

# Éditorial

---

*Chères lectrices, chers lecteurs,*

*c'est avec beaucoup de plaisir et d'enthousiasme que je rejoins le comité de rédaction de la Gazette, succédant ainsi à Bernard Helffer qui assumait la tâche de rédacteur en chef depuis quelques numéros. Je le remercie pour son travail et l'accueil chaleureux qu'il m'a réservé depuis plusieurs mois. Avec un comité de rédaction élargi, nous espérons pouvoir répondre davantage à vos attentes et vous proposer une Gazette ambitieuse, vivante et dynamique. Nous revenons d'ailleurs dans ces pages sur les résultats du questionnaire qui vous a été proposé au printemps dernier et dont nous tiendrons bien sûr compte pour des évolutions à venir. D'ores et déjà, Sébastien Gouezel, Damien Gayet et Stéphane Seuret rallient l'équipe de rédaction.*

*Ils existent ! Des mathématiciens à la fois brillants, récents lauréats de l'académie des sciences, et suffisamment courageux pour tenter une expérience inédite : rédiger simultanément deux articles jumeaux sur deux médias différents, le papier pour la Gazette et la toile pour Images des Mathématiques (IdM). Notre partenariat avec IdM se poursuit et c'est au tour de Julien Barré et Frédéric Klopp de relever le défi.*

*Mais à n'en pas douter le congrès international des mathématiciens, qui s'est déroulé cet été à Séoul, est bien l'événement incontournable de cette rentrée mathématique. Les feux de l'actualité sont naturellement braqués sur les nouveaux lauréats de la médaille Fields. Une promotion frappée du sceau de la nouveauté. Ils nous viennent de contrées inédites : d'Autriche, du Brésil, du Canada, et d'Iran. Mais aussi un peu d'Angleterre, des États-Unis, d'Inde, de Suisse et même... de France. Et puis, certains d'entre eux sont même... une femme. Enfin ! La Gazette a fait le voyage et vous offre dans ce numéro le premier volet d'un grand dossier consacré à l'ICM 2014.*

*Plus confidentiel, mais la rumeur vous est peut-être déjà parvenue : le mathématicien Vladimir Voevodsky se détournerait depuis quelques temps de ses premières amours mathématiques. Mais pour quels motifs ? Quelques éléments de réponse à découvrir dans un dossier sur les mathématiques certifiées et la théorie des types.*

*Pour finir cet éditorial, je voudrais adresser un remerciement particulier à Valérie Berthé et à Gaél Octavia, qui, en plus des membres du comité de rédaction, ont particulièrement œuvré à l'élaboration de ce numéro. Je salue également Christian Rétoré dont le mandat est arrivé à sa fin et qui quitte donc le comité de rédaction.*

*En vous souhaitant une bonne rentrée et une agréable lecture,*

— Boris Adamczewski



**Revue  
d'histoire  
des mathématiques**  
Tome 20, Fascicule 1

**Sommaire**

**Éditorial**

**Sloan Evans Despeaux**

Mathematical questions: a convergence of mathematical practices in British journals of the eighteenth and nineteenth centuries

**Alberto Cogliati**

Riemann's *Commentatio Mathematica*, a reassessment

**Christophe Eckes**

Weyl et la géométrisation de la physique

prix public\* : 43 € - prix membre\* : 30 €

frais de port non compris

(Revue disponible aussi par abonnement)



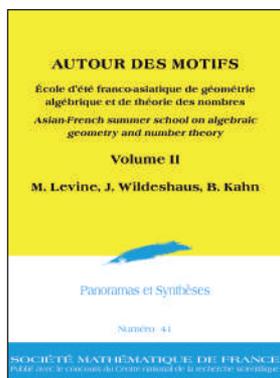
Institut Henri Poincaré  
11 rue Pierre et Marie Curie  
F-75231 PARIS CEDEX 05

<http://smf.emath.fr>

# SOMMAIRE DU N° 142

---

<b>SMF</b>	
Mot du Président .....	5
<b>MATHÉMATIQUES</b>	
Percolation de la rigidité, <i>J. Barré</i> .....	7
Électrons en interaction dans un milieu aléatoire, <i>F. Klopp</i> .....	19
<b>NOUVELLES DU CONGRÈS INTERNATIONAL</b>	
Séoul 2014 : quelques mots pour un ICM, <i>G. Octavia</i> .....	35
Le théorème de la baguette magique de A. Eskin et M. Mirzakhani, <i>A. Zorich</i> .....	39
Artur Avila, un génie carioca à Paris, <i>P. Hubert, R. Krikorian</i> .....	55
En aparté avec Manjul Bhargava et Martin Hairer .....	70
<b>THÉORIE DES TYPES ET MATHÉMATIQUES CERTIFIÉES</b>	
Formalisation mathématique, certification logicielle, même combat! <i>P.-L. Curien</i> .....	83
La bifurcation de Vladimir Voevodsky .....	87
Homotopy type theory, <i>Á. Pelayo, M. A. Warren</i> .....	95
<b>CARNET</b>	
Pierre Liardet, <i>J.-P. Allouche, H. Daudé</i> .....	111
<b>VIE DE LA SOCIÉTÉ</b>	
La <i>Gazette</i> et vous .....	115
Les prix d'Alembert et Anatole Decerf 2014, <i>P. Pansu</i> .....	128
<b>INFORMATIONS</b>	
Quelques nouvelles de l'Insmi, <i>S. David, C. Fermanian Kammerer</i> .....	131
<b>LIVRES</b> .....	133



## Panoramas et Synthèses

### Autour des Motifs II École d'été franco-asiatique de géométrie algébrique et de théorie des nombres

M. Lévine, J. Wildeshaus, B. Kahn

Ce volume contient la seconde partie des notes de cours de l'École d'été franco-asiatique de géométrie algébrique et de théorie des nombres, qui s'est tenue à l'Institut des Hautes Études Scientifiques (Bures-sur-Yvette) et à l'université Paris-Sud XI en juillet 2006. Cette école était consacrée à la théorie des motifs et à ses récents développements, ainsi qu'à des sujets voisins, comme la théorie des variétés de Shimura et des représentations automorphes. Cette seconde partie est constituée de versions développées des cours de M. Levine consacrés aux catégories triangulées de motifs et à la théorie homotopique des schémas (Six lectures on motives) et des leçons de J. Wildeshaus sur les motifs bords et leurs applications (Boundary motives, relative motives and extensions of motives) et de B. Kahn sur une version triangulée des conjectures de Tate et Beilinson sur les cycles algébriques sur les corps finis (The full faithfulness conjectures in characteristic  $p$ ).

*This volume contains the second part of the lectures notes of the Asian-French summer school on algebraic geometry and number theory, which was held at the Institut des Hautes Études Scientifiques (Bures-sur-Yvette) and the université Paris-Sud XI (Orsay) in July 2006. This summer school was devoted to the theory of motives and its recent developments, and to related topics, notably Shimura varieties and automorphic representations. The contributions in this second part are expanded versions of the series of lectures by M. Levine on triangulated categories of motives and motivic homotopy of schemes (Six lectures on motives), and of the additional lectures by J. Wildeshaus on boundary motives and their applications (Boundary motives, relative motives and extensions of motives) and by B. Kahn on a triangulated version of the conjectures of Tate and Beilinson on algebraic cycles over a finite field (The full faithfulness conjectures in characteristic  $p$ ).*

ISBN 978-2-85629-784-1

prix public : 56 € - prix membre : 39 € frais de port non compris



Institut Henri Poincaré  
11 rue Pierre et Marie Curie  
F-75231 PARIS CEDEX 05

<http://smf.emath.fr>

## Mot du Président

---

L'été 2014 est celui du Congrès International de Séoul, où les mathématiques françaises ont été à l'honneur. Ce numéro de la *Gazette* revient longuement sur cet événement ; je vous invite donc à le parcourir en détail et vous livre quelques réflexions qu'il m'a inspirées.

Il y a bien sûr la médaille Fields d'Artur Avila qui nous réjouit et confirme le rang de notre école dans le monde. Il est important de se rappeler aussi l'importance de la délégation française invitée à Séoul, forte d'une quarantaine de membres, et qui couvre tout le spectre des mathématiques, que ce soit les domaines au cœur des fondements, ceux riches d'applications, ceux aux interfaces avec d'autres disciplines mais aussi l'histoire des mathématiques ou le partage du savoir avec des publics variés.

La France compte à ce jour 13 médaillés Fields. Dix d'entre eux sont des anciens élèves de l'École normale supérieure de la rue d'Ulm et neuf ont occupé un poste de chargé de recherche en début de carrière. La présence des Éns et le statut de chercheur au CNRS sont donc de formidables leviers pour attirer et retenir des jeunes mathématiciennes et mathématiciens brillants. Artur Avila présente un profil différent : formé au Brésil, dont l'école mathématique a tissé des liens très étroits avec la France depuis plusieurs décennies et tout particulièrement en « systèmes dynamiques », il a pu trouver en France des conditions favorables pour mener à bien ses travaux de recherche. Cette récompense de notre collègue, je la lis comme un constat de réussite pour le travail de structuration des mathématiques françaises. On pense bien sûr aux outils formidables que sont l'IHP, l'IHÉS et le CIRM, qui travaillent en étroite collaboration et assurent une visibilité internationale de tout premier plan ; mais les mathématiques en France c'est aussi un grand nombre de laboratoires répartis sur tout le territoire, coordonnés par les instituts nationaux que sont le CNRS et INRIA et représentés par des sociétés savantes qui essayent au mieux d'être proches du terrain.

Il nous faut cependant rester très vigilants car ces résultats sont loin d'être assurés pour l'avenir ; on ne peut que s'inquiéter du fait que le financement public de la recherche en France soit très en dessous de celui d'autres pays européens, des États-Unis et de pays émergents. Le nombre de postes de maître de conférences et de professeurs a chuté de façon spectaculaire ces dernières années ; le phénomène a été amplifié par les difficultés financières que traversent les universités et la chute des effectifs de nos masters qui rend difficile le maintien des postes lorsque la logique comptable prévaut. Une des spécificités du système français par rapport à de nombreux autres pays développés est d'offrir dès la sortie de thèse des postes permanents de chercheurs ou d'enseignants-chercheurs, susceptibles de retenir les jeunes mathématiciennes et mathématiciens. Ces conditions matérielles favorisent

le travail de longue haleine nécessaire pour aborder des questions difficiles, favoriser la maturation des idées, créer des ponts avec de nouvelles thématiques... Cette spécificité est pour beaucoup à mon avis dans la réussite et l'attractivité de notre école ; elle est malheureusement peu à peu mise à mal par le financement sur projet qui se généralise et l'apparition de nombreux contrats de travail à durée limitée. Comment dans ces conditions continuer à attirer les jeunes générations vers les métiers de la recherche, elles qui déjà se détournent des métiers de l'enseignement ?

J'en viens à présent à ce qui sans nul doute restera le symbole du millésime ICM 2014 : la récompense de Maryam Mirzakhani. Enfin, une médaille Fields décernée à une femme ! Cette reconnaissance au plus haut niveau est un formidable message pour les jeunes femmes à travers le monde. Elle nous interpelle en particulier en France en cette période où il est très difficile d'attirer les jeunes filles vers les disciplines scientifiques et où les mathématiciennes en poste rencontrent de nombreux obstacles au cours de leur carrière. Les analyses et rencontres sur la parité se multiplient, le déséquilibre s'accroît pourtant. Fasse que la médaille de Maryam Mirzakhani interpelle et modifie cet état de fait. Attention ! de nombreux voyants sont au rouge : très peu de femmes dans les recrutements récents de chercheurs et d'enseignants-chercheurs, notamment chez les professeurs, un déficit chronique de candidatures féminines lors des campagnes d'avancement,... Le fait que lors de la campagne de recrutement du printemps 2014, aucune femme de la section CNU 25 n'ait été recrutée « professeure » doit nous faire réagir. Dans certains pays, notamment en Europe, des politiques de « quotas » ont été mises en place depuis plusieurs années, pour essayer d'inverser cette dynamique. Il nous faut être conscient que, sans réaction claire et efficace de notre communauté sur cette question, on peut y être acculé à terme en France. Je ne crois pas que ce soit souhaitable.

Puisque j'ai évoqué ci-dessus les concours récents de professeurs, j'aimerais conclure ce mot en évoquant la politique de non-recrutement local amorcée il y a une vingtaine d'années et qui est une spécificité de notre discipline en France. Celle-ci a indéniablement renforcé le maillage du territoire par nos laboratoires, favorisé les interactions et participé à sa façon au dynamisme des mathématiques françaises. Mais menée de façon trop obstinée, en refusant en particulier de prendre en compte les questions de rapprochement de conjoints, elle induit des effets pervers et désespère de nombreux collègues... Et là aussi, les mathématiciennes sont tout particulièrement touchées par ce phénomène, renvoyant ainsi à la question de la parité évoquée ci-dessus. Introduire un peu de souplesse et d'humanité dans le mécanisme de recrutement en évitant les dérives du « localisme » n'est pas aisé, à notre communauté de faire preuve d'imagination ! Je suis convaincu qu'elle le peut.

Je vous souhaite une bonne rentrée.

Le 1<sup>er</sup> octobre 2014  
*Marc Peigné*

# MATHÉMATIQUES

---

Comme dans le numéro précédent, la rubrique de mathématiques donne la parole à deux autres lauréats de grands prix de l'académie en 2013 : Julien Barré et Frédéric Klopp. Cette publication se fait dans le cadre d'une collaboration de la Gazette avec Images des Mathématiques (IdM) qui publiera simultanément un texte court des mêmes auteurs sur son site. Côté IdM, Maxime Bourrigan et Clément Caubel ont assuré la coordination de l'évaluation par des chercheurs et doctorants et le secrétariat a été assuré par Carole Gaboriau et Maï Sauvageot.

## Percolation de la rigidité

Julien Barré<sup>1</sup>

---

### 1. Introduction

S'il est naturel que les jeux de réflexion soient à l'origine de questions mathématiques variées, on imagine moins facilement que cela puisse être aussi le cas de jeux pour tout-petits. Les boules et barres aimantées de la figure 1 sont destinées aux enfants d'un an environ. Les boules jouent le rôle de pivots, autour desquels les barres peuvent tourner librement ; les barres peuvent avoir des longueurs différentes, et chacune fixe la distance entre deux boules. Les structures ainsi formées peuvent être déformables, ou rigides. Sur l'exemple de la figure 1 à gauche, on voit facilement que la structure est rigide ; mais on s'aperçoit vite que si le nombre de barres et de pivots augmente, la question est beaucoup plus ardue ; il n'est pas si facile de déterminer par exemple si la structure de la figure 1 à droite est rigide ou pas. Cette question naturelle et intuitive va nous entraîner de

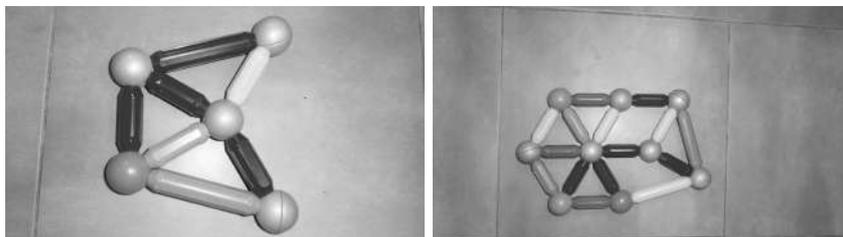


FIG. 1. Structures de barres et pivots en 2D. Celle de gauche est rigide ; et celle de droite ?

---

<sup>1</sup> Laboratoire Dieudonné, UMR CNRS 7351, Université de Nice-Sophia Antipolis, France.



FIG. 2. Une structure de barres et pivots en 3D. La théorie reste incomplète dans ce cas.

la géométrie algébrique à la théorie des graphes, aux probabilités et à la physique. Nous rencontrerons de beaux théorèmes, pas toujours difficiles à démontrer, mais surtout beaucoup plus de questions ouvertes que de problèmes résolus. La théorie de la rigidité dont il sera question ici est un domaine vivant et varié, auquel il ne sera pas véritablement rendu justice : en effet, cet article se concentrera sur les aspects probabilistes du problème.

Pour simplifier, et c'est ce que nous ferons dans la plus grande partie de l'article, nous avons considéré une structure de barres et de pivots en deux dimensions. Il est clair qu'on peut imaginer beaucoup de problèmes analogues, décrivant d'autres situations : par exemple une structure de barres et de pivots en trois dimensions, comme à la figure 2 ; ou une structure, en deux ou trois dimensions, dans laquelle les pivots seraient remplacés par des corps solides ; on peut aussi imaginer qu'en plus de la contrainte de distance (une barre fixe la distance entre deux pivots), l'angle entre deux barres adjacentes au même pivot soit fixé.

Ce dernier exemple n'est pas choisi au hasard : la longueur d'une liaison chimique entre deux atomes, ainsi que l'angle entre deux liaisons adjacentes peuvent parfois être considérés comme constants. Cette idée est à l'origine de l'utilisation de la théorie de la rigidité pour étudier certains verres, comme ceux constitués d'alliages Germanium-Selenium [3, 4, 5, 6], en proportion respective  $x$  et  $1 - x$ . Un tel alliage est noté  $Ge_xSe_{1-x}$ . Dans la phase vitreuse, l'arrangement des atomes est irrégulier ; néanmoins, chaque atome de Germanium forme toujours 4 liaisons et chaque atome de Selenium en forme 2. Les atomes de Germanium sont donc à l'origine de plus de contraintes de longueur et angulaires, et on peut imaginer que, de déformable pour  $x$  petit, la structure devienne rigide pour  $x$  plus grand.

L'exemple des verres covalents détaillé ci-dessus présente deux caractéristiques : le nombre de barres et de joints dans une structure peut être gigantesque, au point qu'on ne peut espérer la décrire entièrement ; l'organisation des liaisons dans un matériau vitreux n'est pas régulière, si bien qu'il est naturel de la représenter en utilisant une part d'aléatoire. Dans la suite, nous nous intéresserons surtout à la rigidité sous cet angle probabiliste. La question posée alors n'est plus « est-ce que la structure dans son ensemble est rigide ou déformable », mais plutôt « est-ce qu'il existe une grande sous-structure rigide » (« grande » pouvant signifier par exemple « de taille comparable à la structure entière »), et « existe-t-il un seuil

pour l'apparition de cette grande structure rigide? » On étudie donc dans ce cas la « percolation de la rigidité » : ce concept est expliqué plus bas.

Je commence par poursuivre la description intuitive de la rigidité des structures de barres et de joints, remettant à plus tard définitions et théorèmes.

## 2. Comptage des contraintes

On attribue à James Clerk Maxwell [1] (connu avant tout par ses travaux sur l'électromagnétisme et la théorie cinétique des gaz) l'idée suivante, simple mais fondamentale : pour savoir si une structure est rigide ou déformable, il suffit en première approximation de compter les degrés de liberté et les contraintes. En deux dimensions, un pivot apporte deux degrés de liberté : en effet, sa position dans le plan est fixée par la donnée de ses deux coordonnées ; et une barre apporte une contrainte : sa longueur est donnée et fixe la distance entre deux pivots. Par ailleurs, une structure rigide a trois degrés de liberté : deux translations et une rotation. Si on note  $n$  le nombre de pivots et  $m$  le nombre de barres, on obtient donc l'alternative (incorrecte, on va le voir) :

$$\begin{aligned} \text{si } m < 2n - 3 & \quad \text{la structure est déformable} \\ \text{si } m \geq 2n - 3 & \quad \text{la structure est rigide.} \end{aligned}$$

Cette idée se généralise aux autres problèmes de rigidité : pour des barres et des pivots en trois dimensions par exemple, il suffit de remplacer  $2n - 3$  par  $3n - 6$ . Si les angles entre barres adjacentes sont fixés, il y a en trois dimensions  $2m - 3$  contraintes angulaires autour d'un pivot relié à  $m$  barres. Il est donc possible de compter les degrés de liberté et les contraintes dans un alliage  $\text{Ge}_x\text{Se}_{1-x}$  avec  $n$  atomes :

$$\begin{aligned} \text{degrés de liberté} &= 3n \\ \text{contraintes de longueur} &= 2nx + n(1-x) \\ \text{contraintes angulaires} &= 5nx + n(1-x). \end{aligned}$$

En faisant le bilan, on conclut que le nombre de contraintes est supérieur au nombre de degrés de liberté si  $x \geq 0.2$ , et inférieur sinon. Cette théorie très simple est en partie confirmée par les expériences puisque des changements de propriétés du matériau sont détectés autour de la valeur critique  $x = 0.2$  [6].

Le comptage des contraintes permet aussi de mettre en valeur une grande idée : décider de la rigidité d'une structure de barres et de joints est a priori un problème géométrique, ou de géométrie algébrique : on étudie les solutions d'un système d'équations polynomiales, exprimant que les barres ont une longueur fixée ; or le comptage des contraintes le transforme en un problème de mathématiques discrètes, de théorie des graphes. Dans ce cas, c'est même un problème de théorie des graphes particulièrement simple : il suffit de compter les sommets (pivots) et les arêtes (barres). En réalité, le comptage des contraintes n'est pas correct, la figure 3 donne un contre-exemple ; néanmoins, on va voir que dans certains cas, ce programme de réduction de la rigidité à un problème de théorie des graphes peut être mené à bien.

Pourquoi le comptage des contraintes ne fonctionne-t-il pas sur la structure de la figure 3 ? On voit que la structure contient une contrainte « redondante », que l'on

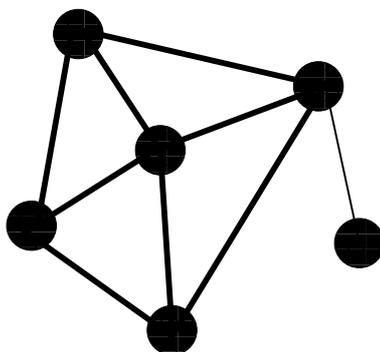


FIG. 3. Un assemblage avec  $n = 6$  boules et  $m = 2n - 3$  barres, qui n'est pas rigide. On peut enlever n'importe laquelle des barres en trait épais sans modifier ses propriétés de rigidité.

peut enlever sans changer les déformations possibles. Si on enlève cette contrainte redondante, le comptage redevient correct. La question devient donc « comment identifier les contraintes redondantes ? » Clairement, si une structure contient  $n$  pivots et strictement plus que  $2n - 3$  barres, elle contient au moins une contrainte redondante. On peut espérer que la réciproque soit vraie : si une structure contient une contrainte redondante, alors elle contient une sous-structure avec  $n$  pivots et strictement plus que  $2n - 3$  barres. C'est en effet une idée correcte pour les structures de barres et de pivots en deux dimensions, sous certaines hypothèses de généralité : c'est l'objet du célèbre théorème de Laman [2].

### 3. Théorème de Laman

On considère des graphes  $G = (V, E)$ , où  $V = (v_1, \dots, v_n)$  (avec  $n \geq 3$ ), et  $E \subset V \times V$ .  $V$  est l'ensemble des sommets du graphe,  $E$  l'ensemble des arêtes (toutes les arêtes sont distinctes, et une arête ne peut pas connecter un sommet à lui-même).

Une structure est une réalisation du graphe, c'est-à-dire la donnée du graphe et d'une application  $\varphi : V \rightarrow \mathbb{R}^2$  qui associe un point du plan à chaque sommet du graphe ; les longueurs des arêtes  $(l_e)_{e \in E}$  sont alors fixées. La réalisation  $(G, \varphi)$  est rigide si les déplacements des sommets du graphe qui préservent toutes les longueurs  $(l_e)$  préservent aussi toutes les distances entre sommets du graphe qui ne sont pas reliés par des arêtes.

**Définition 3.1.** On appelle graphe de Laman un graphe  $G$  avec  $n$  sommets et  $2n - 3$  arêtes, tel que tout sous-graphe de  $G$  contenant  $n'$  sommets contienne au plus  $2n' - 3$  arêtes.

**Remarque 3.2.** Un graphe de Laman possède donc juste assez d'arêtes pour être rigide, et aucun sous-graphe avec « trop d'arêtes ».

**Théorème 3.3.** (Laman) Un graphe de Laman admet une réalisation rigide.

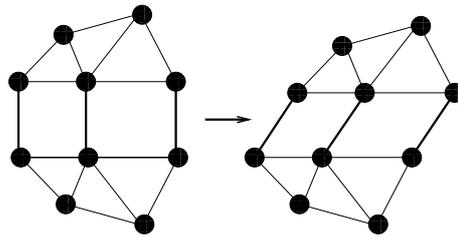


FIG. 4. La structure représentée est associée à un graphe de Laman. On voit néanmoins qu'elle est déformable : la déformation représentée conserve la longueur de chaque barre, mais pas les distances entre chaque paire de sommets. Les 3 barres en gras sont parallèles, ce qui contredit l'hypothèse de généricité nécessaire pour appliquer le théorème de Laman.

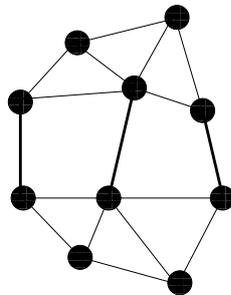


FIG. 5. La structure représentée est associée au même graphe de Laman que la structure de la figure 4, mais elle satisfait à l'hypothèse de généricité ; elle est rigide.

En fait, une réalisation « générique » d'un graphe de Laman est rigide, et une réalisation particulière peut ne pas l'être. Les figures 4 et 5 illustrent cet aspect. La figure 4 montre une structure associée à un graphe de Laman, contredisant l'hypothèse de généricité ; elle est déformable. La figure 5 montre une structure associée au même graphe de Laman, mais satisfaisant à l'hypothèse de généricité ; elle est rigide. Une condition suffisante de généricité est que les coordonnées des pivots soient algébriquement indépendantes sur les rationnels.

La démonstration du théorème de Laman est assez élémentaire : elle repose sur la linéarisation des contraintes de longueurs, et des considérations d'algèbre linéaire.

Il peut sembler naturel de conjecturer des généralisations du théorème de Laman aux autres problèmes de rigidité : on sait que cela ne marche pas toujours, notamment dans le cas des structures de barres et de pivots en trois dimensions illustré par la figure 2.

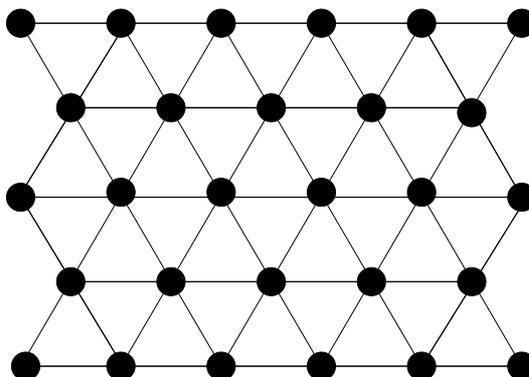


FIG. 6. Un réseau triangulaire.

## 4. Percolation de la rigidité

### 4.1. Graphes aléatoires et percolation

On se place dorénavant dans le cadre de la rigidité générique : le théorème de Laman nous permet donc de transformer le problème original en un problème de théorie des graphes.

Motivés notamment par les applications potentielles en physique, nous nous intéressons à de très grands graphes, dont la définition contient une part aléatoire.

**Exemple 1.** À partir du réseau triangulaire représenté sur la figure 6, on définit pour chaque  $p \in [0, 1]$  un réseau aléatoire en associant à chaque arête une variable de Bernoulli de paramètre  $p$ ; ces variables sont indépendantes. Une arête est considérée comme « présente » si la variable associée vaut 1, et absente sinon.

**Exemple 2.** Un graphe aléatoire de type Erdős-Renyi, noté  $\mathcal{G}(n, \frac{c}{n})$  : c'est un graphe à  $n$  sommets, où chacune des  $n(n-1)/2$  arêtes est présente avec probabilité  $c/n$ .

En percolation classique, on s'intéresse aux composantes connexes de ces graphes, dans la limite où la taille des graphes tend vers l'infini. Par exemple, on pose les questions : existe-t-il un seuil  $p^*$  (exemple 1) ou  $c^*$  (exemple 2) pour l'apparition d'une composante connexe comportant une fraction finie des sommets du graphe? Cette composante connexe « géante » est-elle unique? Dans ce cas, quelle est sa taille?

