mathbb{Z})$, dont il démontre qu'elle entraîne facilement la conjecture d'Oppenheim. Cette idée sera reprise par G. Margulis pour démontrer le théorème énoncé ci-dessus. Le cœur de la preuve de S. Dani et G. Margulis, exposée dans le texte [Cou], est en effet une étude (élémentaire, même si longue et astucieuse) de dynamique topologique des actions de sous-groupes unipotents sur $\mathrm{SL}_n(\mathbb{R})/\,\mathrm{SL}_n(\mathbb{Z})$. En suivant [Ghy], nous donnerons dans le paragraphe 5 de [Pau] une preuve du théorème suivant, démontré par G. Hedlund.

***Théorème* (Hedlund).** *Toute orbite du sous-groupe* $\mathbf{N}$ *de* $\mathrm{SL}_2(\mathbb{R})$ *dans* $\mathrm{SL}_2(\mathbb{R})/\,\mathrm{SL}_2(\mathbb{Z})$ *est périodique ou dense.*

Cette preuve peut être prise comme un guide de lecture pour [Cou].

Vers les années 1990, M. Ratner [Rat1, Rat2] (voir aussi l'excellent survol [Ghy]) démontre la conjecture de Raghunathan. Elle montre en particulier qu'un ensemble du type $\mathrm{SO}(q)\cdot\mathbb{Z}^3$, lorsque q est une forme quadratique non dégénérée indéfinie, est soit fermé soit dense dans l'espace des réseaux unitaires de $\mathbb{R}^3$. La conjecture d'Oppenheim pour $n = 3$ découle alors du fait que $\mathrm{SO}(q)\cdot\mathbb{Z}^3$ est fermé si et seulement si q est rationnelle, résultat dû à M. Raghunathan (voir par exemple [BM, page 166]). Des versions quantitatives renforçant le théorème de Margulis ci-dessus ont été obtenues plus récemment par A. Eskin, G. Margulis, S. Mozes [EMM]. Nous n'utilisons dans cet ouvrage que des arguments simples d'actions de groupes linéaires, en nous restreignant à une étude de dynamique topologique, et non pas mesurable comme dans les travaux de Ratner ou dans la référence [BM].

Le domaine des actions de groupes linéaires sur des espaces homogènes, avec applications arithmétiques potentielles, est mondialement très actif. Nous concluons cette introduction par un exemple de question ouverte dans ces thèmes. Une forme quadratique non dégénérée indéfinie sur $\mathbb{R}^2$ est le produit de deux formes linéaires linéairement indépendantes. Nous étudierons leurs propriétés arithmétiques dans [Dal]. L'étude du produit P de $n \geqslant 3$ formes linéaires en n variables est actuellement un domaine largement ouvert. Par exemple, l'étude de $P = x(y-\alpha x)(z-\beta x)$, lorsque α, β sont des nombres réels fixés, conduit à la conjecture de Littlewood (formulée par J. Littlewood dans les années 1930) qui s'énonce ainsi : pour tous $\alpha, \beta \in \mathbb{R} - \mathbb{Q}$,

$$\liminf_{\substack{q\in\mathbb{Z}\\ q\to+\infty}} \ \inf_{p,p'\in\mathbb{Z}} \ q\,|p-\alpha q|\,|p'-\beta q| = 0.$$

Suite aux travaux de J. Cassels et P. Swinnerton-Dyer [CSD], G. Margulis a montré dans [Mar5] que cette conjecture découle aussi d'une conjecture, dite de Margulis, sur la dynamique topologique du sous-groupe diagonal **A** de $\mathrm{SL}_3(\mathbb{R})$ sur l'espace quotient $\mathrm{SL}_3(\mathbb{R})/\mathrm{SL}_3(\mathbb{Z})$. Nous renvoyons par exemple à [PV, EKL] pour des résultats particuliers mais importants sur la conjecture de Littlewood. La dynamique des sous-groupes diagonaux de dimension $n \geqslant 3$ est encore peu connue et donne lieu actuellement à de nombreuses recherches.

Cet ouvrage ne présuppose connues que des notions de niveau au plus licence sur les formes quadratiques, les groupes linéaires et la topologie. Les trois textes peuvent être lus de manière indépendante, à l'exception du paragraphe 4 de [Dal], qui s'appuie en partie sur les paragraphes 1 et 2 de [Pau], et quitte à admettre dans [Cou] les points nécessaires des textes précédents. Nous nous sommes attachés à dévisser au maximum les notions et arguments, pour que cet ouvrage soit largement accessible. Nous espérons donc qu'il sera attrayant pour de nombreux lecteurs.

Gilles Courtois, Françoise Dal'Bo & Frédéric Paulin