Ici, on s'intéresse aux composantes rigides, et on pose les mêmes questions : existe-t-il un seuil  $p^*$  (exemple 1) ou  $c^*$  (exemple 2) pour l'apparition d'une composante rigide comportant une fraction finie des sommets du graphe? Cette composante rigide « géante » est-elle unique? Quelle est sa taille? Par analogie avec la percolation classique, ce problème est appelé « percolation de la rigidité ».

## 4.2. Graphes aléatoires de type Erdős-Renyi

De façon peut-être un peu contre-intuitive, la percolation de la rigidité sur les graphes de type Erdős-Renyi est beaucoup plus abordable que sur des réseaux triangulaires (exemple 1). Récemment, Kasiviswanathan, Moore et Thérant ont obtenu le résultat suivant (« avec grande probabilité » signifie « avec une probabilité » qui tend vers 1 quand la taille du graphe  $n$  tend vers l'infini) :

**Théorème 4.1.** *Il existe un seuil  $c^* = 3.588 \dots$  tel que :*

- si  $c < c^*$ , alors avec grande probabilité les composantes rigides de  $G(n, \frac{c}{n})$  contiennent 1, 2 ou 3 sommets;
- si  $c > c^*$ , alors avec grande probabilité  $G(n, \frac{c}{n})$  contient une unique composante rigide géante, de taille proportionnelle à  $n$ . De plus, la fraction de pivots appartenant à la plus grande composante rigide est discontinue en  $c^*$ ; on dit que la transition est du premier ordre.

La démonstration repose sur le lien entre rigidité et « orientabilité ». Un graphe est dit  $k$ -orientable s'il existe une orientation des arêtes telle que chaque site ait un degré entrant au plus  $k$  (i.e. au plus  $k$  arêtes sont orientées vers lui). On peut donner à cette procédure d'orientation des arêtes une interprétation physique : une arête retire un degré de liberté au site vers lequel elle est orientée; lorsque chaque site a deux degrés de liberté pour modéliser la rigidité en dimension 2, il est logique que rigidité et 2-orientabilité soient reliées. Kasiviswanathan et al. démontrent donc que le seuil au-delà duquel un graphe n'est plus 2-orientable coïncide avec le seuil d'apparition d'une composante rigide géante. La valeur de ce seuil  $3.588 \dots$  avait été calculée précédemment [19, 20], en analysant des algorithmes construisant une 2-orientation. Les démonstrations précises sont assez longues ([19, 20] sont des « résumés détaillés » omettant une partie des preuves).

En réalité, il s'agit d'une démonstration de résultats qui avaient été intuités par les physiciens il y a une quinzaine d'années [9, 10], grâce à l'utilisation de méthodes heuristiques, qui s'appuyaient sur le fait qu'un graphe  $G(n, \frac{c}{n})$  ressemble localement à un arbre, et étudiaient la « propagation de la rigidité » dans cet arbre.

Il est instructif de détailler un peu cette heuristique. Notons  $U_n^{(c)}$  la variable aléatoire qui compte dans un graphe  $G(n, \frac{c}{n})$  le nombre de contraintes redondantes. On note  $E_n^{(c)} = \mathbb{E}(U_n^{(c)})$ . On cherche à étudier

$$e(c) = \lim_{n \rightarrow \infty} \frac{E_n^{(c)}}{n}.$$

On introduit maintenant un couplage entre  $U_n^{(c)}$  et  $U_{n+1}^{(c)}$ . En partant d'un graphe  $G_n$  de loi  $G(n, \frac{c}{n})$ , on ajoute un sommet, et on le relie aux sommets de  $G_n$  avec probabilité  $c/n$ ; on retire ensuite chacune des arêtes avec probabilité  $1/(n+1)$ . Un peu de réflexion montre que le graphe  $G_{n+1}$  construit ainsi est de loi  $G(n+1, \frac{c}{n+1})$ . On note  $\Delta U_{n,s}^{(c)}$  et  $\Delta U_{n,a}^{(c)}$  les variables aléatoires qui comptent la variation du nombre de contraintes redondantes lors des processus d'addition de site ou de retrait d'arêtes utilisés ici. On a donc

$$U_{n+1}^{(c)} \text{ de même loi que } U_n^{(c)} + \Delta U_{n,s}^{(c)} + \Delta U_{n,a}^{(c)}.$$

En prenant l'espérance

$$E_{n+1}^{(c)} - E_n^{(c)} = \mathbb{E}(\Delta U_{n,s}^{(c)}) + \mathbb{E}(\Delta U_{n,a}^{(c)}).$$

En supposant que le membre de droite de la dernière équation a une limite quand  $n$  tend vers l'infini, on en déduit

$$\lim_{n \rightarrow \infty} \frac{E_n^{(c)}}{n} = \lim_{n \rightarrow \infty} \left( \mathbb{E}(\Delta U_{n,s}^{(c)}) + \mathbb{E}(\Delta U_{n,a}^{(c)}) \right).$$

On calcule maintenant les espérances de l'expression ci-dessus en utilisant le fait que les graphes  $G(n, \frac{c}{n})$  ressemblent localement à des arbres. Ainsi, lorsqu'on ajoute par exemple une arête, on peut considérer sous certaines conditions que les 2 sommets qu'elle joint étaient « indépendants » avant l'adjonction de la nouvelle arête. Il est alors possible de calculer assez explicitement la fonction  $e(c)$  ; on voit que  $e(c) = 0$  si  $c \leq c^* = 3.588\dots$ , et  $e(c) > 0$  si  $c > c^*$ .

Cette heuristique est un exemple d'utilisation de la très puissante « méthode de la cavité » [15], qui permet d'obtenir (sans preuve) des résultats beaucoup plus forts, par exemple des fonctions de grandes déviations pour la variable aléatoire  $U_n^{(c)}$  [13, 14]. Malheureusement, les preuves données dans [19, 20] sont assez éloignées de l'heuristique des physiciens. Il est donc intéressant de noter que le récent article [21] introduit une nouvelle preuve, beaucoup plus proche de l'heuristique donnée ci-dessus : les autres résultats en percolation de la rigidité utilisant la méthode de la cavité sont donc peut-être accessibles à une démonstration. Notons que la méthode de la cavité a permis aux physiciens d'étudier des problèmes bien plus difficiles que celui-ci (de type « verres de spin » par exemple [16]), et d'obtenir (répétons-le, sans preuve rigoureuse) de très nombreux résultats en optimisation combinatoire : rendre rigoureux ces raisonnements heuristiques est donc une question qui dépasse très largement le cadre de la rigidité [22].

### 4.3. Réseau triangulaire

En ce qui concerne le problème sur réseau triangulaire, la situation est beaucoup moins favorable. Quelques résultats ont été obtenus par A. Holroyd [17].

**Théorème 4.2.** (Holroyd) *On considère un réseau triangulaire infini, dans lequel chaque arête est présente avec probabilité  $p$ , les arêtes étant indépendantes. Alors il existe un seuil  $p^* \in ]0, 1[$  tel que :*

- i) si  $p < p^*$ , avec probabilité 1 le réseau ne contient pas de composante rigide infinie ;*
- ii) si  $p > p^*$ , avec probabilité 1 le réseau contient une unique composante rigide infinie, sauf peut-être pour un ensemble au plus dénombrable de valeurs de  $p$ .*

Notons que ce théorème nécessite l'extension de la notion de rigidité à des structures infinies, et que la restriction étrange sur les valeurs de  $p$  dans le domaine  $p > p^*$  est presque certainement un problème technique.

Malgré cette avancée, nous sommes encore extrêmement loin d'avoir une compréhension de la transition similaire à celle de la percolation standard, où « composante connexe » remplace « composante rigide ». Les physiciens ont réalisé des simulations numériques, qui semblent indiquer que la percolation de la rigidité en deux dimensions est « du deuxième ordre », c'est-à-dire que la

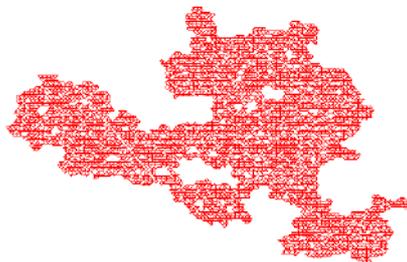


FIG. 7. Une réalisation de la plus grande composante rigide dans un réseau triangulaire de taille  $200 \times 200$  ; chaque arête est présente avec probabilité  $p \simeq 0.656$ , ce qui est proche du seuil de percolation de la rigidité, estimé numériquement.

fraction de pivots appartenant à la plus grande composante rigide est certes une fonction singulière en  $p^*$ , mais continue. La transition est donc fondamentalement différente de celle sur graphe Erdős-Rényi, et très mal connue. La figure 7 montre un exemple de simulation sur réseau triangulaire.

#### 4.4. Renormalisation

Pour aller plus loin, nous allons utiliser une approche de type « renormalisation ». L'idée est de transformer le problème de la rigidité sur une famille de graphes  $G$  décrits par une loi de probabilité  $\mathcal{P}$  en un problème équivalent sur une famille de graphes plus petits, décrits par une loi de probabilité  $\tilde{\mathcal{P}}$ . On peut ensuite étudier la transformation  $\mathcal{P} \mapsto \tilde{\mathcal{P}}$  et ses itérées successives pour comprendre le problème originel. Cette transformation est en général compliquée ; on va analyser certains cas où elle est simple.

Considérons le graphe  $G$ , de la figure 8. Appelons  $H$  le sous-graphe en tireté ; son intersection avec le reste du graphe est réduite aux deux sommets  $A$  et  $B$ . Par ailleurs, si on considère le sous-graphe  $H$  tout seul, les sommets  $A$  et  $B$  n'appartiennent pas à la même composante rigide. Notons que  $A$  et  $B$  appartiennent à la même composante rigide dans  $G$ , mais pas dans  $H$  seul. On construit maintenant le graphe « renormalisé »  $\tilde{G}$  de la façon suivante :

- (1) si  $A$  et  $B$  appartiennent à la même composante rigide dans  $H$ , on remplace tout le sous-graphe  $H$  par les sommets  $A$ ,  $B$  et une arête les reliant ;
- (2) si  $A$  et  $B$  n'appartiennent pas à la même composante rigide dans  $H$ , on supprime tout le sous-graphe  $H$ , sauf les sommets  $A$  et  $B$  : c'est le cas sur la figure 8 ;
- (3) on ne touche pas au reste du graphe  $G$ .

On peut renormaliser une nouvelle fois le graphe obtenu en considérant le sous-graphe en gras, dont l'intersection avec le reste du graphe est réduite aux sommets

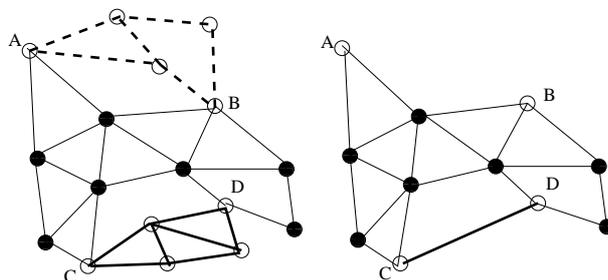


FIG. 8. Les sous-graphes en tireté et en gras ont chacun une intersection avec le reste du graphe réduite à deux sommets. Par l'opération de renormalisation, le sous-graphe en gras est remplacé par une arête ; le sous-graphe en tireté est simplement supprimé. On peut étudier la rigidité du graphe originel sur le graphe « renormalisé ».

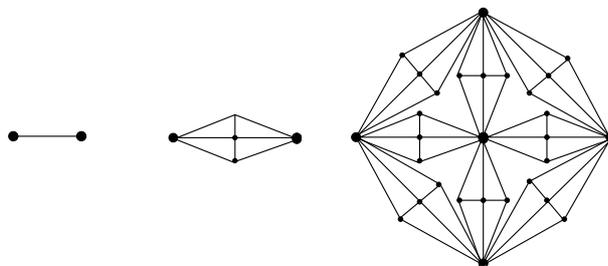


FIG. 9. Construction d'un graphe hiérarchique : à chaque étape, chaque lien est remplacé par une « cellule élémentaire ».

$C$  et  $D$ . Le sous-graphe en gras est remplacé par les sommets  $C$  et  $D$  et une arête les reliant, comme indiqué figure 8.

Il n'est pas difficile de voir que les propriétés de rigidité du graphe  $G$  se transfèrent au graphe renormalisé  $\tilde{G}$ . En particulier, si  $I$  et  $J$  sont deux sommets de  $G$  qui ne sont pas dans  $H$ ,  $I$  et  $J$  appartiennent à la même composante rigide dans  $G$  si et seulement si ils appartiennent à la même composante rigide dans  $\tilde{G}$ . On pourrait également relier le nombre de contraintes redondantes des graphes  $G$  et  $\tilde{G}$ . On peut donc maintenant étudier la rigidité du graphe plus petit,  $\tilde{G}$ . Bien sûr, cette procédure de « renormalisation » ne fonctionne que tant qu'on peut trouver des sous-graphes dont l'intersection avec le graphe principal est réduite à deux sites ; elle ne permet donc pas de réduire la complexité du réseau de percolation triangulaire. En revanche, on peut raisonner dans l'autre sens : il est possible de construire un graphe de telle sorte que la procédure de renormalisation permette de résoudre complètement le problème ! Un exemple de tels graphes, appelés graphes hiérarchiques, est représenté figure 9 ; ces graphes ont été introduits à la fin des années 1970 pour étudier d'autres types de transitions de phase [18].

On met sur ce graphe hiérarchique une distribution des arêtes « de Bernoulli » : chaque arête est présente avec probabilité  $p$ , et les arêtes sont indépendantes entre

elles. Pour une cellule élémentaire fixée, on note  $R_{k,p}$  le graphe construit par distribution de Bernoulli de paramètre  $p$  sur le graphe hiérarchique de niveau  $k$  : il s'agit en fait d'une famille de graphes décrite par une loi de probabilité. On applique alors la procédure de renormalisation détaillée ci-dessus à chaque cellule de dernière génération de  $R_{k,p}$ . On fait assez facilement les constatations suivantes :

- (1) la procédure de renormalisation appliquée à chaque cellule élémentaire transforme un graphe hiérarchique de niveau  $k$  en un graphe hiérarchique de niveau  $k - 1$  ;
- (2) dans le graphe renormalisé, les arêtes sont indépendantes entre elles ;
- (3) chaque arête est présente sur le graphe renormalisé avec probabilité  $\varphi(p)$ , où  $\varphi$  est une fonction de  $[0, 1]$  dans  $[0, 1]$  qui dépend de la cellule élémentaire ;  $\varphi$  peut-être calculée explicitement sans difficulté.

On en conclut qu'une étape de renormalisation transforme la famille de graphes  $R_{k,p}$  en la famille  $R_{k-1,\varphi(p)}$ . Dans ce cas particulier, la nouvelle loi de probabilité après renormalisation est très simple : le graphe conserve la même structure ; les arêtes restent indépendantes ;  $p$  est transformé en  $\varphi(p)$ .

Pour analyser un graphe  $R_{k,p}$  avec  $k$  grand, on répète cette étape de renormalisation et on voit apparaître la suite récurrente  $(p_t)_{t \in \mathbb{N}}$ , qui décrit une probabilité « effective » de présence d'une arête à l'étape  $t$  :

$$p_0 = p ; p_{t+1} = \varphi(p_t).$$

Les propriétés de rigidité du graphe  $R_{k,p}$  se lisent sur ce système dynamique très simple. En particulier, pour la cellule élémentaire de la figure 9,  $\varphi$  a deux points fixes stables  $p = 0$  et  $p = 1$ , et un point fixe instable  $p^*$  ;  $p^*$  est un seuil :

- si  $p > p^*$ , le graphe contient une composante rigide « géante » avec probabilité qui tend vers 1 quand  $k$  tend vers l'infini ;
- si  $p < p^*$ , le graphe ne contient pas de composante rigide géante avec probabilité qui tend vers 1 quand  $k$  tend vers l'infini.

De plus, les quantités reliées à la rigidité, comme le nombre de contraintes redondantes (ou plutôt l'espérance de ce nombre), présentent une singularité en  $p = p^*$ .

Notons que cette stratégie de renormalisation n'est pas limitée au problème de la rigidité des barres et des joints, mais fonctionne aussi sur d'autres problèmes de rigidité [23] ; en revanche, de nouvelles idées sont nécessaires pour le cas du réseau triangulaire, ou pour d'autres réseaux réguliers.

## 5. Conclusion

J'espère avoir montré dans cet article que la compréhension de la percolation de la rigidité est très incomplète, et que le domaine comporte beaucoup plus de problèmes ouverts que de questions résolues : cet aspect devrait la rendre attirante pour les chercheurs, mathématiciens ou physiciens.

Pour conclure, j'ajouterais que la théorie de la rigidité en général est aussi un formidable terrain de vulgarisation scientifique et d'initiation à la recherche, pour tous niveaux : les questions posées sont simples et naturelles, le concept est accessible même pour de jeunes enfants, le comptage des contraintes au collège ou au lycée, et le théorème de Laman en Master, voire Licence.

## 6. Références

- [1] J.C. Maxwell « On the calculation of the equilibrium and stiffness of frames » *Philosophical Magazine Series 4*, Jan 1864.
- [2] G. Laman « On graphs and rigidity of plane skeletal structures », *J. Eng. Math.* **4**, 331 (1970).
- [3] J.C. Phillips « Topology of covalent non-crystalline solids I : Short-range order in chalcogenide alloys », *J. Non-Cryst. Solids* **34**, 153 (1979).
- [4] M.F. Thorpe « Continuous deformations in random networks », *J. Non-Cryst. Solids* **57**, 355 (1983).
- [5] H. He and M. F. Thorpe « Elastic properties of glasses », *Phys. Rev. Lett.* **54**, 2107 (1985)
- [6] P. Boolchand, X. Feng, D. Selvanathan and W.J. Bresser « Rigidity transition in chalcogenide glasses », in *Rigidity theory and applications*, Eds. M.F. Thorpe and P. Duxbury, Kluwer (1999).
- [7] D.J. Jacobs and M.F. Thorpe « Generic rigidity percolation : the pebble game », *Phys. Rev. Lett.* **75**, 4051 (1995).
- [8] C. Moukarzel and P.M. Duxbury « Stressed backbone and elasticity of random central-force systems », *Phys. Rev. Lett.* **75**, 4055 (1995).
- [9] C. Moukarzel, P. M. Duxbury and P. L. Leath « First-order rigidity on Cayley trees », *Phys. Rev. E* **55**, 5800 (1997).
- [10] P.M. Duxbury, D.J. Jacobs, M.F. Thorpe and C. Moukarzel « Floppy modes and the free energy : Rigidity and connectivity percolation on Bethe lattices », *Phys. Rev. E* **59**, 2084 (1999).
- [11] L. Thérán « Rigid components of random graphs », in Proc. of the 21st Canadian Conference on Computational Geometry, Vancouver, BC, 2009.
- [12] S. P. Kasiviswanathan, C. Moore and L. Thérán « The rigidity transition in random graphs » in SODA '11, 1237 (2011).
- [13] O. Rivoire and J. Barré « Exactly solvable models of adaptive networks » *Phys. Rev. Lett.* **97**, 148701 (2006).
- [14] J. Barré, A. Bishop, T. Lookman and A. Saxena « Random bond models of the intermediate phase in network forming glasses » in « Rigidity and Boolchand intermediate phases in nanomaterials », Eds. M. Micoulaut, M. Popescu, INOE Publishing House (2009).
- [15] M. Mézard et G. Parisi, *J. Stat. Phys.* **111**, 1 (2003).
- [16] M. Mezard, G. Parisi et M. A. Virasoro, « Spin glass theory and beyond », World Scientific (1987).
- [17] A. E. Holroyd « Existence and Uniqueness of Infinite Components in Generic Rigidity Percolation », *The Annals of Applied Probability* **8**, 944 (1998).
- [18] A.N. Berker and S. Ostlund « Renormalisation-group calculations of finite systems : order parameter and specific heat for epitaxial ordering » *J. Phys C* **12**, 4961 (1979).
- [19] D. Fernholz and V. Ramachandran « The k-orientability thresholds for  $G(n, p)$  », in SODA'07, 459 (2007).
- [20] J. A. Cain, P. Sanders, and N. Wormald « The random graph threshold for k-orientability and a fast algorithm for optimal multiple-choice allocation », in SODA'07, 469 (2007).
- [21] M. Lelarge « A new approach to the orientation of random hypergraphs », in SODA '12, 251 (2012).
- [22] J. Salez, Quelques conséquences de la convergence locale faible pour les graphes aléatoires, thèse de doctorat (2011).
- [23] J. Barré « Combinatorial models of rigidity and renormalization », *J. Stat. Phys.* **146**, 359-377 (2012).
- [24] J. Barré « Hierarchical models of rigidity percolation », *Phys. Rev. E* **80**, 061108 (2009).

**Remerciements.** *Je remercie vivement J. Buzzi, T. Barbot et J. Melleray pour leur relecture très attentive, leurs nombreuses suggestions et leurs encouragements. Je remercie aussi tous mes collaborateurs passés et présents sur ce sujet passionnant.*

# Électrons en interaction dans un milieu aléatoire

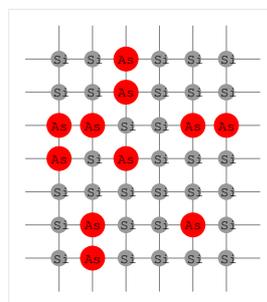
Frédéric Klopp<sup>1</sup>

## 1. Introduction

La physique de la matière condensée est la source de nombreux problèmes mathématiques intéressants et, souvent, difficiles. Tous les domaines mathématiques sont concernés, l'algèbre, la théorie des nombres, l'analyse, et les probabilités. Dans ce texte, je vais présenter un modèle simple pour des électrons en interaction dans un milieu aléatoire et décrire l'état fondamental d'un tel système, c'est-à-dire, son état d'équilibre à température nulle. Les questions que nous évoquerons seront essentiellement du ressort de l'analyse et des probabilités. Avant de décrire le modèle qui va nous intéresser au premier chef, parlons un peu des questions de physique dont il est issu.

Le problème du transport des électrons dans les solides est l'une des questions de physique de la matière condensée les plus anciennes; c'est aussi l'une des plus actuelles. En 1900, l'un des premiers modèles, celui de Drude ([2]) traitait les électrons comme des particules classiques... la mécanique quantique n'était pas encore inventée! Dans ce modèle, les interactions à distance étaient négligées ainsi que celles avec le milieu ambiant.

Avec l'avènement de la mécanique quantique, les électrons devinrent des ondes régies par l'équation de Schrödinger. Le vide fut remplacé par un milieu d'abord supposé périodique, un empilement périodique d'atomes supposés immobiles dans lequel se déplacent les électrons. On commença par étudier les modèles à une particule c'est-à-dire que l'on négligea les interactions entre les électrons. Avec les avancées technologiques et la création



de nouveaux matériaux, en particulier, les semi-conducteurs, les milieux dans lesquels on chercha à comprendre la conduction électrique se firent plus compliqués : on introduisit la notion de milieux aléatoires ou solides désordonnés ([1]).

Dans le même temps, on prit en compte les interactions entre les électrons ainsi que d'autres interactions avec le milieu ambiant que le seul potentiel électrostatique (phonons, etc.).

<sup>1</sup> Sorbonne Universités, UPMC, UMR 7586, IMJ-PRG, F-75005, Paris – Univ. Paris Diderot, Sorbonne Paris Cité, UMR 7586, IMJ-PRG, F-75205 Paris – CNRS, UMR 7586, IMJ-PRG, F-75005, Paris, France.

## 2. Les milieux désordonnés et la localisation : un modèle simplifié

Les milieux solides qui nous intéressent sont des solides désordonnés. Ils sont de bons modèles pour de nombreux matériaux réels comme les semi-conducteurs, certains alliages, etc. (voir [9]). L'un des exemples les plus simples de solides désordonnés est celui des alliages : on considère un substrat cristallin dont l'ordonnement est périodique (voir la figure 1). On substitue alors certains des atomes par des impuretés (voir la figure 2). Macroscopiquement, on ne connaît pas la position exacte des atomes substitués mais seulement leur statistique ; par exemple, on sait qu'un atome sur deux a été échangé. On parle alors de potentiel ou milieu aléatoire au sens où le milieu est une réalisation d'un processus aléatoire.

Le modèle concret qui va nous occuper est d'une nature un peu différente. Le milieu aléatoire est unidimensionnel et constitué d'une suite d'intervalles contigus de longueurs aléatoires que l'on appellera « pièces ». La distribution des points délimitant les pièces est poissonnienne d'intensité 1, i.e., les points délimitant les pièces sont le support d'un processus de Poisson d'intensité 1. Ceci peut se décrire de la façon suivante (voir aussi la

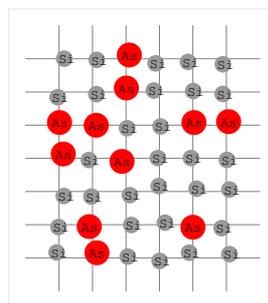


FIG. 2. Un exemple de solide désordonné

partie 2.1.2) : pour  $L$  grand, avec une excellente probabilité,

- le nombre de pièces dans l'intervalle  $[0, L]$  est égal à  $L$  à une petite erreur relative près,
- les longueurs des pièces sont distribuées identiquement et suivent une loi exponentielle de paramètre 1 à une petite erreur près,
- les longueurs des pièces sont stochastiquement indépendantes.

### 2.1. Un modèle très simple de milieu aléatoire

Avant de définir notre modèle très simple de milieu aléatoire, le modèle de Luttinger-Sy, rappelons quelques éléments utiles sur le laplacien de Dirichlet sur un intervalle.

#### 2.1.1. Le laplacien de Dirichlet sur un intervalle

Soit  $I = [0, \ell]$  ( $\ell > 0$ ), un intervalle, et considérons le problème aux valeurs propres suivant

$$(2.1) \quad \begin{cases} -\frac{d^2}{dx^2} \varphi(x) = \lambda \varphi(x), & x \in I, \\ \varphi(0) = \varphi(\ell) = 0. \end{cases}$$

La question est donc l'existence de solutions  $(\lambda, \varphi)$  où  $\lambda$  est un nombre complexe et  $\varphi$  une fonction deux fois différentiable à valeurs complexes, non identiquement nulle, solution de (2.1). Le problème (2.1) étant linéaire, à chaque valeur propre  $\lambda$  est associé un espace vectoriel de fonctions propres  $\varphi$ .

Le calcul explicite des solutions de l'équation différentielle  $\varphi'' + \lambda\varphi = 0$  montre que le problème aux valeurs propres (2.1) a pour solutions les couples  $(\lambda_k, \psi_k)$  tels que

$$(2.2) \quad \lambda_k = \frac{(k\pi)^2}{\ell^2} \quad \text{et} \quad \psi_k \in \text{Vect}(\varphi_k) = \mathbb{C}\varphi_k \quad \text{où} \quad \varphi_k(x) = \frac{1}{\sqrt{2\ell}} \sin\left(\frac{\pi k x}{\ell}\right)$$

lorsque  $k$  parcourt les entiers naturels non nuls.

La théorie des séries de Fourier (voir [5]) montre que la famille  $(\varphi_k)_{k \geq 1}$  forme une base orthonormée de  $L^2(I)$ , l'espace des fonctions de carré intégrable sur  $I$ .

On peut alors définir le laplacien de Dirichlet sur  $I$ , noté  $\Delta_I^D$ , comme l'opérateur (linéaire) dont la matrice (infinie) dans la base  $(\varphi_k)_{k \geq 1}$  est la matrice diagonale des éléments  $(-\lambda_k)_{k \geq 1}$ . Cet opérateur linéaire est non borné : il n'est pas défini sur tous les vecteurs de  $L^2(I)$ . Pour qu'un vecteur de  $L^2(I)$ , disons  $u$ , soit dans le domaine de  $\Delta_I^D$ , il faut et il suffit que ses coefficients dans la base  $(\varphi_k)_{k \geq 1}$ , disons  $(\hat{u}_k)_{k \geq 1}$ , vérifient  $\sum_{k \geq 1} |\lambda_k \hat{u}_k|^2 < +\infty$ . On vérifie alors que  $u$  est une fonction

continûment différentiable qui s'annule en 0 et en  $\ell$  et dont la dérivée seconde (au sens des distributions) est de carré intégrable sur  $[0, \ell]$ .

### 2.1.2. Le modèle de Luttinger-Sy

Dans  $\mathbb{R}$ , on considère un processus ponctuel de Poisson  $d\mu(\omega)$  d'intensité 1. Décrivons cette mesure aléatoire  $d\mu(\omega)$  plus rigoureusement que dans le début de la section 2. C'est une mesure ponctuelle qui affecte la masse unité à chacun des points de son support (i.e. cette mesure est une somme de masses de Dirac) telle que

- pour un intervalle  $I$ , la variable comptant le nombre de points tombés dans  $I$  suit une loi de Poisson de paramètre  $|I|$ , la mesure de Lebesgue de  $I$ ,
- les variables aléatoires comptant les points tombés dans des intervalles disjoints sont stochastiquement indépendantes.

Soit  $(x_k(\omega))_{k \in \mathbb{Z}}$  le support de  $d\mu(\omega)$  (i.e.,  $d\mu(\omega) = \sum_{k \in \mathbb{Z}} \delta_{x_k(\omega)}$ ), les points

$(x_k(\omega))_{k \in \mathbb{Z}}$  sont ordonnés de façon croissante.

Sur  $L^2(\mathbb{R})$ , on définit le modèle de Luttinger-Sy (ou modèle des pièces, voir [10, 11]) de la façon suivante. Pour  $L > 0$ , on définit l'intervalle  $\Lambda = \Lambda_L = ]0, L[$ . On considère les points de  $\{x_k(\omega); k \in \mathbb{Z}\}$  tombés dans  $\Lambda$  :

$$0 < x_{k_-}(\omega) < x_{k_-+1}(\omega) < \cdots < x_{k_+-1}(\omega) < x_{k_+}(\omega) < L$$

où  $k_- = \min\{k; x_k > 0\}$  et  $k_+ = \max\{k; x_k < L\}$ . Ces nombres sont aléatoires. On pose  $x_{k_- - 1} = 0$  et  $x_{k_+ + 1} = L$ . On définit alors la  $k$ -ième pièce comme  $\Delta_k(\omega) := ]x_k(\omega), x_{k+1}(\omega)[$ . Le modèle des pièces sur l'intervalle  $[0, L]$  est alors donné par la somme directe orthogonale suivante :

$$(2.3) \quad H_\omega(L) = H_\omega(\Lambda) = \bigoplus_{k_- - 1 \leq k \leq k_+} -\Delta_{\Delta_k(\omega)}^D.$$

Pour simplifier, dans la suite, on appelle  $m(\omega)$  le nombre de pièces dans  $[0, L]$  et on renumérote les pièces de 1 à  $m(\omega)$ . On sait qu'avec une très bonne probabilité, on a  $m(\omega) = L + O(L^{2/3})$ .

Sur la figure 3, on a représenté les pièces en abscisse et les énergies autorisées dans chaque pièce en ordonnée. Dans chaque pièce, les niveaux d'énergies autorisés pour les électrons sont quantifiés : ce sont les valeurs propres du laplacien de Dirichlet sur l'intervalle données par (2.2).

Il est clair que l'on peut définir la limite de  $H_\omega(L)$  quand  $L \rightarrow +\infty$  de la façon suivante :

$$(2.4) \quad H_\omega = \bigoplus_{k \in \mathbb{Z}} -\Delta_{\Delta_k(\omega)}^D.$$

C'est un opérateur essentiellement auto-adjoint sur  $L^2(\mathbb{R})$ . En utilisant les propriétés ergodiques du processus de Poisson, on vérifie simplement que le spectre de  $H_\omega$  ne dépend presque sûrement pas de  $\omega$ . De plus,  $H_\omega$  n'a pas de spectre continu : son spectre est constitué uniquement de valeurs propres. En effet,  $H_\omega$  s'écrit comme la somme directe d'opérateurs n'ayant que du spectre ponctuel. Enfin, la formule explicite des valeurs propres du laplacien de Dirichlet sur un intervalle (voir (2.2)) et la définition du processus de Poisson (voir la description des longueurs des pièces donnée juste avant la partie 2.1) montre que, les valeurs propres de  $H_\omega$  sont dans la demi-droite  $[0, +\infty[$ .

D'autre part, presque sûrement, les fonctions propres associées aux valeurs propres de  $H_\omega$  sont toutes à support compact : chaque fonction propre est associée à une pièce et elle est supportée dans cette pièce.

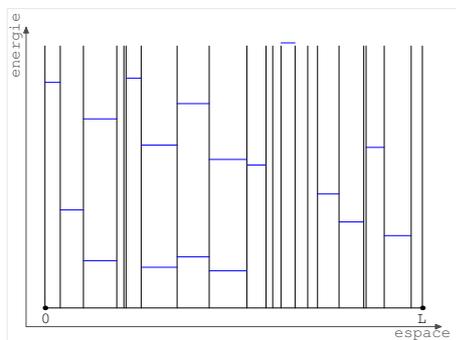


FIG. 3. Le milieu aléatoire et les niveaux d'énergie autorisés

Les propriétés que nous venons de voir pour le modèle de Luttinger-Sy (à savoir, que le spectre de l'opérateur aléatoire est purement ponctuel et que les valeurs propres sont associées à des vecteurs propres qui décroissent exponentiellement à l'infini) sont partagées par de nombreux modèles aléatoires ergodiques. Un modèle aléatoire ergodique est une famille d'opérateurs auto-adjoints munie d'une structure de probabilité et d'une relation permettant de transporter l'action d'une famille de transformations ergodiques sur la structure de probabilité en l'action d'une famille d'opérateurs unitaires. Ces modèles ont fait l'objet d'une étude systématique (voir, par exemple, [6, 4]). Il est démontré de façon très générale que le spectre ainsi que les composantes spectrales (les spectres purement ponctuel, absolument continu et singulier continu) sont les mêmes pour presque tous les éléments de la famille.

Le fait que le spectre soit purement ponctuel dans certaines régions d'énergie est appelé « localisation » : c'est un phénomène très général caractéristique de la propagation des ondes dans les milieux désordonnés qui ne se limite pas aux ondes

régies par l'équation de Schrödinger (voir [9]). La localisation a été démontrée mathématiquement pour de nombreux modèles aléatoires (voir [4]).

### 2.1.3. La densité d'états intégrée

La densité d'états intégrée du système est définie de la façon suivante. On fixe une énergie  $E$  et un intervalle de longueur  $L$ . Puis, on compte le nombre de niveaux d'énergie inférieure à  $E$  dans le système, i.e., le nombre de valeurs propres de l'opérateur inférieures à  $E$  par unité de volume. Enfin, on prend la limite  $L \rightarrow +\infty$ . Ainsi, pour  $E \in \mathbb{R}$ , on pose

$$N(E) = \lim_{L \rightarrow +\infty} \frac{\#\{\text{valeurs propres de } H_\omega(L) \text{ dans } ]-\infty, E]\}}{L}.$$

Pour le modèle de Luttinger-Sy, l'existence de cette limite découle de la loi des grands nombres. En effet, pour ce modèle, quand  $L \rightarrow +\infty$ , à une petite erreur près, on peut considérer les pièces comme des quantités aléatoires indépendantes; en particulier, leurs longueurs sont des variables aléatoires indépendantes suivant une distribution exponentielle de paramètre 1 (voir la description donnée juste avant la partie 2.1). La loi des grands nombres nous dit que, presque sûrement, le nombre de niveaux d'énergie de  $H_\omega(L)$  inférieurs à  $E$  est asymptotique au nombre de pièces multiplié par l'espérance du nombre de niveaux inférieurs à  $E$  contenus dans une pièce. Comme la longueur d'une pièce suit une loi exponentielle de paramètre 1, la description exacte du spectre d'une pièce (2.2) nous dit que la loi du nombre de niveaux sous  $E$  contenus dans une pièce est

$$\begin{aligned} \forall k \in \mathbb{N}, \quad & \mathbb{P} \left( \left\{ \begin{array}{l} \text{une pièce } \Delta \text{ contient exactement} \\ k \text{ niveaux inférieurs à l'énergie } E \end{array} \right\} \right) \\ &= \mathbb{P} \left( \left\{ \frac{(\pi k)^2}{|\Delta|^2} \leq E < \frac{(\pi(k+1))^2}{|\Delta|^2} \right\} \right) \\ &= \mathbb{P} \left( \left\{ \frac{k\pi}{\sqrt{E}} \leq |\Delta| < \frac{(k+1)\pi}{\sqrt{E}} \right\} \right) \\ &= \exp\left(-\frac{k\pi}{\sqrt{E}}\right) - \exp\left(-\frac{(k+1)\pi}{\sqrt{E}}\right). \end{aligned}$$

Ainsi, comme le nombre des pièces est asymptotique à  $L$ , la densité d'états intégrée à l'énergie  $E$  est donnée par

$$\begin{aligned} (2.5) \quad N(E) &= \sum_{k \geq 1} k \left( e^{-\frac{k\pi}{\sqrt{E}}} - e^{-\frac{(k+1)\pi}{\sqrt{E}}} \right) \\ &= \frac{\exp(-\ell_E)}{1 - \exp(-\ell_E)} \mathbf{1}_{E \geq 0} \quad \text{où} \quad \ell_E := \frac{\pi}{\sqrt{E}}. \end{aligned}$$

La longueur  $\ell_E$  est la plus petite longueur telle qu'une pièce de cette longueur a une valeur propre inférieure ou égale à  $E$ .

Remarquons que comme la fonction  $N(E)$  est continue, la convergence dans la limite (2.5) est localement uniforme par le théorème de Dini : les éléments de la suite sont des fonctions croissantes et leur limite est continue (voir (2.5)).

En utilisant (2.2), on peut aussi facilement calculer la densité d'états pour le laplacien libre, i.e., quand le milieu aléatoire est absent :

$$\begin{aligned} N_{-\Delta}(E) &= \lim_{L \rightarrow +\infty} \frac{\#\{\text{valeurs propres de } (-\Delta)|_{[0,L]} \text{ dans } ]-\infty, E]\}}{L} \\ &= \lim_{L \rightarrow +\infty} \frac{1}{L} \#\left\{k \geq 1; \frac{(\pi k)^2}{L^2} \leq E\right\} \\ &= \lim_{L \rightarrow +\infty} \frac{1}{L} \#\left\{k \geq 1; k \leq \frac{\sqrt{E}}{\pi} L\right\} = \frac{\sqrt{E}}{\pi} \mathbf{1}_{E \geq 0}. \end{aligned}$$

Les deux fonctions  $N$  et  $N_{-\Delta}$  sont, bien sûr, croissantes ; elles sont aussi continues et s'annulent sur  $]-\infty, 0]$ . Il est intéressant de noter que l'annulation en 0 (qui est le bord du spectre presque sûr du modèle (2.4)) des deux densités d'états intégrées est très différente : la densité d'états du modèle aléatoire s'annule exponentiellement vite en 0 alors que celle du laplacien libre ne s'annule que polynomialement.

L'existence de la densité d'états intégrée peut être démontrée pour de nombreux modèles aléatoires ergodiques (voir [6, 4]). La décroissance exponentielle de la densité d'états intégrée au bord du spectre presque sûr porte le nom d'« asymptotique de Lifshitz » ; c'est la première des caractéristiques des systèmes aléatoires localisés ; elle est typique des modèles aléatoires et a été démontrée pour de nombreux modèles (voir [7]). Dans le cas du modèle de Luttinger-Sy traité ci-dessus, on pourrait penser que l'asymptotique de Lifshitz est due à la distribution exponentielle des longueurs des pièces dans ce modèle. En fait, le phénomène sous-jacent est un phénomène de grande déviation qui est typique des processus aléatoires.

### 3. La limite thermodynamique

On s'intéresse maintenant aux propriétés d'un système d'électrons en interaction dans un milieu aléatoire que nous supposons être décrit par le modèle de Luttinger-Sy. On considère un grand échantillon d'un tel milieu, disons, un intervalle  $\Lambda$  de longueur  $|\Lambda|$  dans lequel on place  $n$  électrons. On veut étudier la limite thermodynamique du système, i.e., ce qui se passe quand  $|\Lambda|$  et  $n$  croissent vers l'infini de façon que  $n/|\Lambda|$  tende vers  $\rho > 0$ .

Les électrons sont des fermions c'est-à-dire que ce sont des particules indistinguables qui obéissent au principe d'exclusion de Fermi : un état quantique donné ne peut contenir au plus qu'une particule. Ceci se traduit mathématiquement par le fait que les états du système sont décrits par des fonctions (totalement) antisymétriques : si  $\Psi$  est la fonction d'onde de  $n$  particules dont les coordonnées sont  $(x_1, \dots, x_n)$  et que  $\sigma$  est une permutation de  $\{1, \dots, n\}$  de signature  $\text{sign}(\sigma)$ , alors

$$\Psi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \text{sign}(\sigma) \Psi(x_1, \dots, x_n), \quad \forall (x_1, \dots, x_n) \in \Lambda^n.$$

#### 3.1. Le hamiltonien de $n$ particules

On définit l'espace des fonctions antisymétriques de carré intégrable sur  $\Lambda^n$

$$(3.1) \quad \mathfrak{H}^n(\Lambda) = \bigwedge_{j=1}^n L^2(\Lambda).$$

Sur cet espace, on considère l'opérateur

$$(3.2) \quad H_\omega^0(\Lambda, n) = \sum_{i=1}^n \underbrace{\mathbf{1}_{\mathfrak{H}} \otimes \dots \otimes \mathbf{1}_{\mathfrak{H}}}_{i-1 \text{ fois}} \otimes H_\omega(\Lambda) \otimes \underbrace{\mathbf{1}_{\mathfrak{H}} \otimes \dots \otimes \mathbf{1}_{\mathfrak{H}}}_{n-i \text{ fois}},$$

c'est-à-dire, toutes les  $n$  particules se déplacent dans le même paysage aléatoire décrit par  $H_\omega(\Lambda)$ .

Les électrons interagissent. On va supposer que cette interaction se fait par paire : chaque paire d'électrons génère une interaction répulsive (i.e. positive) ; mais les groupes de trois électrons ou plus ne créent pas d'interactions supplémentaires (voir la forme du potentiel d'interaction total (3.5)). De plus, comme nos particules sont des électrons, on supposera que l'interaction est répulsive. On choisit ainsi une fonction  $U : \mathbb{R} \rightarrow \mathbb{R}^+$  bornée et paire. Il sera également nécessaire de contrôler les interactions à longue distance. On supposera pour cela que

$$(3.3) \quad x^3 \int_x^{+\infty} U(t) dt \xrightarrow{x \rightarrow +\infty} 0.$$

Sur  $\mathfrak{H}^n(\Lambda)$ , on considère l'opérateur

$$(3.4) \quad H_\omega^U(\Lambda, n) = H_\omega^0(\Lambda, n) + W_n$$

où

$$(3.5) \quad W_n(x^1, \dots, x^n) := \sum_{i < j} U(x^i - x^j).$$

On considère maintenant l'état fondamental de ce système ainsi que l'énergie fondamentale. L'énergie fondamentale est définie par

$$(3.6) \quad E_\omega^U(\Lambda, n) := \inf_{\substack{\Psi \in \mathcal{D}_\omega^n(\Lambda) \\ \|\Psi\| \neq 0}} \frac{\langle H_\omega^U(\Lambda, n) \Psi, \Psi \rangle}{\|\Psi\|^2}$$

où

$$(3.7) \quad \mathcal{D}_\omega^n(\Lambda) := \left( \bigoplus_{1 \leq k \leq m(\omega)}^\perp H_0^1(\Delta_k(\omega)) \right)^{\otimes n} \cap \mathfrak{H}^n(\Lambda).$$

En fait, l'infimum dans (3.6) est un minimum qui est atteint sur un sous-espace vectoriel de  $\mathfrak{H}^n(\Lambda)$  de dimension finie. Tous les minimiseurs sont appelés « états fondamentaux » du système.

La question principale est maintenant de calculer  $E_\omega^U(\Lambda, n)$  ainsi que de caractériser les minimiseurs de (3.6) quand  $|\Lambda| \rightarrow +\infty$  et  $n/|\Lambda| \rightarrow \rho$  où  $\rho > 0$  est une constante fixée.

Comme nous allons le voir, quand l'interaction  $U$  est nulle, ce problème est explicitement résoluble. On veut alors comprendre quelles sont les modifications induites par les interactions. On veut en particulier comprendre comment la densité  $\rho$  et les caractéristiques de l'interaction  $U$  (taille, vitesse de décroissance à l'infini, etc.) influent sur les états fondamentaux et l'énergie fondamentale.

### 3.2. Les matrices densité

L'une des difficultés que l'on rencontre lorsque l'on étudie la limite thermodynamique est que, le nombre de particules augmentant, le nombre de variables dont dépendent les fonctions d'ondes du système augmente. Les particules composant le système étant identiques, on peut les décrire en utilisant des matrices densité définies de la façon suivante.

Considérons  $\Psi$  un état normalisé du système, i.e.  $\Psi \in \mathfrak{H}^n(\Lambda)$  et  $\|\Psi\| = 1$ . La *matrice densité à une particule* de  $\Psi$  est l'opérateur sur  $\mathfrak{H}^1(\Lambda) = L^2(\Lambda)$  dont le noyau est donné par

$$(3.8) \quad \gamma_{\Psi}(x, y) = \gamma_{\Psi}^{(1)}(x, y) = n \int_{\Lambda^{n-1}} \Psi(x, \tilde{x}) \overline{\Psi(y, \tilde{x})} d\tilde{x}$$

où  $\tilde{x} = (x^2, \dots, x^n)$  et  $d\tilde{x} = dx^2 \dots dx^n$ .

La *matrice densité à deux particules* de  $\Psi$  est l'opérateur sur  $\mathfrak{H}^2(\Lambda) = \bigwedge_{j=1}^2 L^2(\Lambda)$

dont le noyau est donné par

$$(3.9) \quad \gamma_{\Psi}^{(2)}(x^1, x^2, y^1, y^2) = \frac{n(n-1)}{2} \int_{\Lambda^{n-2}} \Psi(x^1, x^2, \tilde{x}) \overline{\Psi^*(y^1, y^2, \tilde{x})} d\tilde{x}$$

où  $\tilde{x} = (x^3, \dots, x^n)$  et  $d\tilde{x} = dx^3 \dots dx^n$ .

L'opérateur  $\gamma_{\Psi}$  (resp.  $\gamma_{\Psi}^{(2)}$ ) décrit l'ensemble des particules (resp. des paires de particules) dans le système.

Les deux opérateurs  $\gamma_{\Psi}$  et  $\gamma_{\Psi}^{(2)}$  sont positifs et à trace (i.e. leur spectre est discret et leurs valeurs propres sont sommables); si  $\text{Tr}$  désigne la trace d'un opérateur, on calcule

$$(3.10) \quad \text{Tr} \gamma_{\Psi} = n \quad \text{et} \quad \text{Tr} \gamma_{\Psi}^{(2)} = \frac{n(n-1)}{2}.$$

Lorsque  $n$  tend vers l'infini, on peut bien sûr de façon analogue définir des matrices densité à  $k$  particules pour  $k$  arbitraire.

On peut maintenant envisager de définir simplement la limite de  $(\gamma_{\Psi_n}^{(1)})_{n \geq 1}$  ou  $(\gamma_{\Psi_n}^{(2)})_{n \geq 2}$  quand  $n$  tend vers  $+\infty$ .

## 4. $n$ électrons sans interaction dans un milieu aléatoire

On va commencer par construire l'état fondamental sans interaction; on calculera ensuite sa matrice densité à une particule. On obtiendra simultanément l'énergie fondamentale sans interaction.

### 4.1. L'état fondamental sans interaction

La décomposition spectrale du hamiltonien du système sans interaction  $H_{\omega}^0(\Lambda, n)$  (voir (3.2)) se calcule assez facilement à partir de celle du hamiltonien à une particule  $H_{\omega}(\Lambda)$  (voir (2.3)).

Pour ce faire, on appelle  $(E_{j,\omega}^{\Lambda})_{j \geq 1}$  et  $(\varphi_{j,\omega}^{\Lambda})_{j \geq 1}$  respectivement les valeurs et vecteurs propres associés de  $H_{\omega}(\Lambda)$ . On suppose les valeurs propres ordonnées de façon croissante. Les formules explicites (2.2) montrent que, pour le modèle de

Luttinger-Sy, presque sûrement, les valeurs propres sont toutes simples. Fixons maintenant  $\omega$  et  $1 \leq j_1 < j_2 < \dots < j_n$  des entiers et définissons l'état

$$(4.1) \quad \begin{aligned} \Psi_{\vec{j}}(x_1, \dots, x_n) &= \left( \prod_{k=1}^n \varphi_{j_k, \omega}^\Lambda \right) (x_1, \dots, x_n) \\ &= \frac{1}{\sqrt{n!}} \text{Det} \left( \left( \varphi_{j_k, \omega}^\Lambda(x_k) \right)_{1 \leq j, k \leq n} \right) \end{aligned}$$

où  $\vec{j} = (j_1, \dots, j_n)$ . Un état de cette forme est appelé « déterminant de Slater ». La fonction  $\Psi_{\vec{j}}$  est bien sûr totalement antisymétrique : c'est donc un état de  $\mathfrak{H}^n(\Lambda)$ . De plus, un calcul simple montre que

$$\left( H_\omega^0(\Lambda, n) - \sum_{k=1}^n E_{j_k, \omega}^\Lambda \right) \Psi_{\vec{j}} = 0.$$

Enfin, comme  $(\varphi_{j, \omega}^\Lambda)_{j \geq 1}$  forme une base orthonormée de  $L^2(\Lambda)$ , on vérifie que la famille  $(\Psi_{\vec{j}})_{1 \leq j_1 < j_2 < \dots < j_n}$  forme une base orthonormée de  $\mathfrak{H}^n(\Lambda)$ . Ainsi,  $H_\omega^0(\Lambda, n)$  est « diagonal » dans cette base : ses valeurs propres sont les nombres

$$\left( \sum_{k=1}^n E_{j_k, \omega}^\Lambda \right)_{1 \leq j_1 < j_2 < \dots < j_n}$$

associés aux vecteurs propres  $(\Psi_{\vec{j}})_{1 \leq j_1 < j_2 < \dots < j_n}$ .

Comme les valeurs propres sont ordonnées de façon croissante, l'état fondamental de  $H_\omega^0(\Lambda, n)$  est l'état  $\Psi_{(1, 2, \dots, n)}$  et il est associé à l'énergie fondamentale

$$E_\omega^0(\Lambda, n) = \sum_{j=1}^n E_{j, \omega}^\Lambda.$$

Comme les valeurs propres de  $H_\omega(\Lambda)$  sont simples presque sûrement, l'état fondamental est simple, i.e., quand  $U \equiv 0$ , le minimiseur dans (3.6) est presque sûrement un espace vectoriel de dimension 1.

## 4.2. L'asymptotique de l'énergie fondamentale par particule

Calculons maintenant l'asymptotique de  $E_\omega^0(\Lambda, n)$ . Pour cela, considérons la fonction croissante, constante par morceaux

$$E \mapsto N_{\Lambda, \omega}(E) = \frac{\#\{\text{valeurs propres de } H_\omega(\Lambda) \text{ dans } ] - \infty, E]\}}{L}.$$

Remarquons que, par définition de  $E_{n, \omega}^\Lambda$  (comme les valeurs propres de  $H_\omega(\Lambda)$  sont simples), on a

$$N_{\omega, \Lambda}(E_{n, \omega}^\Lambda) = \frac{n}{L}.$$

Comme, presque sûrement,  $N_{\omega, \Lambda}$  converge vers  $N$  uniformément (voir la remarque suivant (2.5)) et que  $n/L$  converge vers  $\rho$  quand  $L \rightarrow +\infty$ , on voit que  $E_{n, \omega}^\Lambda$  converge vers  $E_\rho$ , l'unique solution de  $N(E) = \rho$ . L'énergie  $E_\rho$  s'appelle l'énergie

de Fermi du système.

De même, presque sûrement, on calcule

$$\frac{1}{n} \sum_{j=1}^n E_{j,\omega}^\Lambda = \frac{L}{n} \int_{-\infty}^{E_{n,\omega}^\Lambda} E dN_{\Lambda,\omega}(E) \xrightarrow[\substack{L \rightarrow +\infty \\ n/L \rightarrow \rho}]{} \frac{1}{\rho} \int_0^{E_\rho} E dN(E).$$

On obtient ainsi que, dans la limite thermodynamique, l'énergie fondamentale par particule du système sans interaction converge vers

$$\mathcal{E}^0(\rho) := \frac{1}{\rho} \int_0^{E_\rho} E dN(E).$$

### 4.3. La matrice densité à une particule de l'état fondamental

Pour ce qui concerne l'état fondamental, on calcule sa matrice densité à une particule explicitement pour obtenir

$$\gamma_{\Psi_\omega^0(\Lambda,n)} = \sum_{j=1}^n \gamma_{\varphi_{j,\omega}^\Lambda} = \mathbf{1}_{]-\infty, E_{n,\omega}^\Lambda]}(H_\omega(\Lambda))$$

i.e. la matrice densité à une particule de l'état fondamental est le projecteur spectral de  $H_\omega(\Lambda)$  sur l'intervalle d'énergie  $]-\infty, E_{n,\omega}^\Lambda]$ . Ainsi, l'opérateur  $\gamma_{\Psi_\omega^0(\Lambda,n)}$  converge au sens fort vers le projecteur spectral de  $H_\omega$  sur l'intervalle d'énergie  $]-\infty, E_\rho]$ . On voit donc que dans l'état fondamental, pour le système sans interactions, dans la limite thermodynamique, les particules occupent tous les états disponibles sous l'énergie de Fermi  $E_\rho$  (voir la figure 4).

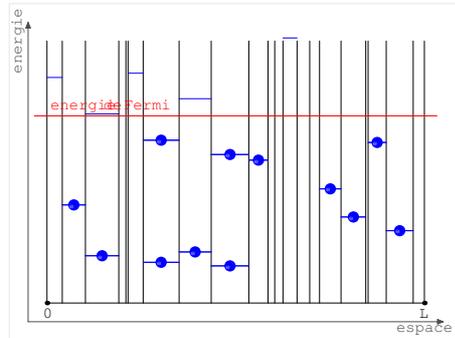


FIG. 4. L'énergie de Fermi

À l'énergie de Fermi, on peut associer la longueur de Fermi : c'est la longueur minimale que doit avoir une pièce afin d'avoir au moins un niveau d'énergie sous l'énergie de Fermi. Celle-ci existe car les niveaux d'énergie d'une pièce sont des fonctions décroissantes de la longueur de cette pièce. Notons-la  $\ell_F$ . On a  $\ell_F = \pi/\sqrt{E_\rho}$ . On sait alors que dans l'état fondamental du système sans interaction, une pièce de longueur inférieure à  $\ell_F$  ne porte pas d'électron. La loi exacte des niveaux d'énergie d'une pièce entraîne qu'une pièce de longueur comprise entre  $k\ell_F$

et  $(k+1)\ell_F$ ,  $(k+1)\ell_F$  exclue, porte exactement  $k$  électrons. On peut alors représenter l'état fondamental du système sans interaction de la façon suivante : en abscisse, on place les longueurs possibles pour une pièce et, en ordonnée, le nombre d'électrons contenu dans une telle pièce (dans l'état fondamental du système sans interaction). On obtient la figure 5.

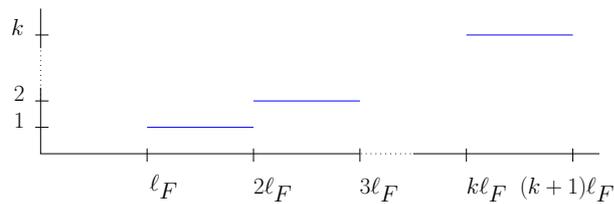


FIG. 5. La répartition des électrons dans l'état fondamental du système sans interaction

### 5. $n$ électrons en interaction dans un milieu aléatoire

On veut maintenant comprendre ce qui se passe lorsque l'on tient compte des interactions entre les électrons. Les électrons étant de même charge, ces interactions sont répulsives c'est-à-dire que l'énergie du système augmente quand on tient compte des interactions. Rappelons que l'on a supposé que les interactions se font par paire. Pour simplifier, nous commencerons par supposer que l'interaction entre deux électrons est nulle si ces deux électrons sont suffisamment éloignés l'un de l'autre, i.e., que  $U$  dans (3.4) est à support compact. Nous discuterons le cas plus général, celui quand seule l'hypothèse (3.3) est satisfaite, un peu plus bas.

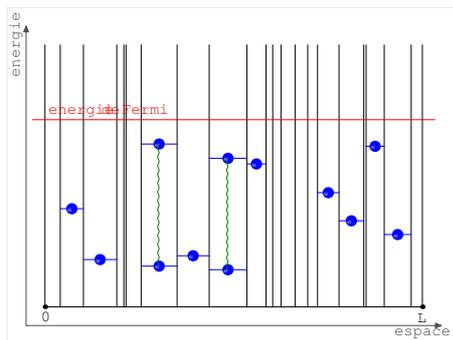


FIG. 6. Interaction entre les électrons

Si on part de l'état fondamental sans interaction et que l'on « allume » les interactions, les électrons interagissent, en particulier ceux vivant dans la même pièce (voir la figure 6). Il peut donc être plus économique énergétiquement d'éloigner les uns des autres certains électrons quitte à créer un état dont l'énergie dans le système sans interaction ne sera plus minimale : pour un système donné, un gain en énergie d'interaction peut compenser une perte en énergie sans interaction (voir la figure 7). Ceci ne concerne bien sûr que les électrons qui interagissent avec d'autres électrons : comme le potentiel d'interaction a un support borné, tous les électrons de l'état fondamental sans interaction disposés dans des pièces suffisamment éloignées de toutes les autres pièces portant un électron ne seront pas affectés par les interactions. L'éloignement minimal dépendra du potentiel d'interaction.

#### 5.1. L'énergie fondamentale par particule

Le premier résultat garantit l'existence d'une limite thermodynamique pour  $n^{-1}E_{\omega}^U(\Lambda, n)$ .

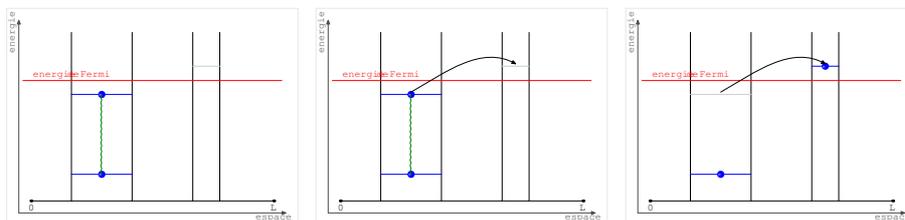


FIG. 7. Dissociation d'une paire d'électrons

**Théorème 5.1** ([8]). *Sous nos hypothèses, la limite existe presque sûrement et dans  $L^1_\omega$*

$$(5.1) \quad \mathcal{E}^U(\rho) := \lim_{\substack{L \rightarrow +\infty \\ n/L \rightarrow \rho}} \frac{E_\omega^U(\Lambda, n)}{n}.$$

*De plus, celle limite est indépendante de  $\omega$ .*

L'existence de la limite thermodynamique pour l'énergie fondamentale par particule peut être démontrée pour des systèmes assez généraux (voir [3, 13, 12]).

Nous avons vu que l'énergie  $\mathcal{E}^0(\rho)$  se calcule explicitement en terme de la densité d'états du modèle des pièces (voir la partie 4.2). Dans le cas de système en interaction, on obtient un développement asymptotique à deux termes quand  $\rho$  est petit, soit,

**Théorème 5.2** ([8]). *Soit  $\rho > 0$ . Sous nos hypothèses, quand  $\rho$  est assez petit, on calcule*

$$(5.2) \quad \mathcal{E}^U(\rho) = \mathcal{E}^0(\rho) + \pi^2 \left(1 - \exp\left(-\frac{\gamma}{8\pi^2}\right)\right) \frac{\rho}{|\log \rho|^3} + o(\rho |\log \rho|^{-3})$$

et

$$(5.3) \quad \mathcal{E}^0(\rho) = E_\rho \left(1 + O\left(\sqrt{E_\rho}\right)\right) = \frac{\pi^2}{|\log \rho|^2} \left(1 + O\left(\frac{1}{|\log \rho|}\right)\right)$$

où  $\gamma$  est une constante positive dépendant seulement de  $U$  définie dans la Proposition 5.3.

**Proposition 5.3** ([8]). *Considérons deux électrons dans  $[0, \ell]$  en interaction à travers le potentiel  $U$  vérifiant nos hypothèses, i.e., sur  $\mathfrak{H}^2([0, \ell]) = L^2([0, \ell]) \wedge L^2([0, \ell])$ , on considère l'opérateur*

$$(5.4) \quad \left(-\Delta_{x_1}^D|_{[0, \ell]}\right) \otimes \mathbf{1}_{\mathfrak{H}} + \mathbf{1}_{\mathfrak{H}} \otimes \left(-\Delta_{x_2}^D|_{[0, \ell]}\right) + U(x_1 - x_2)$$

avec conditions au bord de Dirichlet.

Pour  $\ell$  grand,  $E^U([0, \ell], 2)$ , l'énergie fondamentale de cet opérateur admet le développement asymptotique suivant :

$$(5.5) \quad E^U([0, \ell], 2) = \frac{5\pi^2}{\ell^2} + \frac{\gamma}{\ell^3} + o\left(\frac{1}{\ell^3}\right)$$

où  $\gamma = \gamma(U) > 0$  si  $U$  n'est pas identiquement nul.

Le développement (5.2) montre alors que, pour  $\rho$  petit, le premier terme de correction ne dépend que des interactions entre deux particules vivant dans la même pièce. Ceci sera expliqué par la description de l'état fondamental.

## 5.2. La matrice densité à une particule des états fondamentaux

### 5.2.1. Unicité de l'état fondamental

Par construction, il n'y a pas de principe de prolongement unique pour le modèle des pièces, la réunion des pièces n'étant pas connexe; ainsi, on ne s'attend pas en toute généralité à l'unicité de l'état fondamental, même si on peut espérer que celui-ci soit unique presque sûrement comme dans le cas du système sans interaction. Quand on tient compte des interactions, on peut démontrer le

**Théorème 5.4** ([8]). *Supposons que le potentiel d'interaction  $U$  est réel analytique. Alors, presque sûrement, pour tout  $L$  et  $n$ , l'état fondamental  $H_\omega^U(L, n)$  est unique.*

### 5.2.2. Description des états fondamentaux

Pour simplifier la description, nous supposerons maintenant que  $U$  a un support compact (auquel cas on ne sait pas si l'état fondamental est unique ou non). La description reste valide lorsque le potentiel d'interaction décroît suffisamment vite à l'infini, par exemple, de façon exponentielle avec un taux de décroissance assez grand.

Pour une pièce  $\Delta_k(\omega)$ , on appelle  $\zeta_{\Delta_k(\omega)}^j$  le  $j$ -ième vecteur propre normalisé de  $-\Delta_{|\Delta_k(\omega) \times \Delta_k(\omega)}^D + U$  agissant sur  $\bigwedge_{j=1}^2 L^2(\Delta_k(\omega))$  (on suppose que les valeurs propres sont ordonnées de façon croissante). Remarquons que, si  $U = 0$ , cet état à deux particules s'écrit aussi  $\zeta_{\Delta_k(\omega)}^{1,U=0} = \varphi_{\Delta_k(\omega)}^1 \wedge \varphi_{\Delta_k(\omega)}^2$  (voir (4.1)). On définit la matrice densité à une particule suivante :

$$\gamma_{\Psi_{\Lambda, n}^{\text{opt}}} = \sum_{\ell_F - \rho\gamma_* \leq |\Delta_k(\omega)| \leq 2\ell_F - \log(1-\gamma_*)} \gamma_{\varphi_{\Delta_k(\omega)}^1} + \sum_{2\ell_F - \log(1-\gamma_*) \leq |\Delta_k(\omega)|} \gamma_{\zeta_{\Delta_k(\omega)}^1}.$$

On démontre

**Théorème 5.5** ([8]). *Il existe  $\rho_0 > 0$  et  $C > 0$  tels que, pour  $\rho \in (0, \rho_0)$ , presque sûrement, si  $\Psi_\omega^U(\Lambda, n)$  est un état fondamental, on a*

$$\limsup_{\substack{L \rightarrow +\infty \\ n/L \rightarrow \rho}} \frac{1}{n} \left\| \gamma_{\Psi_\omega^U(\Lambda, n)} - \gamma_{\Psi_{\Lambda, n}^{\text{opt}}} \right\|_{tr} \leq C \frac{\rho}{|\log \rho|}.$$

Le Théorème 5.5 donne la distribution dans les différentes pièces (au sens de la figure 5) des électrons constituant l'état fondamental du système en interaction, ceci à une erreur de taille  $O(n\rho/|\log \rho|)$  près, i.e., il y a au plus  $O(n\rho/|\log \rho|)$  particules qu'on ne contrôle pas.

On peut aussi comparer  $\gamma_{\Psi_{\Lambda,n}^{\text{opt}}}$  à la matrice de densité à une particule de l'état fondamental sans interaction pour obtenir

$$\limsup_{\substack{L \rightarrow +\infty \\ n/L \rightarrow \rho}} \frac{1}{n} \left\| \gamma_{\Psi_{\omega}^0(\Lambda,n)} - \gamma_{\Psi_{\Lambda,n}^{\text{opt}}} \right\|_{\text{tr}} = 2\gamma_*\rho + O\left(\frac{\rho}{|\log \rho|}\right)$$

où

$$\gamma_* = 1 - \exp\left(-\frac{\gamma}{8\pi^2}\right).$$

Ainsi, comme  $\rho$  est petit, environ  $\gamma_*\rho n$  électrons ont été effectivement déplacés lorsque l'on a « allumé » les interactions.

On ne sait donc pas calculer la distribution de façon aussi précise que lorsque les interactions sont nulles mais, si on se restreint aux pièces de longueur inférieure à  $3\ell_F$ , on obtient la figure 8.

On montre que le nombre d'électrons contenus dans les pièces de longueur supérieure à  $3\ell_F$  est de taille  $\rho^2 n$ ; donc, quand  $\rho$  est petit, il est petit par rapport à  $n$ , le nombre total d'électrons. La figure 8 décrit donc la plupart des électrons. On y voit que, dans les pièces de longueur comprise entre  $2\ell_F$  et  $2\ell_F - \log(1 - \gamma_*)$ , pièces qui contenaient deux électrons dans l'état fondamental du système sans interaction, on a retiré un électron pour le replacer dans une pièce de longueur comprise entre  $\ell_F - \gamma_*\rho$  et  $\ell_F$ , pièces qui ne contenaient aucun électron dans l'état fondamental du système sans interactions. Cette description permet alors de calculer l'énergie

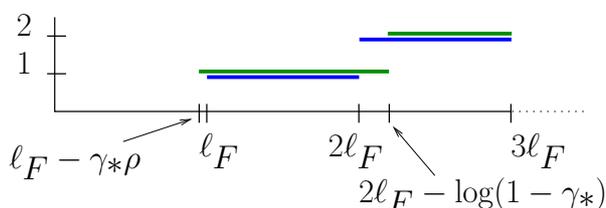


FIG. 8. La distribution des électrons dans l'état fondamental du système en interaction

de l'état fondamental du système en interaction : on obtient l'asymptotique de la correction à apporter à l'énergie de l'état fondamental du système sans interaction, i.e., le Théorème 5.2 quand  $U$  est à support compact.

On peut aussi étudier ce qui se passe quand le support des interactions n'est pas borné sous l'hypothèse (3.3). Quand l'interaction entre deux électrons décroît au moins aussi vite que la puissance quatrième de la distance les séparant, l'état fondamental est encore à peu près décrit par la figure 8 à une modification près : dans les pièces de longueur inférieure à  $\ell_F$ , la distribution des électrons va être modifiée pour optimiser les interactions à grande distance. On peut alors montrer

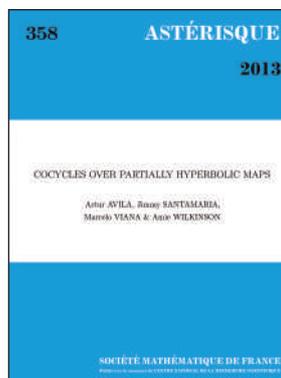
que ce changement n'a pas d'effet sur le terme principal de la correction de l'énergie fondamentale ; ceci donne le Théorème 5.2 sous l'hypothèse (3.3).

Lorsque l'hypothèse (3.3) n'est plus vérifiée, le développement en  $\rho$  de  $\mathcal{E}^U(\rho)$  devrait être modifié : la correction principale ne viendra plus de la dissociation des électrons vivant par paires dans de grandes pièces mais du repositionnement des électrons vivant seul dans leur pièce.

## 6. Références

- [1] P. W. Anderson. Absence of Diffusion in Certain Random Lattices. *Physical Review Online Archive (Prola)*, 109(5) :1492–1505, March 1958.
- [2] N. W. Ashcroft and N. D. Mermin. *Solid state physics*. Holt-Saunders International Editions : Science : Physics. Holt, Rinehart and Winston, 1976.
- [3] X. Blanc and M. Lewin. Existence of the thermodynamic limit for disordered quantum Coulomb systems. *J. Math. Phys.*, 53(9) :095209, 32, 2012.
- [4] M. Disertori, W. Kirsch, A. Klein, F. Klopp, and V. Rivasseau. *Random Schrödinger operators*, volume 25 of *Panoramas et Synthèses [Panoramas and Syntheses]*. Société Mathématique de France, Paris, 2008.
- [5] Y. Katznelson. *An introduction to harmonic analysis*. Dover Publications Inc., New York, corrected edition, 1976.
- [6] W. Kirsch. An invitation to random Schrödinger operators. dans *Random Schrödinger operators*, volume 25 de *Panoramas et Synthèses*, pages 1–119. Société Mathématique de France, Paris, 2008. avec un appendice de Frédéric Klopp.
- [7] W. Kirsch and B. Metzger. The integrated density of states for random Schrödinger operators dans *Spectral theory and mathematical physics : a Festschrift in honor of Barry Simon's 60th birthday*, volume 76 de *Proc. Sympos. Pure Math.*, pages 649–696. Amer. Math. Soc., Providence, RI, 2007.
- [8] F. Klopp, and N. A. Veniaminov. *Interacting electrons in a random medium : a simple one-dimensional model*. ArXiv. <http://fr.arxiv.org/abs/arXiv:1408.5839>, 2014
- [9] A. Lagendijk, B. van Tiggelen, and D. S. Wiersma. Fifty years of Anderson localization. *Physics Today*, 62(8) :24–29, August 2009.
- [10] I. M. Lifshits, S. A. Gredeskul, and L. A. Pastur. *Introduction to the theory of disordered systems*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1988. Traduit du russe par Eugène Yankovsky [E. M. Yankovskii].
- [11] J. M. Luttinger and H. K. Sy. Low-lying energy spectrum of a one-dimensional disordered system. *Phys. Rev. A*, 7 :701–712, Feb 1973.
- [12] N. A. Veniaminov. *Limite thermodynamique pour un système de particules quantiques en interaction dans un milieu aléatoire*. Thèse de doctorat, Université Paris 13, 2012.
- [13] N. A. Veniaminov. The existence of the thermodynamic limit for the system of interacting quantum particles in random media. *Ann. Henri Poincaré*, 14(1) :63–94, 2013.

**Remerciements.** *Un grand merci à Nikolaj Veniaminov pour m'avoir permis de réutiliser certaines figures qu'il a réalisées, ainsi qu'à Maxime Bourrigan, Bernard Helffer et Romain Tessera pour leurs corrections, remarques et enthousiasmes lors de la préparation de ce texte.*



Astérisque

## Cocycles over partially hyperbolic maps

A. Avila, J. Santamaria  
M. Viana and A. Wilkinson

The works collected in this volume, while addressing quite different goals, are focused on the same type of mathematical object: cocycles over partially hyperbolic diffeomorphisms. We begin with a preliminary overview giving background on the history and applications of the study of dynamical cocycles and partially hyperbolic theory and elucidating the connections between the two main articles. The first one investigates effective conditions which ensure that the Lyapunov spectrum of a (possibly non-linear) cocycle over a partially hyperbolic dynamical system is nontrivial. In the second one, the classical Livšic theory of the cohomological equation for Anosov diffeomorphisms is extended to accessible partially hyperbolic diffeomorphisms.

*Les travaux réunis dans ce volume, ayant pourtant des objectifs très différents, sont axés sur le même genre d'objet mathématique : les cocycles au dessus d'un difféomorphisme partiellement hyperbolique. On commence par des rappels sur l'histoire et les applications de l'étude des cocycles dynamiques et la théorie partiellement hyperbolique; ils mettent en évidence des liens entre deux articles principaux. Dans le premier, on étudie des conditions efficaces qui garantissent la non-trivialité du spectre de Lyapunov d'un cocycle (éventuellement non-linéaire) au dessus d'un difféomorphisme partiellement hyperbolique. Dans le second, la théorie classique de Livšic sur l'équation cohomologique pour les difféomorphismes d'Anosov est étendue au cas d'un difféomorphisme partiellement hyperbolique et accessible.*

ISBN : 978-2-85629-778-0

prix public\* : 48 € - prix membre : 34 €

\*frais de port non compris



Institut Henri Poincaré  
11 rue Pierre et Marie Curie  
F-75231 PARIS CEDEX 05

<http://smf.emath.fr>

# NOUVELLES DU CONGRÈS INTERNATIONAL

---

*Le congrès international des mathématiciens, l'ICM 2014, s'est déroulé à Séoul en août dernier. La Gazette vous propose le premier volet d'un grand dossier consacré à cet évènement qui a marqué la rentrée mathématique. À travers son carnet de bord, Gaël Octavia, responsable de la communication pour la Fondation Sciences Mathématiques de Paris (FSMP), vous offre un premier regard sur cet ICM. Anton Zorich d'une part, et Pascal Hubert et Raphaël Krikorian d'autre part, vous invitent ensuite à découvrir les travaux de Maryam Mirzakhani et d'Artur Avila. Pour finir, vous passerez un moment en aparté avec Manjul Bhargava et Martin Hairer. Ces deux entretiens ont été réalisés pendant le congrès, à Séoul, par Gaël Octavia et Boris Adamczewski. Des versions filmées de ces entrevues seront disponibles sur le site de la FSMP : [www.sciencesmaths-paris.fr](http://www.sciencesmaths-paris.fr)*

## Séoul 2014 : quelques mots pour un ICM

Gaël Octavia<sup>1</sup>

---

*Impatience.* C'est ainsi que débute, le 12 août 2014, ce séjour au Congrès International des Mathématiciens, le deuxième auquel j'ai le plaisir d'assister, quatre ans après celui d'Hyderabad. Impatience d'arriver après un interminable vol ponctué de secousses et une bonne heure et demie de bus (heureusement, particulièrement confortable) entre l'aéroport et l'hôtel. Impatience de découvrir Séoul, le centre de congrès, le style de l'organisation, l'ambiance, les mathématiciens présents, les exposés... Impatience, évidemment, de connaître les lauréats des prestigieuses récompenses qui seront décernées dès le lendemain, lors de la cérémonie officielle. En particulier, ceux de la médaille Fields.

*Rouge.* On ne peut pas les manquer, les polos rouges. Ce sont les volontaires – des étudiants pour la plupart – chargés de guider, renseigner, dorloter les cinq mille participants attendus. Vaillants petits soldats de l'organisation dont les nerfs seront mis à rude épreuve pendant ce congrès. En cette veille de cérémonie officielle, ils sont encore frais et pimpants. Au près d'eux, on finalise son inscription et on récupère le badge dont on ne se départira plus pendant les dix prochains jours. On repère celui qui parle français : ça tombe bien, il est inratable, un grand gaillard charpenté comme un déménageur. Que faire, lui demande-t-on, pour patienter jusqu'au soir sans céder à l'envie de faire la sieste ? (Mue par un optimisme béat,

---

<sup>1</sup> Fondation Sciences Mathématiques de Paris (FSMP). Le blog de la FSMP consacré à l'ICM 2014 : [www.icm2014seoul-blog.com](http://www.icm2014seoul-blog.com)

je crois encore pouvoir me caler sur l'heure de Séoul d'ici un ou deux jours, comme à Hyderabad.) Visiter le très beau temple bouddhique, juste en face du centre de congrès. Fontaines, lampions, grande statue de Bouddha, pagodes... avec buildings en arrière-plan. Métaphore d'une coexistence entre des traditions bien ancrées et un amour manifeste de l'ultra-modernité, incarnée par Samsung et ses produits high-tech.

*Spéculation.* Le soir du 12 août, c'est le dîner d'accueil offert par l'organisation du congrès. Autour d'un buffet pas spécialement coréen – pour le peu que je connaisse de cette gastronomie – mais délicieux, la communauté mathématique se retrouve, bavarde, dans la bonne humeur. On repère des lauréats potentiels. La présence d'Artur Avila – qui n'est pas au programme des conférences, a priori – confirme ce que l'on suppose depuis longtemps : une des médailles Fields ira au prodigieux dynamicien franco-brésilien. Pour ceux qui le connaissent et à qui il dissimule – bien forcé – la bonne nouvelle depuis des mois, c'est une joie et un soulagement. Certains jouent quand même à se faire peur : après tout, déjà, en 2010... Le déchiffrement des bribes d'une conversation brésilienne dissipe les derniers doutes : « Wellington [de Melo, donc, le directeur de thèse d'Artur Avila] a-t-il finalement pu venir ? Il a eu un problème de passeport. Il est là ? Ouf ! C'eut été tellement dommage... » Je taquine le principal intéressé en lui demandant s'il est venu venger la Seleçao (opposer les maths et le foot, c'est une mauvaise habitude prise en 2010, année où la débâcle des Bleus « restés dans le bus » au Mondial n'eut d'égal que le triomphe des mathématiciens français raflant deux médailles Fields et un prix Gauss). Il botte habilement en touche : « Rien ne peut venger ça. » Manjul Bhargava et Maryam Mirzakhani sont aussi sur toutes les lèvres. Le palmarès se dessine. J'entends pour la première fois parler d'un certain Martin Hairer, pourtant connu comme le jeune espoir qui enthousiasme le monde des EDP stochastiques. Plus que quelques heures avant la fin du suspense.

*Émotion.* De l'avis général, c'est une bien belle cérémonie qui s'est tenue le 13 août devant une salle comble. Après de longues minutes dans les files d'attente dues aux contrôles de sécurité (présence de la Présidente de la République oblige), après un spectacle chorégraphique coloré et des discours officiels, le moment tant attendu est arrivé. En fait, plus personne n'ignore le nom des lauréats de la médaille Fields, car les informations ont fuité par on ne sait quels canaux percés et les dépêches sont tombées toute la nuit. Mais l'émotion est tout de même là quand, l'un après l'autre, ils sont officiellement désignés, présentés via un court-métrage (cadeau de la Fondation Simons) et invités à monter sur l'estrade : le franco-brésilien Artur Avila (IMPA, CNRS, IMJ-PRG), puis le canado-américain Manjul Bhargava (université de Princeton), ensuite l'autrichien Martin Hairer (université de Warwick) et enfin l'irano-américaine Maryam Mirzakhani (université de Stanford). La cérémonie se poursuivra avec l'attribution du prix Nevanlinna à l'indo-américain Subhash Khot (université de New York), puis du prix Gauss à Stanley Osher (UCLA) et de la médaille Chern à Phillip Griffiths (IAS de Princeton), ces deux derniers étant américains. La remise du dernier prix du congrès, le prix Leelavati, à l'argentin Adrián Paenza sera gardée pour la cérémonie de clôture.

Revenons aux médaillés Fields, quatuor atypique à plus d'un titre. D'abord, particularité d'importance historique, il comporte une femme ! (La photo-souvenir, en fin de cérémonie, sur laquelle lauréats et officiels sourient ensemble à l'objectif, offrira le tableau absolument inédit de cette toute première femme médaillée Fields posant entre Geun-hye Park, toute première présidente de la République de Corée, et Ingrid Daubechies, toute première présidente de l'IMU.) Mais ce n'est pas tout. Chaque lauréat incarne à sa façon une « première fois » dans l'histoire de la médaille : premier Brésilien (et même premier Sud-Américain), premier Indien (« Indien de cœur », selon les propres termes de Manjul Bhargava, et de culture, à défaut de nationalité, qui parle l'hindi à la maison et est célébré par la presse indienne comme un enfant du pays), premier Autrichien et première Iranienne. Chacun porte une forme de métissage culturel et scientifique. D'ailleurs, comme l'a souligné récemment le directeur de l'INSM Christoph Sorger, chacun effectue sa recherche dans un pays qui n'est pas son pays d'origine (au moins la moitié du temps dans le cas d'Artur Avila). Un cru 2014 à l'image d'un monde contemporain globalisé.

*Coqueluche.* Autographes et photos avec le public sont le lot quotidien de tous les lauréats de cet ICM, qui s'y prêtent de bonne grâce (là encore, un signe des temps ?). Cependant, le plus jeune d'entre eux, venu sans chaperon ni conjoint contrairement à ses co-médaillés, inconditionnel du tee-shirt moult noir ou blanc et flanqué d'une réputation qui veut qu'il fasse ses maths à la plage, exerce une fascination toute particulière...

*Conférenciers.* Si on parle beaucoup des prix décernés à l'ICM, il convient de ne pas oublier que l'essentiel du congrès, ce sont les exposés des chercheurs invités à y représenter leur spécialité. Conférences plénières, conférences des sections ou encore conférences spéciales comme celle de James Simons (convié à parler sur le mode « ma vie, mon œuvre »), la conférence Abel (donnée par un lauréat de l'autre prix le plus prestigieux des mathématiques, cette année John Milnor, véritable légende vivante qui entreprit ici de retracer quatre siècles de topologie en une heure), la Noether Lecture (qui met à l'honneur une grande mathématicienne, ici Georgia Benkart)... Faire un exposé à l'ICM est à la fois un honneur et un exercice difficile puisqu'il s'agit, surtout pour les conférences plénières, d'intéresser un public beaucoup plus large que le cercle des spécialistes de son domaine, sans pour autant frustrer ces derniers (Artur Avila affirme par exemple que sa conférence plénière de 2010 lui a coûté quelques cheveux). Certains semblent particulièrement taillés pour ce type de performance : nous fûmes nombreux à être éblouis par la conférence plénière de Manjul Bhargava, grand moment d'éloquence, de clarté et de pédagogie, où l'on commençait par se demander dans quel cas l'évaluation entière d'une expression mathématique est un carré d'entier, pour poursuivre avec l'équation de Pell, Fermat, Ramanujan, les courbes elliptiques et hyper-elliptiques, et terminer, en douceur, sur la conjecture de Birch et Swinnerton-Dyer et les résultats les plus récents du brillant orateur. Un grand regret, en revanche, partagé par beaucoup : n'avoir pas pu voir Maryam Mirzakhani exercer ses talents de conférencière, puisqu'elle dut malheureusement annuler son exposé au dernier moment.

*École française.* S'il est normal de se réjouir de la médaille Fields d'Artur Avila, le signe le plus probant de la bonne santé de la recherche mathématique française actuelle est lisible à la lecture du programme des conférences de cet ICM : la France est une nation incontournable, avec un cinquième des orateurs et une présence dans quasiment toutes les sections. Tombé pendant le congrès, le classement de Shanghai pour les mathématiques en est une attestation supplémentaire : on se félicitera notamment du quatrième rang mondial de l'université Pierre et Marie Curie. D'aucuns souligneront quand même que notre dernier médaillé Fields est le premier à n'avoir pas été formé chez nous. Excellence française, oui, mais qu'il faudra veiller à faire perdurer.

*Vulgarisation.* La nécessité de diffuser les mathématiques auprès du grand public, via l'enseignement et au-delà, semble de plus en plus affirmée à l'ICM. Ainsi, on y décerne depuis 2010 une récompense distinguant un grand vulgarisateur : le prix Leelavati, attribué cette année à Adrián Paenza. La question de comment transmettre et populariser efficacement une science objectivement difficile et souffrant peut-être plus que toute autre d'une image faussée, est posée à Séoul lors de tables rondes et de conférences. Notamment celle d'Étienne Ghys qui, devant une salle comble, évoque trois expériences personnelles en la matière : *Dimension* et *Chaos*, ses films en accès gratuit, sous-titrés dans des dizaines de langues et vus par des millions de gens ; le site *Images des Maths*, qu'il dirige ; sa conférence dans le cadre des *Ernests* (dont le slogan est : *quinze minutes pour changer notre vision du monde*), également disponible sur Internet. Un exposé dont on retiendra trois messages essentiels. Premièrement : la vulgarisation est une chose difficile, exigeant du temps, des connaissances, du savoir-faire, et méritant par conséquent d'être davantage valorisée. Deuxièmement : l'outil Internet recèle d'immenses possibilités dans ce domaine, encore en partie non exploitées. Enfin : la culture mathématique doit rester gratuite et il revient aux institutions compétentes de se donner les moyens humains et financiers de mettre des contenus de qualité à la disposition du public.

*Presse.* On ne peut pas dire que la presse française ait boudé cet ICM. Des émissions de radio et de télévision, de nombreux articles, souvent pertinents, parus peu avant, pendant, ou juste après le congrès, ont été consacrés à des personnalités de la communauté mathématique en général et aux lauréats Fields en particulier, avec peut-être un intérêt plus marqué que lors des précédentes éditions – Cédric Villani est passé par là. Mais on peut déplorer que, comme en 2010, aucun grand organe de presse hexagonal n'ait daigné envoyer un correspondant spécialement pour l'événement. Heureuse surprise, tout de même, à la sortie de la conférence de presse des lauréats, juste après la cérémonie officielle : un journaliste et un caméraman de France 24 sont là, attendant d'interviewer Artur Avila. Aurais-je médité sur nos bons vieux médias ? En fait, m'avouent-ils, ils ont été envoyés à Séoul pour la venue du Pape. C'est sur place qu'ils ont entendu parler du congrès et qu'ils ont décidé d'y faire un saut. Un miracle, en quelque sorte.

*Lendemain.* Particulièrement réussi, l'ICM 2014 se clôt en se projetant vers l'avenir. D'abord en direction de Rio, où se tiendra l'ICM 2018, dont le président

de la Société Brésilienne de Mathématiques, Marcelo Viana, dévoile les ambitions lors de la cérémonie de clôture du 21 août. Ensuite, peut-être, vers la France, qui a officiellement fait part de son souhait d'accueillir l'ICM 2022 à Paris, plus d'un siècle après le congrès historique de 1900 qui avait notamment vu David Hilbert énoncer sa célèbre liste de problèmes. Une candidature à suivre !

## Le théorème de la baguette magique de A. Eskin et M. Mirzakhani

Anton Zorich<sup>1</sup>

---



Avec l'aimable autorisation de Maryam Mirzakhani

Lors de la séance d'ouverture du congrès international des mathématiciens à Séoul le 13 août 2014, Maryam Mirzakhani a reçu la médaille Fields « *pour ses contributions exceptionnelles à la dynamique et à la géométrie des surfaces de Riemann et de leurs espaces de modules* » devenant ainsi la première femme à recevoir la médaille Fields. Voici quelques extraits de l'éloge de l'ICM à son sujet [ICM] :

« *Maryam Mirzakhani a obtenu des résultats extraordinaires dans la théorie des surfaces de Riemann et de leurs espaces de modules ; elle a ouvert de nouveaux horizons dans ce domaine. Ses percées mélangent des méthodes de plusieurs branches des mathématiques comme la géométrie algébrique, la topologie et la théorie des probabilités.*

*En géométrie hyperbolique, Mirzakhani a découvert le comportement asymptotique du nombre de géodésiques fermées sans auto-intersection sur une surface de Riemann de genre  $g$ . Elle a ensuite utilisé ces résultats pour donner une preuve nouvelle et complètement inattendue de la conjecture de Witten, une formule portant sur les classes caractéristiques des espaces de modules de surfaces de Riemann avec des points marqués.*

---

<sup>1</sup> Institut de mathématiques de Jussieu – Paris Rive Gauche, Institut Universitaire de France.

*En dynamique, elle a trouvé une nouvelle construction remarquable qui établit un lien entre les aspects holomorphe et symplectique de l'espace des modules et l'a utilisée pour montrer que le « flot du tremblement de terre » de Thurston est ergodique et mélangeant.*

*Très récemment, Mirzakhani et ses collaborateurs ont obtenu une preuve de la conjecture espérée depuis longtemps selon laquelle – alors que l'adhérence d'une géodésique réelle dans un espace de modules peut avoir une structure très fractale, rendant toute classification impossible – l'adhérence d'une géodésique complexe est toujours une sous-variété algébrique.*

*Ses travaux ont révélé que la théorie de la rigidité des espaces homogènes (développée par Margulis, Ratner et d'autres) a un certain écho dans le contexte hautement inhomogène mais aussi fondamental des espaces de modules, où de nombreux développements sont toujours en cours. »*

Nous commençons par une brève notice biographique sur Maryam Mirzakhani (pour plus de détails regarder l'excellent article en ligne [KI] de Erica Klarreich). Puis nous tentons de donner une idée de ses recherches en nous concentrant sur un résultat fondamental particulier. Des motivations provenant de la théorie de la conductivité présentées dans la section 1 nous amènent naturellement aux feuilletages mesurés. Dans la section 2 nous introduisons le langage des surfaces de translation ; ce langage est extrêmement simple et très utile pour étudier les feuilletages mesurés. Nous continuons en expliquant dans la section 3 comment la dynamique sur une surface de translation individuelle est liée à la dynamique dans l'espace (de dimension assez grande) de toutes les surfaces de translations. Dans la section 4 nous constatons que la théorie ergodique est complètement inutile dans des études des trajectoires isolées. Finalement, dans la section 5 nous formulons les résultats de A. Eskin et M. Mirzakhani [EMi], et de A. Eskin, M. Mirzakhani et A. Mohammadi [EMiMh], qui servent de baguette magique pour de nombreuses applications (le choix des applications dans cet article repose plus sur la simplicité de présentation que sur leur importance).

La présente note est en relation étroite avec une partie de la note [HuKr] de P. Hubert et de R. Krikorian dans le même numéro de la *Gazette* dédiée aux résultats d'Artur Avila, portant sur la dynamique dans l'espace de Teichmüller (voir [HuKr]). Les deux articles se complètent.

Pour une présentation plus large des œuvres mathématiques de M. Mirzakhani nous conseillons une courte note [Mc2] écrite par C. McMullen pour les publications de l'ICM. Pour une présentation plus courte et abordable nous conseillons un petit résumé [G] fait par É. Ghys pour *Images des Mathématiques*.

### **Brève notice biographique**

Maryam Mirzakhani est née en 1977 à Téhéran. Ayant passé avec succès les tests d'entrée, elle a été admise au collège et puis au lycée Farzanegan à Téhéran. Ces établissements pour les filles sont administrés par l'*Organisation nationale de l'Iran pour le développement des Talents Exceptionnels*.

Maryam a raconté à Erica Klarreich, journaliste du magazine *Quanta* (voir [KI] pour les détails) qu'avec son amie, Roya Beheshti, elles ont convaincu la directrice de leur lycée d'organiser des cours d'entraînement pour les Olympiades Internationales de mathématiques (à cette époque l'équipe iranienne ne comportait pas

de fille). La détermination de Maryam l'a amenée à des résultats exceptionnels : elle a reçu des médailles d'or en 1994 et en 1995.

Elle commence ensuite des études universitaires à l'université Sharif à Téhéran où elle obtient une licence en 1999. Par la suite, Maryam Mirzakhani part à Harvard où elle choisit Curt McMullen comme directeur de thèse. Sa thèse, qu'elle soutient en 2004, lui apporte une renommée internationale. Maryam y démontre que le nombre  $N(X, L)$  de géodésiques fermées simples (i.e. sans auto-croisement) de longueur au plus  $L$  sur une surface de Riemann  $X$  croît asymptotiquement comme

$$N(X, L) \sim \text{const}(X) \cdot L^{6g-6} \text{ quand } L \rightarrow \infty.$$

Cette croissance est polynomiale, alors que, classiquement, le nombre de *toutes* les géodésiques fermées croît exponentiellement, comme  $e^L/L$  : la plupart des géodésiques fermées se croisent. Un autre résultat majeur de la même thèse est une nouvelle preuve de la conjecture de Witten (la première preuve avait été obtenue par M. Kontsevich en 1992).

Suite à cette thèse extraordinaire, Maryam Mirzakhani a reçu une prestigieuse bourse pour la recherche de l'Institut mathématique Clay. En plus du salaire et des fonds de fonctionnement généreux, le boursier (ou la boursière) obtient la liberté du choix où effectuer sa recherche<sup>2</sup>.

Pendant quelques années, Maryam Mirzakhani a travaillé à l'université de Princeton. En 2008, à l'âge de 31 ans, elle est devenue professeur permanent à l'université de Stanford, où elle travaille depuis. Maryam est mère d'une charmante petite fille.

D'un point de vue personnel, Maryam est extrêmement sympathique, ouverte, et tout sauf snob ; en la rencontrant à un colloque, vous la prendriez au premier regard plutôt pour une jeune postdoc que pour une mathématicienne célèbre. Ses exposés auxquels j'ai pu assister ont toujours rayonné d'enthousiasme et d'optimisme contagieux, et ont été pleins d'appréciation de la beauté des mathématiques ; ils vous inspirent pour vous attaquer à des problèmes audacieux et à ne pas renoncer quand ils résistent.

## 1. De la conductivité aux feuilletages mesurés

En un sens, les systèmes dynamiques étudient tout ce qui bouge, souvent lorsque le mouvement a déjà atteint une sorte de régime stable. La « chose qui bouge » pourrait être le système solaire, ou un système de particules dans une boîte, ou une boule de billard sur une table (d'une forme pas forcément rectangulaire), ou des courants dans l'océan, ou des électrons dans un métal, etc. On peut observer certains phénomènes communs dans de grandes classes de systèmes dynamiques ; en particulier, les billards mathématiques sont des modèles jouets représentant le comportement d'un gaz dans une boîte. Ces modèles simplifiés permettent d'élaborer des outils, qu'on peut ensuite utiliser pour étudier la dynamique de systèmes plus réalistes provenant de la physique, de la chimie, de la biologie, de l'informatique (ou d'autres domaines des mathématiques).

Un de ces outils est le langage des feuilletages mesurés sur les surfaces, développé par Bill Thurston (il généralise les lignes de pente irrationnelle qui s'enroulent

<sup>2</sup> Notons que trois parmi les quatre lauréats de la médaille Fields de 2014 sont d'anciens récipiendaires de cette bourse de l'Institut Clay.

indéfiniment autour d'un tore plat). Il s'avère fort utile pour comprendre toute une classe de systèmes dynamiques, comprenant des billards périodiques dans le plan (comme le « modèle *windtree* » introduit par Paul et Tatiana Ehrenfest il y a un siècle ; voir l'article de P. Hubert et R. Krikorian dans ce numéro de la *Gazette* pour plus de détails), ainsi que le mouvement d'un électron sur une surface de Fermi en présence d'un champ magnétique homogène (voir le survol [MINo] pour les détails sur ce problème de Novikov).

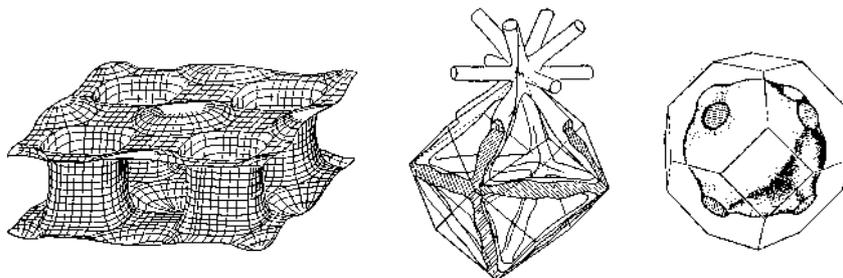


FIG. 1. Domaines fondamentaux de surfaces de Fermi d'étain, de fer et d'or reproduits de [ALK]. Les trajectoires des électrons dans ces métaux en présence d'un champ magnétique homogène correspondent à des sections planaires des surfaces périodiques correspondantes.

Un flot le long des feuilles d'un tel feuilletage mesuré sur une surface décompose la surface en deux types de domaines : en composantes périodiques remplies par des trajectoires fermées et en composantes minimales dans lesquelles chaque trajectoire est dense.

En appliquant une chirurgie naturelle, le feuilletage peut être en quelque sorte « globalement redressé » sur chaque composante minimale. Plus précisément, on peut choisir des coordonnées appropriées (dites plates), dans lesquelles le feuilletage est représenté par une famille de lignes verticales  $x = \text{const}$ . Des versions de ce « théorème de redressement » ont été démontrées dans des contextes différents et dans différents termes par E. Calabi [Ca], A. Katok [Ka], J. Hubbard et H. Masur [HdMa], et d'autres auteurs. Ces théorèmes impliquent que pour étudier une importante classe de systèmes dynamiques il suffit de limiter l'étude à un modèle simplifié et d'étudier des feuilletages en droites sur les « surfaces de translation » que nous considérons dans la section suivante.

## 2. Surfaces de translation

Dans cette section, nous décrivons une construction concrète d'un feuilletage vertical sur une surface munie d'une métrique plate très particulière. Cette métrique est légèrement singulière : elle a un nombre fini de singularités coniques isolées. Le « théorème de redressement » mentionné à la fin de la section précédente affirme que tous les feuilletages mesurés orientables sur des surfaces peuvent être en un sens précis réduits à ceux considérés dans la présente section.

Soit  $\vec{v}_1, \dots, \vec{v}_n$  une collection de vecteurs dans  $\mathbb{R}^2$ . Assemblons ces vecteurs dans une ligne brisée. Formons maintenant une autre ligne brisée en composant

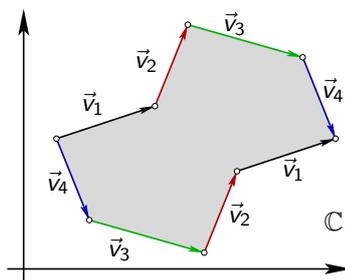


FIG. 2. En identifiant par des translations appropriées tous les couples de côtés parallèles d'un polygone comme sur la figure, nous obtenons une surface plate de genre deux avec une seule singularité conique.

les mêmes vecteurs dans un autre ordre  $\vec{v}_{\pi(1)}, \dots, \vec{v}_{\pi(n)}$ , où  $\pi$  est une permutation de  $n$  éléments. Par construction les deux lignes brisées ont les mêmes extrémités. Supposons que les lignes brisées ne se croisent pas, elles délimitent alors un polygone comme sur la figure 2. En identifiant les couples de côtés représentés par les mêmes vecteurs  $\vec{v}_j$ ,  $j = 1, \dots, n$ , par des translations appropriées, nous obtenons une surface sans bord.

La surface ainsi construite est munie d'une métrique plate héritée de la métrique plate du plan. Dans le cas particulier de  $n = 2$  et de  $\pi = (2, 1)$  nous obtenons un tore plat habituel provenant de l'identification des côtés opposés d'un parallélogramme. Une collection plus grande de vecteurs produit une surface de genre plus grand ; le genre de la surface obtenu est déterminé par la permutation  $\pi$ . Pour simplifier, on ne considérera que des permutations sympathiques, pour lesquelles la surface est non dégénérée ; voir [Ma1] ou [Ve] pour les détails.

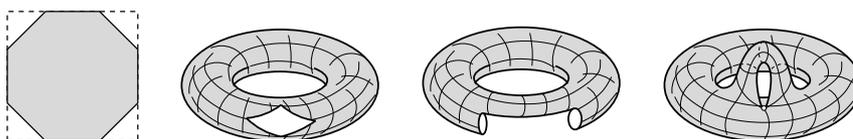


FIG. 3. Un dessin animé montrant le recollement progressif d'une surface de genre deux à partir d'un patron en forme d'octogone régulier.

Par exemple, un octogone régulier produit une surface de genre deux, voir la figure 3. Pour effectuer le recollement progressivement, identifions d'abord les côtés horizontaux et les côtés verticaux entre eux. Nous obtenons un tore habituel (comme celui obtenu par l'identification des côtés opposés d'un carré), sauf que cette fois notre tore aura un trou en forme de petit carré tourné de  $45^\circ$  (voir le deuxième cadre de la figure 3). Nous allons légèrement tricher sur le cadre suivant en prétendant que ce petit trou carré n'est pas tourné. En recollant un couple de côtés parallèles du trou, nous obtenons cette fois un tore avec deux trous isolés (comme sur le troisième cadre). En identifiant le dernier couple de côtés parallèles

(représentant les deux trous) nous obtenons un *tore avec une anse*, autrement dit, une surface de genre deux.

Comme dans le cas du tore, la surface provenant de l'octogone régulier ou d'un octogone comme dans la figure 2 hérite d'une métrique plate. La différence avec le cas du tore est que maintenant la métrique plate a une singularité au point obtenu en identifiant les sommets de l'octogone.

Notons que la métrique plate ainsi obtenue est très particulière : comme toutes les identifications des côtés du polygone sont effectuées par des translations, le transport parallèle d'un vecteur tangent le long d'un chemin fermé amène le vecteur en lui-même. En d'autres termes l'*holonomie* de la métrique est triviale. En particulier, comme le transport parallèle le long d'un petit lacet contournant une singularité conique ne change pas la direction d'un vecteur tangent, l'angle conique de la singularité est un multiple entier de  $2\pi$ . Dans la situation la plus générale notre surface plate aura des singularités coniques d'angles  $2\pi(d_1 + 1), \dots, 2\pi(d_m + 1)$ , où  $d_1 + \dots + d_m = 2g - 2$  (et  $g$  est le genre de la surface).

Nous considérerons que le choix d'une direction verticale (invariante par holonomie) fait partie de notre structure géométrique. Une surface munie d'une métrique plate d'holonomie triviale et d'un choix d'une direction verticale s'appelle une *surface de translation*. Deux polygones obtenus l'un à partir de l'autre par une translation engendrent la même surface de translation, tandis que le même polygone tourné (génériquement) engendre une surface de translation différente.

Nous pouvons considérer le plan  $\mathbb{R}^2$  dans lequel est plongé le patron polygonal d'une surface de translation comme le plan complexe  $\mathbb{C} \simeq \mathbb{R}^2$  muni d'une coordonnée  $z$ . La surface de translation obtenue par l'identification des côtés correspondants du polygone hérite donc d'une structure complexe. Vu que les lois du recollement de côtés sont décrites dans notre coordonnée comme  $z = \tilde{z} + \text{const}$ , nous constatons que la 1-forme fermée  $dz$  est bien définie pas seulement sur le polygone, mais aussi sur la surface de translation recollée. Un exercice d'analyse complexe montre que la structure complexe s'étend aux points provenant de sommets du polygone, et que la 1-forme  $dz$  s'étend en une 1-forme holomorphe sur la surface de Riemann résultante. Cette 1-forme  $\omega$  a des zéros d'ordres  $d_1, \dots, d_m$  exactement aux points où la métrique plate a des singularités coniques d'angles  $2\pi(d_1 + 1), \dots, 2\pi(d_m + 1)$ .

Réciproquement, étant donnée une 1-forme holomorphe  $\omega$  sur une surface de Riemann, nous pouvons choisir une coordonnée locale  $z$  (dans un domaine simplement connexe ne contenant aucun zéro de  $\omega$ ) telle que  $\omega = dz$  dans cette coordonnée. Cette coordonnée est définie à une constante additive près. Elle induit la structure d'une surface de translation sur la surface de Riemann. En dessinant sur la surface des coupures appropriées qui joignent les singularités coniques sans se recouper, nous pouvons déplier la surface de translation pour obtenir un polygone dans le plan  $\mathbb{C}$ .

Cette construction montre que les deux structures géométriques sont complètement équivalentes : la métrique plate plus le choix d'une direction verticale, ou la structure de surface de Riemann avec une 1-forme holomorphe. Le système dynamique que l'on cherche à comprendre sur un tel objet est le flot vertical, c'est-à-dire le déplacement à vitesse constante dans la direction verticale.

### 3. Familles de surfaces de translation et dynamique dans l'espace des modules

Le patron polygonal utilisé dans notre construction d'une surface plate dépend continûment des vecteurs  $\vec{v}_i$ . Cela implique que la topologie de la surface de translation recollée à partir du polygone (notamment, son genre  $g$  ainsi que le nombre et le type des singularités coniques) persiste après une petite perturbation des vecteurs  $\vec{v}_i$ . Pour chaque collection d'angles coniques  $2\pi(d_1 + 1), \dots, 2\pi(d_m + 1)$  vérifiant  $d_1 + \dots + d_m = 2g - 2$  avec  $d_i$  entiers pour  $i = 1, \dots, m$ , nous obtenons une famille  $\mathcal{H}(d_1, \dots, d_m)$  de surfaces de translation. Les vecteurs  $\vec{v}_1, \dots, \vec{v}_n$  peuvent être considérés comme des coordonnées complexes dans cet espace, et s'appellent *coordonnées cohomologiques*. Ces coordonnées définissent une structure d'*orbifold complexe* (une variété avec des singularités modérées) sur chaque famille  $\mathcal{H}(d_1, \dots, d_m)$ . La géométrie et la topologie de ces espaces de surfaces plates sont loin d'être pleinement explorées.

Cette description en termes de patrons polygonaux suffit amplement pour lire la suite de cet article. Néanmoins, si des lecteurs préfèrent le langage de la géométrie algébrique, ils peuvent voir la famille des surfaces de translation avec des angles coniques fixés  $2\pi(d_1 + 1), \dots, 2\pi(d_m + 1)$  comme une strate  $\mathcal{H}(d_1, \dots, d_m)$  dans l'espace des modules  $\mathcal{H}_g$  des couples (surface de Riemann  $C$  ; 1-forme holomorphe  $\omega$  sur  $C$ ), où la strate est définie par la collection des degrés  $d_1, \dots, d_m$  des zéros de la forme  $\omega$  ; ici  $d_1 + \dots + d_m = 2g - 2$ . Tandis que l'espace des modules  $\mathcal{H}_g$  est un  $\mathbb{C}^g$ -fibré holomorphe ayant comme base l'espace des modules  $\mathcal{M}_g$  des surfaces de Riemann, les strates individuelles n'ont pas en général de structure de fibré. Par exemple, la strate minimale  $\mathcal{H}(2g - 2)$  (où il y a une unique singularité conique d'angle maximal) a une dimension complexe  $2g$  alors que l'espace des modules  $\mathcal{M}_g$  a une dimension complexe  $3g - 3$ . La seule existence d'une forme holomorphe avec un seul zéro d'ordre  $2g - 2$  sur une surface de Riemann  $C$  impose déjà des contraintes fortes sur  $C$ .

Pour compléter cette description des espaces de surfaces de translation, nous devons ajouter une structure extrêmement importante pour la suite : l'action du groupe  $GL(2, \mathbb{R})$  sur  $\mathcal{H}(d_1, \dots, d_m)$ . Cette action est particulièrement simple à décrire en terme du patron polygonal  $\Pi$  d'une surface de translation  $S$ . Une matrice  $g \in GL(2, \mathbb{R})$  agit linéairement sur le plan  $\mathbb{R}^2$  ; cette action transforme le polygone  $\Pi$  en un nouveau polygone  $g\Pi$ . Les côtés du nouveau polygone  $g\Pi$  viennent encore par paires de côtés parallèles entre eux et de même longueur. Cela signifie que nous pouvons recoller par paires les côtés du nouveau polygone  $g\Pi$  par des translations appropriées, pour obtenir une nouvelle surface de translation que nous appelons  $gS$ . La définition de  $gS$  ne dépend pas du choix du polygone  $\Pi$  qui déplie  $S$  : tout patron polygonal de  $S$  produira la même surface de translation  $gS$ . Notons que nous avons utilisé le choix d'une direction verticale dans notre construction pour faire agir la matrice  $g$ .

Le sous-groupe  $SL(2, \mathbb{R}) \subset GL(2, \mathbb{R})$  préserve l'aire (définie à partir de la métrique plate) d'une surface de translation. Cela implique que l'action de  $SL(2, \mathbb{R})$  préserve l'hypersurface réelle  $\mathcal{H}_1(d_1, \dots, d_m)$  des surfaces de translation d'aire 1 dans chaque strate  $\mathcal{H}(d_1, \dots, d_m)$ . L'espace  $\mathcal{H}_1(d_1, \dots, d_m)$  est analogue à une sphère unitaire (ou plutôt à un hyperboloïde unitaire) dans l'espace ambiant  $\mathcal{H}(d_1, \dots, d_m)$ .

Rappelons que sous certaines restrictions naturelles sur la permutation  $\pi$ , les  $n$  vecteurs

$$\vec{v}_1 = \begin{pmatrix} v_{1,x} \\ v_{1,y} \end{pmatrix}, \dots, \vec{v}_n = \begin{pmatrix} v_{n,x} \\ v_{n,y} \end{pmatrix},$$

comme dans la figure 2, définissent des coordonnées locales dans l'espace  $\mathcal{H}(d_1, \dots, d_m)$  des surfaces de translation.

Soit  $d\nu := dv_{1,x}dv_{1,y} \dots dv_{n,x}dv_{n,y}$  l'élément de volume associé à nos coordonnées. Il est facile de vérifier qu'en fait  $d\nu$  ne dépend pas du choix du patron polygonal définissant des coordonnées  $\vec{v}_1, \dots, \vec{v}_n$ . Il est par conséquent correctement défini, partout sur l'espace  $\mathcal{H}(d_1, \dots, d_m)$ .

La mesure de Lebesgue dans un espace euclidien induit une mesure sur toutes les hypersurfaces de cet espace. De même, la mesure  $\nu$  induit ici un élément de volume  $\nu_1$  sur l'hyperboloïde unitaire  $\mathcal{H}_1(d_1, \dots, d_m)$ . Il est facile de vérifier que l'action du groupe  $SL(2, \mathbb{R})$  préserve l'élément de volume  $d\nu_1$ .

Le théorème suivant démontré indépendamment et simultanément par H. Masur [Ma1] et par W. Veech [Ve] est le résultat clé dans ce domaine.

**Théorème** (H. Masur ; W. Veech). *Le volume total de chaque strate  $\mathcal{H}_1(d_1, \dots, d_m)$  est fini.*

*Le groupe  $SL(2, \mathbb{R})$  et son sous-groupe diagonal agissent ergodiquement sur chaque composante connexe de chaque strate  $\mathcal{H}_1(d_1, \dots, d_m)$ .*

En genre 1, l'espace des modules des surfaces de translation d'aire 1 s'identifie à  $SL(2, \mathbb{R})/SL(2, \mathbb{Z})$ . Ainsi, la première assertion généralise le fait bien connu que  $SL(2, \mathbb{R})/SL(2, \mathbb{Z})$  est de volume fini.

Ici « ergodiquement » signifie que chaque ensemble mesurable invariant sous l'action du groupe a soit une mesure nulle soit une mesure pleine. D'après le théorème ergodique, sous ces hypothèses, l'orbite de presque tout point remplit l'espace ambiant de façon homogène. Dans notre situation concrète l'ergodicité de l'action du groupe implique entre autres la propriété suivante. Pour presque chaque polygone comme sur la figure 2 nous pouvons choisir une suite  $t_i$  de temps telle qu'en contractant le polygone verticalement par le facteur  $e^{t_i}$  et en le dilatant horizontalement par le même facteur  $e^{t_i}$  et en appliquant ensuite au polygone modifié quelques transformations (bien choisies) de découpage et de recollage (voir la figure 4) nous pouvons obtenir un polygone arbitrairement proche de l'octogone régulier tourné de n'importe quel angle choisi à l'avance.

Tout est enfin prêt pour présenter le premier trésor de notre histoire. Supposons que nous cherchons certaines propriétés fines du flot vertical sur une surface de translation individuelle. En appliquant une homothétie si nécessaire, nous pouvons supposer que la surface de translation est d'aire 1. Howard Masur et William Veech proposent l'approche suivante pour étudier le flot vertical. Considérons notre surface de translation  $S$  (munie du choix de direction verticale) comme un point dans la strate ambiante  $\mathcal{H}_1(d_1, \dots, d_m)$ . Considérons l'orbite  $SL(2, \mathbb{R}) \cdot S$  (ou, selon le contexte, l'orbite de  $S$  sous l'action du sous-groupe diagonal  $\begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}$ ). De nombreuses propriétés importantes du flot vertical sur  $S$  sont reflétées par des propriétés géométriques de l'adhérence de l'orbite correspondante. Cette approche a mis l'étude des adhérences d'orbites de  $SL(2, \mathbb{R})$  et de leur géométrie au centre de

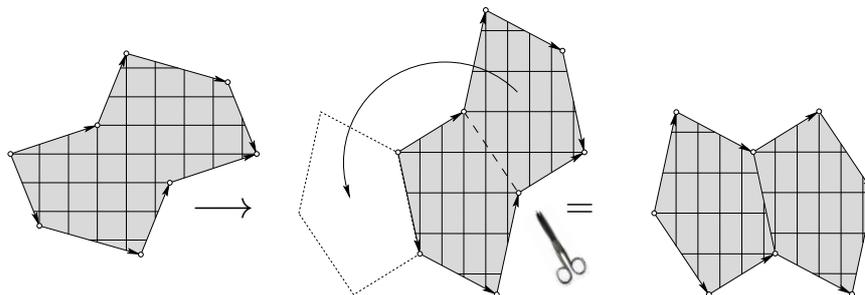


FIG. 4. Notons que la transformation de dilatation-contraction (l'action du sous-groupe diagonal) change la surface de translation tandis que la modification du patron par découpage-recollage ne la change pas.

la recherche dans ce domaine depuis les trois dernières décennies. Pour illustrer la puissance de cette approche sur un exemple nous présentons le critère de Masur d'unique ergodicité du flot vertical.

À la fin des années 60 et au début des années 70 quelques chercheurs (incluant W. Veech, M. Keane, A. Katok) ont découvert (dans des termes différents et dans un contexte différent) le phénomène que nous allons illustrer dans l'exemple suivant. Considérons une surface de translation comme sur la figure 5, où le rectangle a les dimensions  $1 \times 2$ , et les coupures ont une longueur irrationnelle. On recolle la partie gauche de la première coupure à la partie droite de la seconde, et inversement. (Nous ne sommes pas restreints aux patrons comme sur la figure 2 dans nos constructions des surfaces de translation : par exemple, nous pouvons assembler une telle surface en partant de triangles plongés dans le plan euclidien, à condition que tous les recollements de triangles soient des translations.)

Il s'avère que pour une collection non dénombrable de directions, le flot linéaire dans ces directions est minimal (chaque orbite est dense), mais n'est pas ergodique : certaines trajectoires passent la plupart du temps dans la partie centrale de la surface, tandis que les autres passent la plupart du temps dans la partie complémentaire (voir [Ma2] pour les détails). Clairement, en appliquant une rotation appropriée à la surface de translation de la figure 5 nous pouvons mettre une direction non ergodique en position verticale.

Ayant illustré cet étrange phénomène, nous sommes prêts à présenter le critère de Masur d'unique ergodicité du flot vertical.

**Théorème (H. Masur).** *Soit  $S$  une surface de translation. Supposons que le flot dans la direction verticale sur  $S$  n'est pas uniquement ergodique. Alors, la trajectoire de  $S$  (considérée comme un point de l'espace ambiant de surfaces de translation,  $\mathcal{H}(d_1, \dots, d_m)$ ) sous l'action du sous-groupe diagonal quitte à partir d'un certain rang tout sous-ensemble compact  $K$ . Autrement dit, pour chaque partie compacte  $K \subset \mathcal{H}(d_1, \dots, d_m)$ , il existe un temps  $t_0$  tel que pour tout  $t > t_0(K)$  nous avons  $g_t \cdot S = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \cdot S \notin K$  : la trajectoire s'échappe à l'infini.*

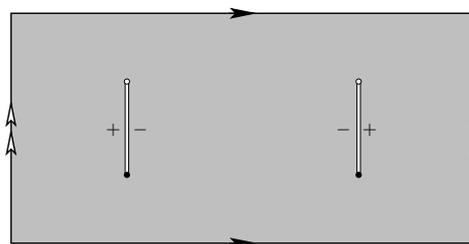


FIG. 5. Pour des directions appropriées du flot linéaire sur cette surface de translation toutes les trajectoires sont denses, mais le flot n'est pas ergodique : des trajectoires sont distribuées sur la surface de façon *non uniforme* !

(En fait, l'énoncé est encore plus fort : la projection de la trajectoire  $g_t \cdot S$  sur l'espace de modules des surfaces de Riemann  $\mathcal{M}_g$  quitte tout sous-ensemble compact de  $\mathcal{M}_g$  à partir d'un certain rang.)

Le flot vertical sur la surface de translation de la figure 5 est périodique, et donc extrêmement non-ergodique. Effectivement, l'action du sous-groupe diagonal transforme notre tore avec deux coupures en tore de plus en plus long et de plus en plus étroit. Dans ce cas la famille  $\{g_t \cdot S\}_{t>0}$  de surfaces déformées quitte chaque sous-ensemble compact de l'espace des modules d'une façon particulièrement transparente : une géodésique plate fermée est écrasée par le flot  $g_t$ . D'après le critère de Masur, les exemples minimaux et non ergodiques mentionnés ci-dessus correspondent à certains angles  $\theta$  tels que le flot  $g_t$  appliqué à la surface de translation  $S$  tournée par la rotation  $r_\theta$  quitte à partir d'un certain rang toute partie compacte.

À première vue, nous avons juste réduit l'étude d'un système dynamique relativement simple — le flot vertical sur une surface de translation — à l'étude d'un système dynamique vraiment compliqué : l'étude de l'action du groupe  $GL(2, \mathbb{R})$  sur l'espace  $\mathcal{H}(d_1, \dots, d_m)$ . Pourtant, cette approche s'est avérée être incroyablement fructueuse et puissante, et cela malgré le fait que ni la géométrie ni la topologie des espaces de surfaces de translation ne soient encore suffisamment explorées. Par exemple, Kerckhoff, Masur et Smillie ont démontré dans [KMS] en utilisant le critère de Masur que, pour toute surface de translation, l'ensemble des directions  $\theta$  dans lesquelles le flot linéaire est uniquement ergodique est de mesure de Lebesgue pleine. Notons qu'on ne connaît aucune preuve de ce résultat qui ne passe pas par la dynamique dans l'espace des modules ! Ainsi, pour l'exemple de la figure 5, l'ensemble des mauvaises directions (qu'on sait être indénombrable) est malgré tout assez petit.

Cette approche est extrêmement efficace. Cependant, comme nous allons l'expliquer dans la section suivante, il faut un outil supplémentaire pour la transformer en science systématique encore plus puissante : c'est le théorème de la baguette magique démontré par A. Eskin et M. Mirzakhani (ainsi que son extension due à A. Eskin, M. Mirzakhani et A. Mohammadi).

#### 4. « Presque tout » contre « tout »

Même pour les classes de systèmes dynamiques les mieux comprises, toute prévision sur « le sort d'une particule au bout d'une longue période de temps » contient toujours une version du mot « typiquement », signifiant habituellement « pour un ensemble de données initiales de mesure pleine ». Le gros problème (qui selon le point de vue peut être interprété comme un avantage : la théorie ergodique n'est pas sensible aux fluctuations hasardeuses) est que même pour les systèmes dynamiques les mieux étudiés, où nous avons acquis des connaissances à peu près complètes sur le comportement « générique » des trajectoires, nous sommes incapable de dire quoi que ce soit sur une trajectoire individuelle concrète : il n'y a pas de moyen de déterminer si les données initiales particulières sont « génériques » ou pas. Quand vous réalisez en boucle des milliers d'expériences avec des données de départ aléatoires et établissez une certaine statistique, vous n'êtes pas concerné par des fluctuations occasionnelles atypiques. Par contre, si vous êtes préoccupé par le destin d'un astéroïde B612 particulier, et seulement par cela, la plupart des méthodes de systèmes dynamiques deviennent complètement inutiles pour vous.

La difficulté est conceptuelle; elle n'est liée ni au manque de connaissances dans l'état actuel du développement des mathématiques ni à la présence inévitable de bruit ou de friction en systèmes dynamiques réalistes. Même pour les systèmes absolument déterministes, et même en imposant toutes les abstractions nécessaires comme l'absence de bruit ou de friction, le problème est toujours là.

La raison est que pour la plupart des systèmes dynamiques (y compris très lisses et gentils) certaines trajectoires individuelles sont extrêmement complexes. Notamment, elles peuvent remplir des ensembles fractals au bout d'une grande échelle de temps.

Par exemple, l'application  $f : x \mapsto \{2x\}$  enroulant un cercle  $S^1 = \mathbb{R}/\mathbb{Z}$  deux fois autour de lui-même d'une façon homogène a des orbites remplissant des ensembles de Cantor de pratiquement toute dimension de Hausdorff entre 0 et 1. La même application a des orbites infinies évitant certains arcs du cercle, etc. Autrement dit, cette application très simple a certaines orbites (rares) avec un comportement très bizarre.

Toutes ces propriétés deviennent nettement mieux visibles en passant à la représentation binaire (au lieu de décimale) d'un nombre réel  $x \in [0, 1[$ . Écrivons

$$x = \frac{n_1}{2} + \cdots + \frac{n_k}{2^k} + \cdots,$$

où tous les chiffres binaires  $n_k$  sont des zéros ou des un. L'application  $f$  agit sur la suite  $(n_1, n_2, \dots, n_k, \dots)$  en effaçant le premier chiffre. (Cette opération sur les suites semi-infinies de zéros et de un s'appelle *décalage de Bernoulli*.) Ce codage montre qu'on a une liberté presque totale pour prescrire le comportement de certaines orbites.

Le flot géodésique sur toute surface de Riemann de courbure négative constante a un comportement similaire. H. Furstenberg et B. Weiss ont observé que les adhérences de trajectoires individuelles peuvent atteindre pratiquement toutes les dimensions de Hausdorff entre 1 (pour des trajectoires fermées) et 3 (pour des trajectoires génériques).

Le flot linéaire sur un tore  $\mathbb{T}^n = \mathbb{R}^n / \mathbb{Z}^n$  est l'exemple exceptionnel d'un système dynamique pour lequel l'adhérence de *chaque* orbite est une variété symplectique. Soit  $\vec{V} = (V_1, \dots, V_n)$  la direction du flot. L'adhérence de *toute* orbite du flot dans la direction  $\vec{V}$  est un sous-tore  $\mathbb{T}^k$ , où  $1 \leq k \leq n$  est le degré d'irrationalité  $k = \dim_{\mathbb{Q}}\{V_1, \dots, V_n\}$  de la direction choisie. Dans le cas particulier d'un tore de dimension  $n = 2$ , toutes les trajectoires dans une direction rationnelle sont déjà fermées — elles forment des cercles  $S^1 = \mathbb{T}^1$ ; l'adhérence de toute orbite dans une direction irrationnelle donne tout le tore  $\mathbb{T}^2$ . Il n'y a rien de surprenant à cela : le tore est un espace homogène, et le groupe d'automorphismes du tore préservant le flot agit transitivement sur le tore.

En un certain sens, jusqu'à présent les dynamiciens ne connaissaient qu'une seule classe de systèmes dynamiques pour lesquels il était possible de trouver l'adhérence de chaque orbite, et pour lesquels la liste de toutes les adhérences possibles était réduite à quelques variétés lisses concrètes comme dans l'exemple du flot linéaire sur le tore  $\mathbb{T}^n$  : c'est le cas pour certains systèmes dynamiques d'origine algébrique dans des espaces homogènes, c'est-à-dire des espaces quotients d'un groupe de Lie, dans lesquels tous les points sont équivalents. Un des énoncés clé dans cette théorie a été démontré par Marina Ratner ; des contributions très importantes ainsi que des applications fantastiques (notamment en théorie des nombres) ont été développées par S. G. Dani, G. Margulis, et d'autres mathématiciens de premier plan, incluant A. Eskin, S. Mozes, et N. Shah. Le spectre des applications de cette théorie aux différentes branches des mathématiques ne cesse d'augmenter. Ce n'est pas étonnant : des espaces homogènes apparaissent partout en mathématiques ! (Et la théorie et la liste des chercheurs qui l'ont créée mériteraient un article individuel plutôt qu'un seul paragraphe.)

## 5. Le théorème de la baguette magique

Nous arrivons finalement au résultat central de cet article, obtenu récemment par Alex Eskin et de Maryam Mirzakhani [EMi] (intégrant également le résultat commun de ces auteurs et d'Amir Mohammadi [EMiMh]).

Il est bien connu que l'espace des modules *n'est pas* un espace homogène. Cependant, les adhérences d'orbites de  $GL(2, \mathbb{R})$  dans des espaces de surfaces de translation sont aussi belles qu'on peut l'espérer : ce sont des variétés complexes ayant éventuellement quelques singularités modérées (plus précisément, des orbifolds complexes). Dans ce sens, l'action des groupes  $GL(2, \mathbb{R})$  et  $SL(2, \mathbb{R})$  sur les espaces de surfaces de translation imite certaines propriétés des systèmes dynamiques dans les espaces homogènes décrits dans la section précédente.

**Théorème de la baguette magique.** *Considérons l'action de  $GL(2, \mathbb{R})$  sur une famille de surfaces de translation  $\mathcal{H}(d_1, \dots, d_m)$ .*

*L'adhérence de toute  $GL(2, \mathbb{R})$ -orbite est un sous-orbifold complexe (éventuellement avec des auto-croisements); dans les coordonnées cohomologiques  $\vec{v}_1, \dots, \vec{v}_n$ , elle est localement représentée par un sous-espace affine.*

*Considérons de plus l'hypersurface  $\mathcal{H}_1(d_1, \dots, d_m)$  des surfaces de translation d'aire un, et une mesure de probabilité  $\mu_1$  sur  $\mathcal{H}_1(d_1, \dots, d_m)$  invariante et ergodique sous l'action de  $SL(2, \mathbb{R})$ . Alors le support d'une telle mesure est également un sous-orbifold. Dans les coordonnées  $\vec{v}_1, \dots, \vec{v}_n$  ce sous-orbifold est représenté*

par l'intersection  $E \cap \mathcal{H}_1(d_1, \dots, d_m)$  où  $E$  est un sous-espace affine invariant par  $GL(2, \mathbb{R})$  comme ci-dessus. De plus,  $\mu_1$  est (à multiplication scalaire près) la mesure induite par la mesure affine de  $E$  sur  $E \cap \mathcal{H}_1(d_1, \dots, d_m)$ .

Comme une vague conjecture (ou plutôt comme un rêve très optimiste) ces propriétés ont longtemps été discutées, mais les experts n'avaient pas la moindre idée d'une démonstration générale. La seule exception est le cas des surfaces de genre deux, où il y a dix ans Curt McMullen a obtenu un résultat très précis [Mc1] classifiant toutes les adhérences des orbites. Il a utilisé, entre autres, la lourde artillerie du théorème de Ratner astucieusement appliquée dans ce cas particulier. Cependant, le résultat de McMullen repose sur des propriétés spécifiques des surfaces de genre deux qui ne s'étendent pas aux genres supérieurs.

La démonstration d'Alex Eskin et de Maryam Mirzakhani est un travail gigantesque qui a pris plusieurs années. Ce travail repose sur de nombreux développements fondamentaux à propos de systèmes dynamiques qui n'ont pas de rapport visible avec les espaces de modules. Pour n'en citer que quelques-uns, la preuve intègre certaines idées de la méthode de basse entropie de M. Einsiedler, A. Katok, E. Lindenstrauss; des résultats de G. Forni et de M. Kontsevich sur les exposants de Lyapunov du flot géodésique de Teichmüller; des idées provenant des travaux de Y. Benoit et de J.-F. Quint sur les mesures stationnaires pour les marches aléatoires sur les groupes; l'amélioration itérative des propriétés de la mesure inspirée par l'approche de G. Margulis et de G. Tomanov pour étudier les actions des flots unipotents sur les espaces homogènes; certains résultats ergodiques fins développés par Y. Guivarch et A. Raugi. Notons que, comme dans le cas du théorème de Ratner, l'énoncé topologique sur l'adhérence des orbites s'appuie sur la classification des mesures invariantes.

Que pouvons-nous faire maintenant que le théorème est démontré? Dans certaines situations ce théorème fonctionne comme une baguette magique, qui permet de toucher *tout* billard donné dans certaines classes de billards et, en théorie (et de plus en plus souvent dans la pratique), de trouver l'adhérence de l'orbite correspondante dans l'espace des modules des surfaces de translation. La géométrie de cette adhérence de l'orbite permet de répondre à pratiquement toutes les questions intéressantes sur le billard initial.

Supposons par exemple que vous voulez étudier le billard dans un plan rempli périodiquement avec des obstacles comme sur la figure 6 (voir l'article de P. Hubert et de R. Krikorian [HuKr] dans le même numéro de la *Gazette* discutant un tel modèle *windtree*).

Une trajectoire peut partir loin, puis revenir relativement près du point de départ, puis faire d'autres longues excursions. Le *taux de diffusion*  $\nu$  décrit la vitesse moyenne  $T^\nu$  à laquelle la trajectoire se propage dans le plan sur une grande échelle de temps  $T \gg 1$ . Plus formellement,

$$\nu := \limsup_{T \rightarrow \infty} \frac{\log(\text{diamètre du segment de la trajectoire pour le temps } [0, T])}{\log T}.$$

Pour la marche aléatoire habituelle dans le plan, ou pour un billard avec des obstacles périodiques ronds, le taux de diffusion est connu :  $\nu = \frac{1}{2}$  (ce qui correspond au théorème central limite usuel). Le point le plus éloigné d'un morceau de trajectoire pour l'intervalle de temps  $[0, T]$  est situé à peu près à une distance  $\sqrt{T}$  du

point de départ. (Nous ne discutons pas du moment  $t_0 \in [0, T]$  où la trajectoire est aussi loin.)

Le théorème de la baguette magique (combiné avec des résultats supplémentaires) permet de démontrer que pour *toute* forme d'obstacle comme dans la figure 6, le taux de diffusion  $\nu$  est le même pour tous les points de départ et pour presque toutes les directions. En outre, on peut même calculer le taux de diffusion ! Pour effectuer cette tâche il faut procéder comme suit. Trouvez la surface de translation  $S$  associée au billard, c'est facile. En utilisant le théorème de la baguette magique (ainsi que son développement par A. Wright [W]) trouvez l'adhérence  $\mathcal{L}$  de l'orbite correspondante sous l'action de  $GL(2, \mathbb{R})$ , dans l'espace des modules des surfaces de translation. Par un théorème très récent de J. Chaika et de A. Eskin [ChE], presque toutes les directions pour *toute* surface de translation sont Lyapunov-génériques; il suffit donc de retrouver l'exposant de Lyapunov approprié du « flot géodésique de Teichmüller » sur  $\mathcal{L}$ , et le problème est résolu ! (Voir les détails sur le modèle windtree et sur les exposants de Lyapunov dans l'article de P. Hubert et de R. Krikorian [HuKr] dans le même numéro de la *Gazette*.)

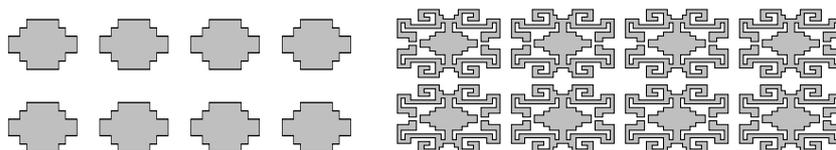


FIG. 6. Le taux de diffusion dépend seulement du nombre d'angles pour presque tout obstacle symétrique comme sur la figure.

Notamment, pour presque tout obstacle symétrique ayant  $4m - 4$  angles de  $3\pi/2$  et  $4m$  angles de  $\pi/2$ , V. Delecroix et l'auteur ont démontré que le taux de diffusion est

$$\frac{(2m)!!}{(2m+1)!!} \sim \frac{\sqrt{\pi}}{2\sqrt{m}} \quad \text{quand } m \rightarrow \infty.$$

Cela répond à une question posée par J.-C. Yoccoz, qui voulait savoir si le taux de diffusion pouvait être arbitrairement petit pour certaines formes d'obstacles, et développe la réponse originale pour  $m = 1$  obtenue dans [DHL].

Une autre application du théorème de la baguette magique qui est facile à décrire est une avancée dans le *problème d'illumination*. Ce problème demande si une pièce (en dimension 2 pour simplifier) dont les murs sont des miroirs peut toujours être complètement éclairée par une source de lumière placée en un seul point. R. Penrose a conçu en 1958 le plan d'une salle aux murs en miroirs plats et elliptiques qui a toujours des régions sombres, indépendamment de l'endroit où vous placez une bougie dans cette salle. En 1995, G. Tokarsky a construit une salle polygonale avec une propriété similaire (bien que plus faible) : il reste un point noir si la bougie idéalisée est placée à un point bien choisi. En s'appuyant sur le théorème de la baguette magique, S. Lelièvre, T. Monteil, et B. Weiss ont démontré dans [LMtW] que pour toute surface de translation  $M$ , et pour tout point  $x \in M$ , l'ensemble des points  $y$  non éclairés par  $x$  est toujours fini.

Il ne faut pas avoir l'impression que la théorie développée par A. Eskin, M. Mirzakhani, A. Mohammadi et d'autres chercheurs dans ce domaine a été développée dans l'optique de comprendre les billards. Un billard dans un polygone est juste une jolie façon de décrire certaines classes de systèmes dynamiques ; nous avons vu que des systèmes dynamiques de même nature apparaissent dans la théorie de la conductivité, en modèles de gaz, etc.

Le résultat de A. Eskin et de M. Mirzakhani ouvre de nouveaux horizons dans l'étude des espaces de modules qui, durant ces dernières décennies, ont attiré l'intérêt à la fois des mathématiciens et des physiciens. Nous ne connaissons pas encore toutes les applications possibles du théorème de la baguette magique qui pourraient être obtenues dans cette direction.

Le calcul intégral a été partiellement développé par Kepler (un siècle avant Newton et Leibniz) afin de mesurer le volume de fûts de vin. Qui pouvait imaginer à cette époque que le volume d'un solide de révolution serait traité dans tous les manuels de mathématiques pour débutants et que le calcul intégral deviendrait un élément essentiel de toute l'ingénierie contemporaine ? Le théorème prouvé par Alex Eskin et Maryam Mirzakhani est si beau et puissant que, personnellement, je n'ai aucun doute qu'il trouvera de nombreuses applications bien au-delà de notre imagination actuelle.

## 6. Références

- [ALK] M. Ya. Azbel, I. M. Lifshits, M. I. Kaganov. *Electron Theory of Metals*. Consultants Bureau (1973).
- [Ca] E. Calabi, *An intrinsic characterization of harmonic 1-forms*, *Global Analysis*, In : D. C. Spencer and S. Iyanaga (ed) *Papers in Honor of K. Kodaira (1969)*, 101–117.
- [ChE] J. Chaika, A. Eskin, *Every flat surface is Birkhoff and Osceledets generic in almost every direction*, *arXiv* :1305.1104 (2013), 1–19.
- [DHL] V. Delecroix, P. Hubert, S. Lelièvre, *Diffusion for the periodic wind-tree model*, *Annales de l'Éns*, **47** :6 (2014), *arXiv* :1107.1810 (2011).
- [EMi] A. Eskin, M. Mirzakhani, *Invariant and stationary measures for the  $SL(2, \mathbb{R})$  action on Moduli space*, *arXiv* :1302.3320 (2013), 1–172.
- [EMiMh] A. Eskin, M. Mirzakhani, A. Mohammadi, *Isolation, equidistribution, and orbit closures for the  $SL(2, \mathbb{R})$  action on Moduli space*, *arXiv* :1305.3015 (2013), 1–46.
- [G] É. Ghys, *Maryam Mirzakhani, médaille Fields 2014*, *Images des Mathématiques*, CNRS (2014), [http ://images.math.cnrs.fr/Maryam-Mirzakhani-medaille-Fields.html](http://images.math.cnrs.fr/Maryam-Mirzakhani-medaille-Fields.html).
- [HdMa] J. Hubbard and H. Masur, *Quadratic differentials and measured foliations*, *Acta Math.*, **142** (1979), 221–274.
- [HuKr] P. Hubert, R. Krikorian, *Artur Avila, un génie carioca à Paris*, *Gazette des Mathématiciens*, **142** (2014).
- [ICM] ICM laudation, [http ://www.icm2014.org/en/awards/prizes/f4](http://www.icm2014.org/en/awards/prizes/f4)
- [Ka] A. Katok, *Invariant measures of flows on oriented surfaces*, *Soviet Math. Dokl.*, **14** (1973), 1104–1108.
- [KMS] S. Kerckhoff, H. Masur and J. Smillie, *Ergodicity of billiard flows and quadratic differentials*, *Annals of Math.*, **124** (1986), 293–311.
- [KI] E. Klarreich, *A Tenacious Explorer of Abstract Surfaces*, *Quanta Magazine*, August 12, 2014, [http ://www.simonsfoundation.org/quanta/20140812-a-tenacious-explorer-of-abstract-surfaces/](http://www.simonsfoundation.org/quanta/20140812-a-tenacious-explorer-of-abstract-surfaces/).
- [LMtW] S. Lelièvre, T. Monteil, B. Weiss, *Everything is illuminated*, *arXiv* :1407.2975 (2014), 1–16.
- [Ma1] H. Masur, *Interval exchange transformations and measured foliations*, *Ann. of Math.* **115** (1982), 169–200.

- [Ma2] H. Masur, *Ergodic Theory of Translation Surfaces*, In : B. Hasselblatt and A. Katok (ed) Handbook of Dynamical Systems, Vol. 1B Elsevier Science B.V., Amsterdam, 527–547 (2006).
- [MINo] A. Ya Maltsev and S. P. Novikov, *Quasiperiodic functions and dynamical systems in quantum solid state physics*, Bull Braz Math Soc, New Series **34(1)** (2003), 171–210.
- [Mc1] C. McMullen, *Dynamics of  $SL(2, \mathbb{R})$  over moduli space in genus two*, *Ann. of Math.* (2) **165** (2007), n° 2, 397–456.
- [Mc2] C. McMullen, *The mathematical work of Maryam Mirzakhani*, Proceedings of the International Congress of Mathematicians, (Seoul, 2014), à paraître. <http://www.math.harvard.edu/~ctm/papers/home/text/papers/icm14/icm14.pdf>
- [Ve] W. A. Veech : *Gauss measures for transformations on the space of interval exchange maps*, *Annals of Math.*, **115** (1982), 201–242.
- [W] A. Wright, *Cylinder deformations in orbit closures of translation surfaces*, arXiv :1302.4108 (2013), 1–24. À paraître dans *Geometry and Topology*.

**Remerciements.** *Je tiens à remercier Jon Chaika, Alex Eskin, et Pascal Hubert pour leurs précieux commentaires. Je suis extrêmement reconnaissant à Sébastien Gouëzel, à Curt McMullen, et à mon père, Vladimir Zorich, qui ont lu attentivement la version préliminaire de cet article et ont fait de nombreuses remarques importantes qui ont contribué à améliorer à la fois le contenu et la présentation. J'ai beaucoup apprécié l'aide de Gwen Le Floc'h et de Sébastien Gouëzel pour des milliers de corrections de mes erreurs en français et pour leur travail littéraire avec ce texte.*

*Je remercie Maryam Mirzakhani pour la baguette magique et pour les photos.*

## Artur Avila, un génie carioca à Paris

P. Hubert<sup>1</sup>, R. Krikorian<sup>2</sup>

---



De nationalité franco-brésilienne, Artur Avila est né en 1979 à Rio de Janeiro. Sous la direction de Welington de Melo, il y a préparé sa thèse, à l'IMPA, et l'a soutenue en 2001. Il a ensuite fait un post-doctorat (2001-03) au Collège de France avec Jean-Christophe Yoccoz. Il a été recruté en 2003 comme Chargé de recherche au CNRS (LPMA, université Pierre et Marie Curie). Il est depuis 2009 Directeur de recherche au CNRS à l'IMJ, université Denis Diderot et détenteur de la chaire Arminio Fraga à l'IMPA.

Artur Avila a reçu la médaille Fields à l'ICM de Séoul 2014. Il avait auparavant obtenu de nombreux prix internationaux dont voici les principaux :

- médaille d'or des Olympiades Internationales de Mathématiques de Toronto (1995)
- cours Peccot (2005)
- conférencier invité au Congrès International de Physique Mathématique
- médaille de bronze du CNRS (2006)
- prix Salem (2006),
- Research Fellow du Clay Mathematics Institute
- Wolff Memorial Lectures at Caltech (2008)

---

<sup>1</sup> Université d'Aix-Marseille, Institut de Mathématique de Marseille.

<sup>2</sup> Sorbonne Universités, UPMC Université Paris 6, UMR7599, LPMA, Paris.

- conférencier invité au Congrès Européen de Mathématiques
- prix de la Société Européenne de Mathématiques (2008)
- grand prix Jacques Herbrand décerné par l'Académie des Sciences (2009)
- conférence plénière au Congrès International des Mathématiciens (ICM), Hyderabad (2010)
- Porter Lectures at Rice, 2010,
- Blyth lectures at Toronto (2011)
- prix Michael Brin (2011)
- AMP Early Career Award (2012)
- prêmio da SBM (2013)
- TWAS Prize (2013)
- Bellow Lectures Northwestern (2014).

Artur Avila travaille dans plusieurs branches des systèmes dynamiques. Ses sujets de prédilection sont la dynamique holomorphe unidimensionnelle (sujet par lequel il a débuté), les cocycles quasi-périodiques, la dynamique dans les espaces de Teichmüller et la dynamique des systèmes conservatifs. Il a écrit plus de 65 articles, dans les meilleurs journaux mathématiques, qui ont pour la plupart eu un impact considérable sur la théorie des systèmes dynamiques et de façon plus générale sur les mathématiques.

Artur est un « problem solver » qui a une imagination hors du commun et des idées fulgurantes, mais il a également su poser de nouvelles problématiques comme nous allons le voir dans ce texte. Souvent, un argument d'apparence simple, la plupart du temps de nature géométrique, lui permet d'aller au-delà de ce que l'on savait faire auparavant, même si la mise en œuvre technique peut s'avérer assez compliquée (mais cela n'est pas un problème pour Artur qui est virtuose dans ce domaine également). Cette impression de simplicité dans son approche des problèmes, le fait qu'il soit très accessible et disponible font que travailler avec lui est un véritable plaisir.

Plutôt que de présenter de façon exhaustive les travaux d'Artur dans tous les domaines des systèmes dynamiques qu'il a abordés, nous avons choisi de n'évoquer dans ce bref article que deux de ses contributions importantes : la simplicité du cocycle de Kontsevich-Zorich et la classification des cocycles quasi-périodiques. Même si c'est très réducteur, cela donnera un aperçu de son travail et de son style.

## 1. Dynamique dans l'espace de Teichmüller

Avila a obtenu plusieurs résultats fondamentaux dans cette thématique. Expliquons à titre d'exemple un théorème d'Avila et Viana qui prouve la simplicité du cocycle de Kontsevich-Zorich. Il faut pour cela rappeler le contexte.

Une surface de translation compacte  $X$  se représente comme un polygone dans le plan complexe dont on a identifié par translation des côtés parallèles et de même longueur (voir figure ??)<sup>3</sup>. La surface  $X$  est munie d'une métrique plate héritée de la métrique plate naturelle du polygone, avec des singularités coniques en certains sommets du polygone. L'exemple de base de surface de translation est le tore plat. Pour tout angle  $\theta$ , le flot linéaire de direction  $\theta$  est bien défini sur  $X$ , et

<sup>3</sup> On se pourra se référer au texte [Z2] de Zorich consacré aux travaux de Maryam Mirzakhani dans cette même *Gazette* pour plus de détails concernant cette définition.

ses propriétés dynamiques sont d'un grand intérêt. Si on regarde l'application de premier retour du flot (disons) vertical sur un segment fixé, on obtient un échange d'intervalles. Cette construction peut être inversée. Les échanges d'intervalles sont une généralisation naturelle des rotations du cercle : prenons l'intervalle  $[0, 1]$ , découpons-le en  $d$  intervalles  $I_1, \dots, I_d$  et permutons-les (par translations) suivant une permutation fixée  $\pi : \{1, \dots, d\} \rightarrow \{1, \dots, d\}$ . L'application que l'on obtient est un échange d'intervalles. Une rotation sur un cercle est un échange de deux intervalles. Un échange d'intervalles est donc déterminé par le nombre d'intervalles, leurs longueurs et la permutation  $\pi$ .

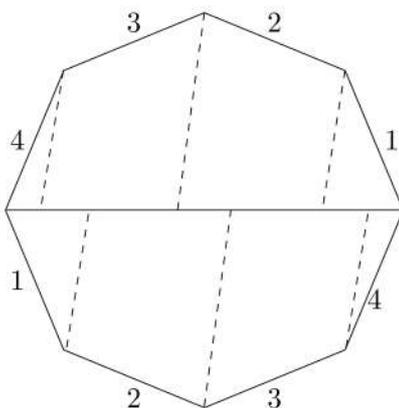


FIG. 1. Une surface de translation de genre 2 (avec 2 trous), le flot linéaire dans une direction donnée, l'application de premier retour sur un segment horizontal qui est un échange d'intervalles. Les segments parallèles sont identifiés.

Lorsqu'on veut comprendre un système dynamique, on l'itère et on essaie de calculer les moyennes d'une fonction le long d'une orbite du système. Le théorème fondamental de Masur et Veech (1982) dit que presque tout échange d'intervalles est ergodique, c'est-à-dire que presque toutes les orbites s'équi-répartissent dans l'intervalle  $([M], [V])^4$ . Déjà dans ce théorème précurseur, l'idée clé est d'introduire une dynamique dans l'espace des paramètres comme on le verra plus tard. Par conséquent, si  $T$  est un échange d'intervalles générique sur  $[0, 1]$  et  $f$  une fonction à valeurs réelles, les moyennes ergodiques

$$\frac{1}{n} \sum_{i=0}^{n-1} f(T^i(x))$$

convergent pour presque tout  $x$  vers  $\int_0^1 f(t) dt$ . Il est plus difficile de déterminer l'écart par rapport à cette moyenne. C'est un problème très naturel du style de ceux

<sup>4</sup> Le presque tout sur les échanges d'intervalles est relatif à la mesure de Lebesgue des longueurs des intervalles échangés, tandis que le presque tout sur les orbites, une fois l'échange d'intervalles fixé, est relatif à la mesure de Lebesgue sur l'intervalle où la dynamique a lieu. On voit apparaître ici des notions du même type, d'une part dans l'espace des paramètres, et d'autre part dans l'espace des phases.

qu'on peut rencontrer en probabilité (théorème de la limite centrale) ou en théorie des nombres (discrépance). La réponse nécessite dans notre situation d'introduire une technologie avancée : les déviations de ces moyennes ergodiques sont régies par les exposants de Lyapunov du flot de Teichmüller (notions que nous allons définir ci-dessous). Zorich [Z1] et Forni [F] ont mené une étude détaillée des déviations des sommes de Birkhoff  $\sum_{i=0}^{n-1} f(T^i(x))$  des échanges d'intervalles par rapport à leur moyenne, sous une hypothèse cruciale de simplicité de ces exposants de Lyapunov. C'est ce résultat fondamental (qui permet à toute la théorie de fonctionner) qui a été démontré par Avila et Viana.

Un exemple très concret qui motive l'intérêt pour les exposants de Lyapunov du flot de Teichmüller est le modèle de « windtree », un exemple de billard périodique. On place un obstacle rectangulaire en chaque point du réseau  $\mathbb{Z}^2$  (voir la figure 2). La table de billard est le complémentaire de ces obstacles, la boule de billard est un point matériel qui suit les lois de la réflexion de Descartes. Si les obstacles étaient ronds au lieu d'être rectangulaires, on se trouverait en présence d'un système chaotique au comportement proche d'un système aléatoire, et on aurait  $d(x, x_t) \approx t^{1/2}$  (où  $x_t$  est la position du point au temps  $t$ ) comme le prédit le théorème de la limite centrale. Dans le cas du « windtree », on a, pour une direction générique,

$$\limsup_{t \rightarrow \infty} \frac{\log d(x, x_t)}{\log(t)} = 2/3.$$

Cet exposant  $2/3$  est aussi ... un exposant de Lyapunov du flot de Teichmüller.

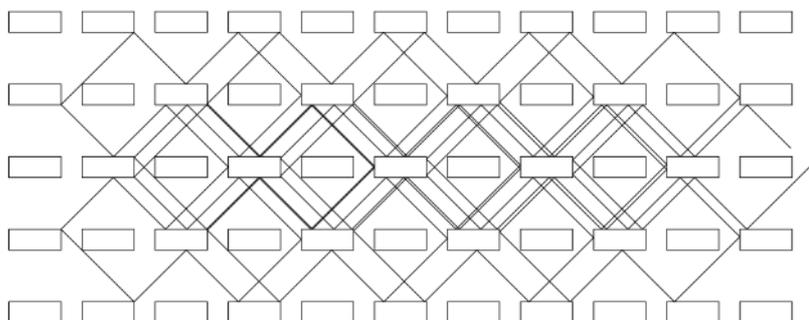


FIG. 2. Modèle de « windtree ».

Définissons maintenant l'espace des surfaces de translation et la dynamique sur cet espace. On fixe tout d'abord le genre de la surface et la combinatoire, c'est-à-dire le nombre de points coniques et l'angle en chaque point conique. La strate  $\mathcal{H}$  de l'espace des modules des surfaces de translation est l'ensemble des surfaces de translation compactes de genre  $g$ , de combinatoire fixée, modulo découpage de la surface et recollement par translation. Le groupe  $GL_2(\mathbb{R})$  agit de façon naturelle sur  $\mathcal{H}$ . Cette action est l'action linéaire sur les polygones, qui est bien définie au niveau des surfaces de translation.

On sait depuis les travaux de Masur et Veech que, pour étudier les échanges d'intervalles ou les flots linéaires sur les surfaces de translation, il faut faire agir le

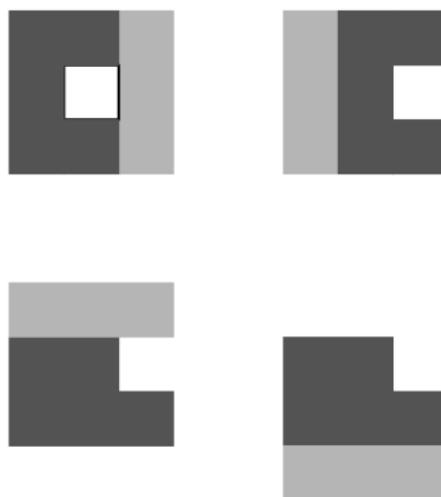


FIG. 3. Trois domaines fondamentaux d'une même surface de translation. Les côtés parallèles et de même longueur sont identifiés. En partant du domaine en haut à gauche puis en découpant, translatant et recollant la partie grise, on obtient le domaine en haut à droite. En repartant de ce même domaine (dessiné en bas à gauche) puis en découpant, translatant et recollant la nouvelle partie grise, on obtient le domaine en bas à droite.

flot géodésique de Teichmüller  $g_t = \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix}$  comme un opérateur de renormalisation. Le flot de Teichmüller contracte les verticales et allonge les horizontales. Masur ([M]) et Veech ([V]) ont montré qu'il existe une mesure  $\mu$  de *probabilité*, absolument continue, sur chaque composante connexe du sous-ensemble  $\mathcal{H}_1$  de  $\mathcal{H}$  constitué des surfaces de translation d'aire 1, qui est invariante, ergodique pour le flot de Teichmüller. C'est cette mesure qui donne la bonne notion de « presque toute surface de translation ».

Kontsevich et Zorich ont beaucoup étudié les exposants de Lyapunov de ce flot. Si l'on suit une orbite périodique du flot, la différentielle du difféomorphisme en ce point est une matrice dont on peut regarder les valeurs propres. Les exposants sont essentiellement les logarithmes des « valeurs propres » d'une trajectoire générique. La partie intéressante pour l'étude des exposants est donnée par le cocycle de Kontsevich-Zorich<sup>5</sup>.

Expliquons intuitivement comment obtenir ce cocycle de façon concrète. On fixe un petit ouvert  $U$  de la strate  $\mathcal{H}$  dans lequel on peut identifier de manière canonique les espaces de cohomologie  $H^1(Y_{\text{top}}, \mathbb{R})$  entre eux lorsque  $Y$  parcourt  $U$ , où  $Y_{\text{top}}$  désigne la surface topologique sous-jacente à la surface de translation  $Y$ . Soit  $X$  un point de  $U$  et  $\alpha$  une classe de cohomologie dans  $H^1(X_{\text{top}}, \mathbb{R})$ . On suit

<sup>5</sup> Un cocycle est une version non commutative d'une somme de Birkhoff. Au lieu de regarder l'évolution d'une fonction au cours du temps, on étudie des matrices dont la valeur est gouvernée par le système dynamique.

par transport parallèle la classe  $\alpha$  sous l'action du flot de Teichmüller  $g_t$  jusqu'à revenir dans  $U$  (ce qui se produit en temps fini pour presque tout  $X$  car le flot est ergodique). La classe  $\alpha_t$  obtenue dans  $H^1((g_t X)_{\text{top}}, \mathbb{R})$  s'identifie de manière canonique à une classe dans  $H^1(X_{\text{top}}, \mathbb{R})$  qui est précisément l'action du cocycle de Kontsevich-Zorich  $G_t^{\text{KZ}}$  sur la classe  $\alpha$ . Comme l'identification se fait au moyen d'un difféomorphisme,  $G_t^{\text{KZ}}$  est une matrice symplectique<sup>6</sup>.

Comme le flot de Teichmüller est ergodique pour la mesure  $\mu$ , on peut appliquer le théorème d'Oseledets au cocycle de Kontsevich-Zorich. Ce théorème est un analogue du théorème ergodique de Birkhoff, mais pour des cocycles à valeurs matricielles. Il affirme qu'il existe des nombres réels  $\lambda_1 > \dots > \lambda_k$  et une décomposition

$$H^1(X_{\text{top}}, \mathbb{R}) = E_1(X) \oplus \dots \oplus E_k(X)$$

dépendant mesurablement de la surface de translation  $X$  telle que, pour presque toute surface  $X$  (par rapport à la mesure de référence  $\mu$ ), si  $\alpha$  est dans  $E_i(X)$ , on a

$$\lim_{t \rightarrow \pm\infty} \frac{1}{t} \log \|G_t^{\text{KZ}}(\alpha)\| = \lambda_i.^7$$

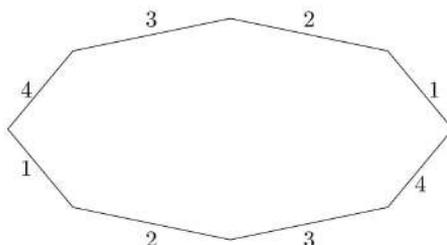


FIG. 4. Action du flot géodésique de Teichmüller sur l'octogone.

Kontsevich et Zorich ont conjecturé que ces exposants sont simples, c'est ce qu'ont démontré Avila et Viana.

**Théorème 1.1** ([AV]). *Pour la mesure de Masur-Veech  $\mu$ , le cocycle de Kontsevich Zorich admet  $2g$  exposants distincts  $\lambda_1 > \dots > \lambda_g > -\lambda_g > \dots > -\lambda_1$ . Autrement dit les espaces  $E_i(X)$  sont de dimension 1<sup>8</sup>.*

Pour démontrer ce théorème, Avila et Viana utilisent un modèle combinatoire du flot de Teichmüller appelé induction de Rauzy-Veech : étant donné un échange d'intervalles sur un intervalle de longueur 1, on lui associe son application de premier retour sur un intervalle idoine que l'on dilate pour en faire un intervalle de longueur 1. La permutation du nouvel échange d'intervalles est a priori différente de celle de l'intervalle de départ. L'induction de Rauzy-Veech est une section du flot

<sup>6</sup> En termes savants, le cocycle de Kontsevich-Zorich représente la monodromie de la connexion de Gauß-Manin le long des géodésiques de Teichmüller.

<sup>7</sup> On peut voir les exposants de Lyapunov comme le logarithme de valeurs propres asymptotiques.

<sup>8</sup> Le fait que  $\lambda_g$  soit strictement positif a été démontré par Forni [F]. En outre, on connaît des mesures invariantes par  $SL_2(\mathbb{R})$ , différentes de  $\mu$ , dont les exposants de Lyapunov vérifient  $\lambda_1 = 1$  et  $\lambda_2 = \dots = \lambda_g = 0$ . Cela illustre la difficulté du problème.

de Teichmüller, i.e., son application de premier retour sur une partie soigneusement choisie de la strate  $\mathcal{H}$ . Une fois encore, on observe une similitude frappante entre les concepts maniés dans l'espace des paramètres (la strate  $\mathcal{H}$ ) et ceux intervenants dans l'espace des phases (l'intervalle).

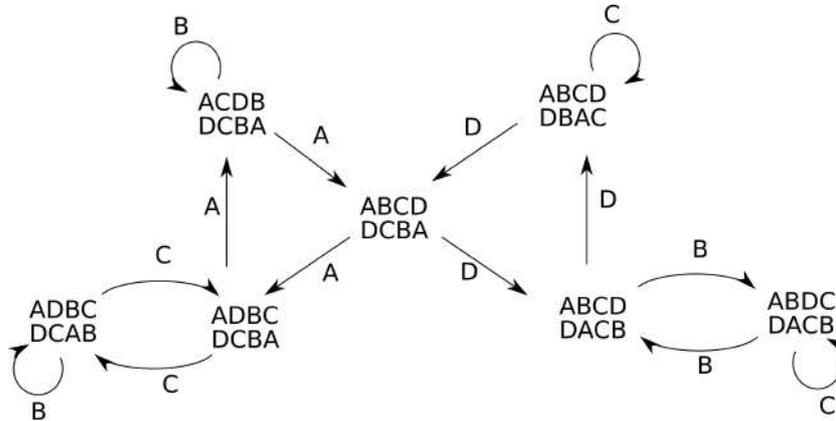


FIG. 5. Diagramme de Rauzy pour des échanges de 4 intervalles étiquetés avec les conventions de Yoccoz.

Concrètement, l'induction de Rauzy est une application markovienne sur un graphe fini dont chaque sommet est un couple : une permutation, et le simplexe donnant les longueurs possibles des intervalles (ces données codent un échange d'intervalles). La figure 5 représente ce graphe pour les échanges de quatre intervalles. Chaque arête est munie d'une matrice explicite : le cocycle de Kontsevich-Zorich du flot de Teichmüller correspond à multiplier ces matrices le long d'un chemin « typique » dans le graphe. Pour comprendre le cocycle, il faut donc étudier le monoïde engendré par ces matrices dans le groupe  $SL_d(\mathbb{R})$ . Des critères de simplicité de cocycles existent depuis longtemps dans le cadre des marches aléatoires sur les groupes linéaires (Guivarc'h-Raugi et Goldstein-Margulis par exemple) mais ils sont difficiles à manier en pratique. Avila et Viana donnent dans ce cadre déterministe un critère très efficace qui a été réutilisé de nombreuses fois (notamment par Matheus-Möller-Yoccoz) : pour avoir simplicité du spectre, il suffit que le cocycle soit assez riche, plus précisément il doit satisfaire aux propriétés de *pinching* et *twisting*. La propriété de *pinching* signifie qu'il existe une matrice hyperbolique dans le monoïde. Le *twisting* veut dire que si deux sous-espaces vectoriels  $F$  et  $G$  de  $\mathbb{R}^d$  vérifient  $\dim(F) + \dim(G) = d$  alors, quitte à appliquer un élément du monoïde à  $F$ , on peut mettre  $F$  et  $G$  en position générique, autrement dit on peut « tourner »  $F$  comme on veut.

Une fois ce critère abstrait démontré, il suffit de vérifier que le cocycle au-dessus des diagrammes de Rauzy vérifie les propriétés de *pinching* et *twisting*. La preuve est extrêmement technique et combinatoire, c'est une induction sur les données combinatoires (idée fort utilisée en dynamique de Teichmüller). L'idée est de considérer des échanges d'intervalles avec une longueur infinitésimale. On voit donc certains diagrammes de Rauzy comme des dégénérescences du diagramme que l'on étudie. Géométriquement, on collapse des singularités de la surface ou bien on

contracte des anses (et on fait alors baisser le genre de la surface). Cette méthode a été raffinée par Avila-Gouëzel-Yoccoz [AGY] pour obtenir une autre propriété statistique du flot de Teichmüller : le flot de Teichmüller est exponentiellement mélangeant pour des observables Hölder<sup>9</sup>. Une conséquence de ce résultat est l'existence d'un trou spectral pour l'action de  $SL_2(\mathbb{R})$  sur l'espace des modules. Ce théorème est tout autant un véritable tour de force. Ce dernier résultat a lui-même été généralisé et amélioré par Avila et Gouëzel [AG] au cas des mesures  $SL_2(\mathbb{R})$  invariantes sans utiliser de codage<sup>10</sup>.

## 2. Opérateurs de Schrödinger et cocycles quasi-périodiques

Les contributions d'Artur Avila à la théorie des opérateurs de Schrödinger quasi-périodiques sont considérables et il est difficile de les décrire toutes en peu de temps. Nous avons donc choisi de présenter dans cette section la théorie d'Artur Avila sur les cocycles analytiques à valeurs dans  $SL(2, \mathbb{R})$  à une fréquence et la classification qu'il en donne. Cette théorie permet de donner une image globale et cohérente de ces dynamiques dont on avait auparavant seulement une connaissance lacunaire. Cette théorie a également des conséquences très importantes dans l'étude du spectre des opérateurs de Schrödinger quasi-périodiques.

*Opérateurs de Schrödinger quasi-périodiques.*— Un opérateur de Schrödinger unidimensionnel discret de potentiel  $(V_n)_{n \in \mathbb{Z}} \in \mathbb{R}^{\mathbb{Z}}$  est un opérateur de  $l^2(\mathbb{Z}) := \{(u_n)_{n \in \mathbb{Z}} : \sum_{n \in \mathbb{Z}} |u_n|^2 < \infty\}$  dans lui-même de la forme

$$H : (u_n) \mapsto (u_{n+1} + u_{n-1} + V_n u_n)_{n \in \mathbb{Z}}.$$

On dit que cet opérateur est *quasi-périodique* quand le *potentiel*  $(V_n)_{n \in \mathbb{Z}}$  est de la forme  $V_n = v(n\alpha + x)$  où  $v : \mathbb{R}^d / \mathbb{Z}^d \rightarrow \mathbb{R}$  est une application continue  $\mathbb{Z}^d$ -périodique,  $\alpha = (\alpha_1, \dots, \alpha_d) \in \mathbb{R}^d$ ,  $x = (x_1, \dots, x_d) \in \mathbb{R}^d$ ; on appelle la fonction  $v$  le *potentiel*,  $\alpha$  le *vecteur de fréquences* et  $x$  la *phase*. Nous noterons  $H_{v, \alpha, x}$  l'opérateur de Schrödinger quasi-périodique de potentiel  $v$ , de vecteur de fréquences  $\alpha$  et de phase  $x$ . Un cas particulier important est celui où  $d = 1$ ,  $\alpha$  est irrationnel et le potentiel  $v$  est de la forme  $v(x) = l \cos x$ ,  $l \in \mathbb{R}$  (la constante de couplage) : on dit alors que  $H$  est un opérateur *presque Mathieu*. Les opérateurs de Schrödinger quasi-périodiques apparaissent naturellement en physique du solide quand on s'intéresse aux propriétés quantiques des électrons dans un quasi-cristal ; de façon plus surprenante, les opérateurs de type presque Mathieu (c'est-à-dire avec ce potentiel très particulier en cosinus) permettent de comprendre l'effet Hall quantique.

Comme  $H_{v, \alpha, x}$  est symétrique et borné, son spectre, c'est-à-dire le complémentaire de l'ensemble des  $E \in \mathbb{C}$  pour lesquels  $H_{v, \alpha, x} - E$  est inversible sur  $l^2(\mathbb{Z})$ , est un compact de  $\mathbb{R}$ . Il n'est pas trop difficile de démontrer que quand  $\alpha$  est irrationnel (c'est-à-dire quand  $1, \alpha_1, \dots, \alpha_d$  sont rationnellement indépendants) le spectre de  $H_{v, \alpha, x}$  est indépendant de la phase  $x$ . On le notera  $\Sigma_{v, \alpha}$ . L'étude de la nature topologique de ce compact est un problème mathématique important et difficile.

<sup>9</sup> Le mélange exponentiel signifie que  $\int_{\mathcal{H}_1} U(x) \cdot V \circ g_t(x) d\mu$  converge vers  $\int_{\mathcal{H}_1} U(x) d\mu \int_{\mathcal{H}_1} V(x) d\mu$  à vitesse exponentielle.

<sup>10</sup> Voir le texte de Zorich [Z2] pour une définition de ces mesures.

Par exemple, il est possible (mais difficile) de démontrer que quand  $v = l \cos$  ( $l \in \mathbb{R} \setminus \{0\}$ ) le spectre  $\Sigma_{v,\alpha}$  est un ensemble de Cantor. Ce résultat, connu sous le nom de « problème des dix Martinis »<sup>11</sup>, a été démontré par A. Avila et S. Jitomirskaya [AJ].

Dans les applications à la physique, en particulier pour comprendre les propriétés de transport des électrons, il est néanmoins souvent nécessaire d'analyser la (une) *mesure spectrale* associée à  $H_{v,\alpha,x}$  : c'est une mesure de probabilité définie sur  $\mathbb{R}$ , dont le support est  $\Sigma_{v,\alpha}$ , qui permet de comprendre la façon dont se « diagonalise »  $H_{v,\alpha,x}$ . En particulier, les propriétés fines de  $H_{v,\alpha,x}$  sont contenues dans la décomposition de sa mesure spectrale  $\mu_{v,\alpha,x}$  en parties absolument continue, purement ponctuelle et singulière continue,  $\mu_{v,\alpha,x} = \mu_{v,\alpha,x}^{ac} + \mu_{v,\alpha,x}^{pp} + \mu_{v,\alpha,x}^{sc}$ . Notons qu'à la différence du spectre  $\Sigma_{v,\alpha}$  ces mesures spectrales  $\mu_{v,\alpha,x}$  dépendent en général de la phase  $x$ . La mesure de probabilité obtenue en prenant la moyenne de ces mesures spectrales  $\nu_{v,\alpha} = \int_{\mathbb{R}^d / \mathbb{Z}^d} \mu_{v,\alpha,x} dx$ , ou plutôt sa fonction de répartition  $N_{v,\alpha}(E) = \nu_{v,\alpha}([-\infty, E])$ , est un objet important dans l'étude des propriétés spectrales des opérateurs de Schrödinger que l'on appelle la *densité intégrée d'états*. Contrairement aux mesures  $\mu_{v,\alpha,x}$ , la mesure  $\nu_{v,\alpha}$  est toujours sans atome, grâce à la moyennisation supplémentaire en  $x$ . De plus, la quantité  $N_{v,\alpha}(b) - N_{v,\alpha}(a) = \nu_{v,\alpha}([a, b])$  est égale à la limite quand  $L \rightarrow \infty$  de  $1/(2L + 1)$  multiplié par le nombre de valeurs propres se trouvant dans l'intervalle  $[a, b]$  de l'opérateur  $H_{v,\alpha,x}^L$  défini comme étant la restriction de  $H_{v,\alpha,x}$  à  $l^2(\{-L, \dots, L\})$  (en particulier, cette limite ne dépend pas de  $x$ ).

Pour simplifier la discussion nous supposons désormais que  $d = 1$  et que  $\alpha$  est fixé et irrationnel.

*Le lien avec les systèmes dynamiques.*— Bien qu'en général l'opérateur  $H_{v,\alpha,x}$  ne soit pas diagonalisable il est important de chercher des solutions non-triviales à croissance modérée (polynomiale) à l'équation (\*) :  $H_{v,\alpha,x}u = Eu$ . En effet, il est possible de démontrer que le spectre  $\Sigma_{v,\alpha}$  coïncide  $\mu_{v,\alpha,x}$ -presque partout avec l'ensemble des  $E \in \mathbb{R}$  pour lesquels cette équation admet des solutions à croissance au plus polynomiale à l'infini. Cette équation aux valeurs propres peut se récrire

$$\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} E - v((n-1)\alpha + x) & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_{n-1} \\ u_{n-2} \end{pmatrix} \text{ ou encore}$$

$$\begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = S_{E-v(x+(n-1)\alpha)} \cdots S_{E-v(x)} \begin{pmatrix} u_0 \\ u_{-1} \end{pmatrix}$$

où  $S_{E-v(x)} = \begin{pmatrix} E - v(x) & -1 \\ 1 & 0 \end{pmatrix}$ . L'étude des solutions de l'équation (\*) est

donc équivalente à celle des produits de matrices  $S_{E-v}^{(n)}(x) = S_{E-v(x+(n-1)\alpha)} \cdots S_{E-v(x)}$ . Or, il existe un système dynamique qui fait naturellement apparaître ces produits, il s'agit du *cocycle quasi-périodique*<sup>12</sup>, c'est-à-dire par

<sup>11</sup> Il semble que ce soit Barry Simon qui ait nommé ainsi ce problème après que Mark Kac eut promis dix Martinis à quiconque le résoudrait. Il existe également une version « dry » de ce problème...

<sup>12</sup> La terminologie « cocycle » est empruntée à la théorie de la cohomologie des groupes dont un des buts est de classifier les extensions (centrales ou pas) d'un groupe donné. En systèmes dynamiques, les cocycles apparaissent naturellement comme une généralisation non-commutative

définition de l'homéomorphisme fibré,  $(\alpha, S_{E-v}) : \mathbb{R}/\mathbb{Z} \times \mathbb{R}^2 \rightarrow \mathbb{R}/\mathbb{Z} \times \mathbb{R}^2$ ,  $(x, y) \mapsto (x + \alpha, S_{E-v}(x)y)$  : le  $n$ -ième itéré de l'homéomorphisme  $(\alpha, S_{E-v})$  est en effet de la forme  $(\alpha, S_{E-v})^n = (n\alpha, S_{E-v}^{(n)})$ . Remarquons que  $S_{E-v}$  est une application de  $\mathbb{R}/\mathbb{Z}$  dans le groupe  $SL(2, \mathbb{R})$ . Nous noterons  $SW_\alpha^k(\mathbb{R}/\mathbb{Z}, SL(2, \mathbb{R}))$  l'ensemble des cocycles quasi-périodiques de classe  $C^k$  ( $k \in \mathbb{N} \cup \{\infty, \omega\}$ ) de la forme  $(\alpha, A) : \mathbb{R}/\mathbb{Z} \times \mathbb{R}^2 \rightarrow \mathbb{R}/\mathbb{Z} \times \mathbb{R}^2$ ,  $(x, y) \mapsto (x + \alpha, A(x)y)$  où  $A : \mathbb{R}/\mathbb{Z} \rightarrow SL(2, \mathbb{R})$  est de classe  $C^k$ . Un cocycle de la forme  $(\alpha, S_{E-v})$  s'appelle un *cocycle de Schrödinger*. On peut associer aux cocycles quasi-périodiques à valeurs dans  $SL(2, \mathbb{R})$  deux quantités importantes :

- le *nombre de rotation fibré*<sup>13</sup> :  $\rho(\alpha, A) = \lim_{n \rightarrow \infty} \frac{\arg A^{(n)}(x)y}{n}$  cette limite étant uniforme en  $n$  et indépendante de  $x \in \mathbb{R}/\mathbb{Z}$  et de  $y \in \mathbb{R}^2 \setminus \{0\}$ <sup>14</sup> ;
- et l'*exposant de Lyapunov fibré*  $L(\alpha, A) = \lim_{n \rightarrow \infty} \int_{\mathbb{R}/\mathbb{Z}} \frac{1}{n} \log \|A^{(n)}(x)\| dx$ .

Deux notions classiques en systèmes dynamiques jouent un rôle fondamental pour comprendre les cocycles quasi-périodiques.

*Réductibilité.*— La notion de *réductibilité* ou de conjugaison fibrée est la suivante : on dit que deux cocycles  $(\alpha, A_i) \in SW_\alpha^k(\mathbb{R}/\mathbb{Z}, SL(2, \mathbb{R}))$ ,  $i = 1, 2$  sont  $C^m$ -conjugués s'il existe une application  $B : \mathbb{R}/\mathbb{Z} \rightarrow SL(2, \mathbb{R})$  (une transformation de jauge, ou conjugaison) de classe  $C^m$  telle que  $(\alpha, A_2) = (0, B) \circ (\alpha, A_1) \circ (0, B)^{-1}$  ou encore  $A_2(\cdot) = B(\cdot + \alpha)A_1(\cdot)B(\cdot)^{-1}$ . Un cocycle  $(\alpha, A)$  est  $C^m$ -réductible s'il est  $C^m$ -conjugué à un cocycle constant  $(\alpha, A_0)$  où  $A_0 \in SL(2, \mathbb{R})$  est constante<sup>15</sup>. Quand cette constante est un élément elliptique de  $SL(2, \mathbb{R})$  on dit que le cocycle est réductible à un elliptique. Dans ce cas les itérés  $(\alpha, A)^n = (n\alpha, A^{(n)})$  sont tels que la suite  $(A^{(n)})_{n \in \mathbb{Z}}$  est uniformément bornée.

L'exposant de Lyapunov fibré est invariant par conjugaison, et le nombre de rotation fibré est invariant par conjugaison homotope à l'identité.

*Hyperbolicité.*— La notion d'*hyperbolicité* pour les cocycles quasi-périodiques se définit comme suit. Un cocycle  $(\alpha, A) \in SW_\alpha^k(\mathbb{R}/\mathbb{Z}, SL(2, \mathbb{R}))$  est *uniformément hyperbolique* (UH) s'il existe des applications continues  $E^s$  et  $E^u$  de  $\mathbb{R}/\mathbb{Z}$  dans  $\mathbb{R}^2$  telles que (a) pour tout  $x \in \mathbb{R}/\mathbb{Z}$ ,  $\mathbb{R}^2 = E^s(x) \oplus E^u(x)$ , (b)  $A(\cdot)E^{s,u}(\cdot) = E^{s,u}(\cdot + \alpha)$  (invariance par la dynamique), (c) Il existe des constantes  $C, l > 0$  telles que pour tous  $x \in \mathbb{R}/\mathbb{Z}$ ,  $n \geq 0$ ,  $y \in E^s(x)$  (resp.  $y \in E^u(x)$ ),  $\|A^{(n)}(x)y\| \leq Ce^{-nl}\|y\|$  (resp.  $\|A^{(-n)}(x)y\| \leq Ce^{-nl}\|y\|$ ).

Si les fibrés  $E^{s,u}$  sont seulement mesurables et définis presque partout, et si la constante  $C$  de la condition (c) précédente dépend mesurablement de  $x$  on dit que le cocycle est *non-uniformément hyperbolique* (NUH). Un cocycle dont l'exposant de Lyapunov est strictement positif est toujours hyperbolique (uniformément ou

---

des sommes de Birkhoff : les itérés de l'application de  $\mathbb{R}/\mathbb{Z} \times \mathbb{R}$  dans lui-même de la forme  $(x, y) \mapsto (x + \alpha, \varphi(x) + y)$  où  $\varphi : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}$  font ainsi naturellement apparaître les sommes de Birkhoff  $\varphi(x) + \varphi(x + \alpha) + \dots + \varphi(x + (n - 1)\alpha)$ . Cette notion est déjà apparue page 59 dans un cadre différent, avec le cocycle de Kontsevich-Zorich.

<sup>13</sup> Il faut supposer que  $A : \mathbb{R}/\mathbb{Z} \rightarrow SL(2, \mathbb{R})$  est homotope à l'identité.

<sup>14</sup> Pour définir correctement le nombre de rotation il faut en fait relever à  $\mathbb{R}/\mathbb{Z} \times \mathbb{R}$  le cocycle  $\mathbb{R}/\mathbb{Z} \times \mathbb{S}^1 \rightarrow \mathbb{R}/\mathbb{Z} \times \mathbb{S}^1$  défini par  $(x, y) \mapsto (x + \alpha, \frac{A(x)y}{\|A(x)y\|})$ .

<sup>15</sup> Dans la notion de réductibilité, on autorise la conjugaison fibrée  $B$  à n'être définie que sur un revêtement  $\mathbb{R}/2\mathbb{Z}$  du tore  $\mathbb{R}/\mathbb{Z}$ .

non) ; c'est le théorème d'Oseledets (voir page 60).

*Attributs spectraux et dynamiques.*– Voici un tableau qui résume quelques liens entre les invariants spectraux des opérateurs de Schrödinger quasi-périodiques et ceux de leurs cocycles de Schrödinger associés.

OBJETS SPECTRAUX		OBJETS DYNAMIQUES
$H_{v,\alpha,x}u = Eu$	$\longleftrightarrow$	$S_{E-v}(\cdot + n\alpha) \begin{pmatrix} u_n \\ u_{n-1} \end{pmatrix} = \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$
ENSEMBLE RESOLVANT $\mathbb{C} \setminus \Sigma_{v,\alpha}$	$\longleftrightarrow$ $=$	HYPERB. UNIFORME $\{E \in \mathbb{R} : (\alpha, S_{E-v}) \text{ Unif. hyperb.}\}$
DENSITE INTEGREE D'ETATS $N_{v,\alpha}(\cdot, ]-\infty, E])$	$\longleftrightarrow$ $=$	NB DE ROTATION $1 - 2\rho(\alpha, S_{E-v})$

*Nature du spectre et propriétés dynamiques.*– On peut préciser le tableau précédent par celui plus heuristique que voici :

ASPECTS SPECTRAUX		ASPECTS DYNAMIQUES
$\Sigma_{v,\alpha}$		$(\alpha, S_{E-v}(\cdot))$
PARTIE AC DE $\Sigma_{v,\alpha}$	$\longleftrightarrow$	REDUCTIBILITE AUX ELLIPTIQUES
PARTIE PP $\Sigma_{v,\alpha}$	$\longleftrightarrow$	HYPERBOLICITE NON UNIFORME
PARTIE SC DE $\Sigma_{v,\alpha}$	$\longleftrightarrow$	?

Dans la suite nous explicitons la signification du tableau précédent.

*Réductibilité et spectre absolument continu.*– La première ligne du tableau précédent est le fait suivant : Si pour Lebesgue-presque tout  $E \in \Sigma_{v,\alpha} \cap I$  (disons  $I$  intervalle) le cocycle  $(\alpha, S_{E-v})$  est réductible à un elliptique alors la restriction du spectre à  $I$  est purement absolument continue :  $\mu_{v,\alpha,x}|I = \mu_{v,x,\alpha}^{ac}|I$  pour tout  $x$ . Or il y a un cas où cette condition de réductibilité est vérifiée (avec  $I = \mathbb{R}$ ), c'est quand  $\alpha$  vérifie une propriété diophantienne<sup>16</sup> et que le potentiel analytique  $v$  est suffisamment petit par rapport à la constante diophantienne de  $\alpha$ . C'est un théorème important de H. Eliasson [E] dont la preuve est basée sur des techniques K.A.M. (Kolmogorov, Arnold, Moser).

*Positivité de l'exposant de Lyapunov et spectre purement ponctuel.*– La seconde ligne du tableau précédent est justifiée par le théorème suivant de Bourgain et Goldstein [BG] : Si  $v \in C^\omega(\mathbb{R}/\mathbb{Z}, \mathbb{R})$  et si pour tout  $E$  dans un intervalle  $I$  et tout  $\alpha$  irrationnel  $L(\alpha, S_{E-v}) > 0$  alors l'ensemble des  $\alpha$  pour lesquels la restriction de  $\mu_{v,\alpha,0}$  à  $I$  est purement ponctuelle est de mesure de Lebesgue totale. La condition  $L(\alpha, S_{E-v}) > 0$  pour tout  $E$  dans un intervalle  $I$  et tout  $\alpha$  irrationnel est assurée pour des  $v$  analytiques suffisamment grands, c'est-à-dire de la forme  $lw$  où  $w \in C^\omega(\mathbb{R}/\mathbb{Z}, \mathbb{R})$  et  $l \gg 1$  (c'est une conséquence d'un théorème d'Herman [H]

<sup>16</sup> Les conditions diophantiennes qui nous intéressent ici sont par exemple : il existe  $\gamma > 0$  (la constante diophantienne) tel que pour tout  $k \in \mathbb{Z} - \{0\}$   $\min_{l \in \mathbb{R}/\mathbb{Z}} |k\alpha - l| \geq \frac{\gamma}{\|k\|^2}$ . L'union sur  $\gamma$  de l'ensemble des points vérifiant cette condition est de mesure de Lebesgue totale.

dans le cas où  $w$  est un polynôme trigonométrique et de Spencer et Sorets [SS] dans le cas général).

*Transition de phase.*— Pour résumer la discussion précédente, si  $w : \mathbb{R}/\mathbb{Z} \rightarrow \mathbb{R}$  est analytique et  $v$  est de la forme  $v = lw$ ,  $l > 0$ ,

(a) Si  $\alpha$  est diophantien et  $l \ll 1$  alors le spectre de  $H_{v,\alpha,x}$  est purement absolument continu pour tout  $x \in \mathbb{R}/\mathbb{Z}$ .

(b) Si  $l \gg 1$ , le spectre de  $H_{v,\alpha,0}$  est purement ponctuel pour Lebesgue presque tout  $\alpha$ .

La nature du spectre de  $H_{w,\alpha,x}$  change donc radicalement suivant le régime ( $l$  petit ou grand) dans lequel on se trouve. En outre, dans le cas où  $v = l \cos$  la situation est beaucoup plus précise : dans (a) on peut remplacer la condition  $l \ll 1$  par  $l < 2$  et dans (b)  $l \gg 1$  par  $l > 2$  : c'est un théorème de Jitomirskaya [J]. Dans ce contexte, on peut démontrer que quand  $l = 2$  le spectre est purement singulier continu. On parle dans cette situation de *transition de phase* quand le paramètre  $l$  passe par la valeur 2.

Il est naturel de demander dans quelle mesure ce type de transition s'étend à des potentiels généraux : c'est une question à laquelle la théorie d'Avila, dont nous décrivons certains aspects dans la suite, permet de répondre. En particulier, cette théorie montre que la transition de phase si nette observée pour  $v = l \cos$  en  $l = 2$  est plutôt exceptionnelle ; Artur Avila montre ainsi que pour de nombreuses perturbations  $v$  de  $2 \cos$  on observe la co-existence d'une partie absolument continue dans le spectre et d'une partie purement ponctuelle [A2].

Nous exposons à présent quelques aspects de la théorie d'Avila.

*Complexification.*— Soit  $(\alpha, A) \in SW^\omega(\mathbb{R}/\mathbb{Z}, SL(2, \mathbb{R}))$  un cocycle analytique (homotope à l'identité) : il existe un  $h > 0$  tel que  $A$  admet une extension holomorphe  $\tilde{A}$  à une bande complexe  $\Omega_h := \mathbb{R}/\mathbb{Z} + i[-h, h]$  de largeur  $2h$  ( $i = \sqrt{-1}$ ),  $\tilde{A} : \Omega_h \rightarrow SL(2, \mathbb{C})$ . Il est alors naturel de considérer pour  $-h < \delta < h$  le cocycle  $(\alpha, A_\delta) : \mathbb{R}/\mathbb{Z} \times \mathbb{C}^2 \rightarrow \mathbb{R}/\mathbb{Z} \times \mathbb{C}^2$ ,  $(x, y) \mapsto (x + \alpha, A(\cdot + i\delta)y)$  et plus particulièrement son exposant de Lyapunov  $\tilde{L}(\delta) := L(\alpha, A(\cdot + i\delta))$ . Il n'est pas difficile de voir que l'application  $\tilde{L} : ]-h, h[ \rightarrow [0, \infty[$  est convexe et paire (cela provient de la sous-harmonicité de l'exposant de Lyapunov).

*Quantification de l'accélération.*— Ce qui est plus surprenant c'est qu'en fait l'application  $\tilde{L} : ]-h, h[ \rightarrow [0, \infty[$  est affine par morceaux et que les pentes de ses parties linéaires sont *quantifiées*.

**Théorème 2.1** ([A1]). *Avec les notations précédentes, l'application  $\tilde{L} : ]-h, h[ \rightarrow [0, \infty[$  est convexe, paire et affine par morceaux. Les pentes de ses parties linéaires (qu'Artur Avila nomme accélérations) sont dans  $2\pi\mathbb{Z}$ .*

On peut préciser le théorème précédent par le résultat dynamique que voici :

**Théorème 2.2** ([A1]). *Le cocycle à valeurs dans  $SL(2, \mathbb{C})$   $(\alpha, A_\delta)$  ( $-h < \delta < h$ ) est uniformément hyperbolique si et seulement si  $\tilde{L}(\delta) > 0$  et  $\tilde{L}$  est affine sur un voisinage de  $\delta$ .*

Une conséquence du théorème précédent est le suivant.

**Corollaire 2.3** ([A1]). *Supposons que le cocycle  $(\alpha, A_E) \in SW^\omega(\mathbb{R}/\mathbb{Z}, SL(2, \mathbb{R}))$  dépende de façon  $C^k$  d'un paramètre  $E$  (par exemple l'énergie si  $(\alpha, A_E)$  est un cocycle de Schrödinger). Alors, le graphe de  $\delta \mapsto L(\alpha, A_E(\cdot + i\delta))$  dépend de façon  $C^k$  de  $E$ .*

Cela résulte de la quantification de l'accélération et du fait que les points de cassure (c'est-à-dire de discontinuité de la dérivée) du graphe (continu) peuvent s'exprimer en fonction de points de contrôle, situés sur les parties linéaires du graphe, qui correspondent à des systèmes dynamiques uniformément hyperboliques; or en ces points la dépendance en le paramètre est régulière (propriété générale des systèmes uniformément hyperboliques).

Si on applique ce résultat à un cocycle de Schrödinger  $(\alpha, S_{E-v})$ ,  $v \in C^\omega(\mathbb{R}/\mathbb{Z}, \mathbb{R})$ ,  $E \in \mathbb{R}$ , on voit en utilisant la parité de  $L$  qu'un des quatre cas suivants se présente (voir la figure 6) :

- (1)  $\delta \mapsto L(\alpha, S_{E-v}(\cdot + i\delta))$  est constant et strictement positif sur un voisinage de 0 (cas uniformément hyperbolique);
- (2) la fonction de  $\delta \mapsto L(\alpha, S_{E-v}(\cdot + i\delta))$  est nulle sur un voisinage de 0;
- (3) 0 est un point de cassure du graphe de  $\delta \mapsto L(\alpha, S_{E-v}(\cdot + i\delta))$  et  $L(\alpha, S_{E-v}) > 0$ ;
- (4) 0 est un point de cassure du graphe de  $\delta \mapsto L(\alpha, S_{E-v}(\cdot + i\delta))$  et  $L(\alpha, S_{E-v}) = 0$

Le premier cas est le cas uniformément hyperbolique et apparaît si et seulement si  $E$  est dans le complémentaire de  $\Sigma_{v,\alpha}$ , le deuxième cas est dit *sous-critique*, le troisième *sur-critique*<sup>17</sup> et le quatrième *critique*.

Notons (cf. les sections précédant celle sur la transition de phase) que si  $v$  est un potentiel de la forme  $lw$  ( $l \in \mathbb{R}$ ) et si  $E \in \Sigma_{lw,\alpha}$  alors

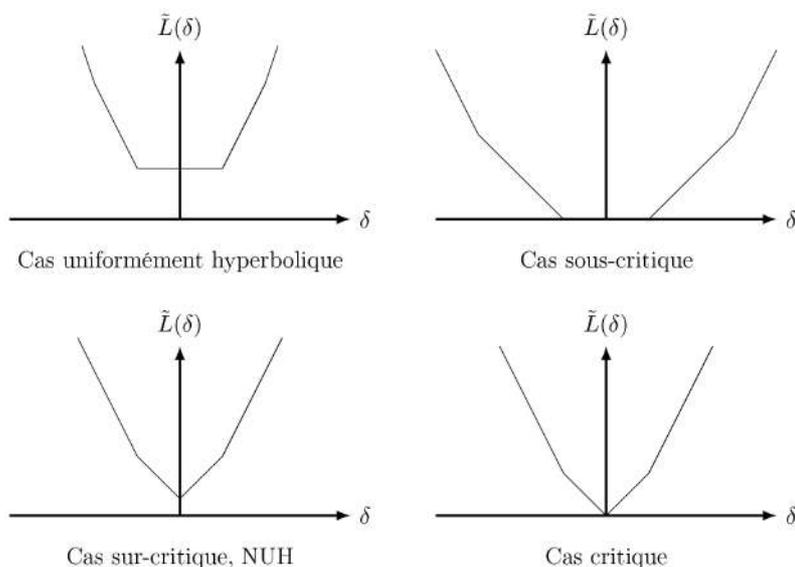
- si  $l \ll 1$  le cocycle  $(\alpha, S_{E-lw})$  est sous-critique;
- si  $l \gg 1$  le cocycle  $(\alpha, S_{E-lw})$  est non-uniformément hyperbolique.

Les paramètres intervenant dans la classification précédente sont la largeur d'un éventuel plateau de  $\tilde{L}$  au voisinage de 0 et sa hauteur. D'après le corollaire 2.3 ce sont des quantités qui dépendent de façon régulière de l'énergie. Les transitions possibles par petites perturbations de  $E$  sont donc

- (a) (sous-critique  $\rightarrow$  sous-critique) ou (sous-critique  $\rightarrow$  unif. hyperbolique),
- (b) (sur-critique  $\rightarrow$  sur-critique) ou (sur-critique  $\rightarrow$  unif. hyperbolique),
- (c) (critique  $\rightarrow$  critique), (critique  $\rightarrow$  sous-critique), (critique  $\rightarrow$  sur-critique) ou (critique  $\rightarrow$  unif. hyperbolique).

*La conjecture de presque-réductibilité.*— Cette conjecture précise ce qui se passe dans le cas sous-critique. Elle généralise considérablement des résultats antérieurs de H. Eliasson [E] et X. Hou-J. You [HY]. Cette conjecture est désormais un théorème qu'a récemment démontré Artur Avila.

<sup>17</sup> Dans ce texte nous réservons la terminologie sur-critique au cas non-uniformément hyperbolique.

FIG. 6. Comportements possibles de  $\tilde{L}$ .

**Théorème 2.4** ([A3]). Soit  $(\alpha, A) \in SW^\omega(\mathbb{R}/\mathbb{Z}, SL(2, \mathbb{R}))$  tel que  $\delta \mapsto L(\alpha, A(\cdot + i\delta))$  soit identiquement nulle sur un voisinage de 0. Alors  $(\alpha, A)$  est analytiquement presque-réductible : il existe une suite  $(B_n)$ ,  $B_n \in C^\omega(\mathbb{R}/\mathbb{Z}, PSL(2, \mathbb{R}))$ , telle que  $B_n(\cdot + \alpha)^{-1}A(\cdot)B_n(\cdot)$  converge vers une constante sur une bande d'analyticité fixe.

*Nature du spectre pour des potentiels « typiques ».*— Une application impressionnante de la théorie précédente à la théorie spectrale des opérateurs de Schrödinger quasi-périodiques est le théorème suivant d'Avila qui montre que pour des potentiels typiques un tel opérateur n'admet pas de spectre singulier.

Le fait que la classification des cocycles en uniformément hyperboliques, sous-critiques, critiques, sur-critiques dépende de deux paramètres (la largeur d'un éventuel plateau de  $\tilde{L}$  au voisinage de 0 et sa hauteur) suggère qu'un potentiel « typique » est *acritique* dans le sens où pour aucun  $E \in \Sigma_{v, \alpha}$  le cocycle  $(\alpha, S_{E-v})$  n'est critique. La notion de potentiel typique (dont nous ne donnons pas la définition) est très forte : elle s'apparente à une notion de mesure totale (prévalence) dans l'ensemble des potentiels analytiques. Ce que suggère la classification des cocycles est en fait un théorème d'Avila.

**Théorème 2.5** ([A2]). Pour un potentiel « typique »  $v \in C^\omega(\mathbb{R}/\mathbb{Z}, \mathbb{R})$ , les cocycles  $(\alpha, S_{E-v})$  ne sont critiques pour aucun  $\alpha$  irrationnel et aucun  $E \in \mathbb{R}$ .

En utilisant la Conjecture de presque réductibilité, Avila montre alors que *pour un potentiel typique la partie singulière du spectre est absente*.

### 3. Références

- [A1] Avila, A. Global theory of one-frequency Schrödinger operators I : stratified analyticity of the Lyapunov exponent and the boundary of nonuniform hyperbolicity. [www.imj-prg.fr/~artur.avila/](http://www.imj-prg.fr/~artur.avila/)
- [A2] Avila, A. Global theory of one-frequency Schrödinger operators II : acriticality and finiteness of phase transitions. [www.imj-prg.fr/~artur.avila/](http://www.imj-prg.fr/~artur.avila/)
- [A3] Avila, A. KAM, Lyapunov exponents and the spectral dichotomy for one-frequency Schrödinger operators. En préparaton.
- [AGY] Avila A., Gouëzel S., Yoccoz J.-C. Exponential mixing for the Teichmüller flow, *Publ. Math. Inst. Hautes Etudes Sci.* (2) 104 (2006), no. 2, p. 143–211.
- [AG] Avila, A., Gouëzel, S. Small eigenvalues of the Laplacian for algebraic measures in moduli space, and mixing properties of the Teichmüller flow. *Ann. of Math.* (2) 178 (2013), no. 2, 385–442.
- [AJ] Avila A., Jitomirskaya S. The Ten Martini Problem. *Ann. of Math.* (2) 170 (2009), no. 1, 303–342.
- [AV] Avila A., Viana M., Simplicity of Lyapunov spectra : proof of the Zorich-Kontsevich conjecture. *Acta Math.* 198 (2007), no. 1, 1–56.
- [BG] Bourgain, J. ; Goldstein, M. On nonperturbative localization with quasi-periodic potential. *Ann. of Math.* (2) 152 (2000), no. 3, 835–879.
- [E] Eliasson, L. H. Floquet solutions for the 1-dimensional quasi-periodic Schrödinger equation. *Comm. Math. Phys.* 146 (1992), no. 3, 447–482.
- [F] Forni G. Deviation of ergodic averages for area-preserving flows on surfaces of higher genus, *Annals of Mathematics* (2) 155 (2002), no. 1, p. 1–103.
- [H] Herman, Michael-R. Une méthode pour minorer les exposants de Lyapounov et quelques exemples montrant le caractère local d'un théorème d'Arnold et de Moser sur le tore de dimension 2. *Comment. Math. Helv.* 58 (1983), no. 3, 453–502.
- [HY] Hou, Xuanji ; You, Jiangong Almost reducibility and non-perturbative reducibility of quasi-periodic linear systems. *Invent. Math.* 190 (2012), no. 1, 209–260.
- [J] Jitomirskaya, Svetlana Ya. Metal-insulator transition for the almost Mathieu operator. *Ann. of Math.* (2) 150 (1999), no. 3, 1159–1175.
- [M] Masur H. Interval exchange transformations and measured foliations. *Annals of Mathematics* (2) 115 (1982), no. 1, p. 169–200.
- [SS] Sorets, Eugene ; Spencer, Thomas Positive Lyapunov exponents for Schrödinger operators with quasi-periodic potentials. *Comm. Math. Phys.* 142 (1991), no. 3, 543–566.
- [V] Veech W. Gauss measures for transformations on the space of interval exchange maps. *Annals of Mathematics* (2) 115 (1982), no. 1, p. 201–242.
- [Z1] Zorich A. Deviation for interval exchange transformations. *Ergodic Theory Dynam. Systems* 17 (1997), no. 6, 1477–1499.
- [Z2] Zorich A. Le théorème de la baguette magique de A. Eskin et M. Mirzakhani. *Gazette des Mathématiciens* 142 (2014).

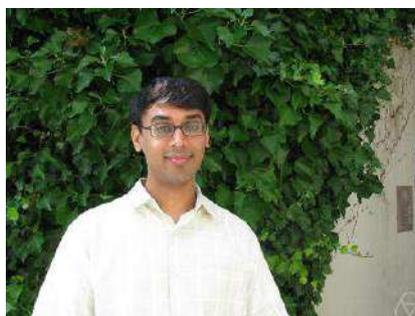
## En aparté avec Manjul Bhargava et Martin Hairer

---

### Manjul Bhargava

*Bonjour Manjul Bhargava.  
Comment as-tu décidé de devenir mathématicien ?*

Aussi loin que je me souviens, j'ai toujours aimé les mathématiques. Très jeune, peut-être dès deux ou trois ans, je m'amusais à multiplier des grands nombres. Ma mère est mathématicienne. Je lui ai posé beaucoup de questions en grandissant et elle a toujours été là pour y répondre. Lorsque je ne connaissais pas une réponse, elle me poussait à la découvrir par moi-même. Elle a été une grande source d'encouragement et d'inspiration dans ma jeunesse.



*Tu as grandi au Canada ou aux États-Unis ?*

Je suis né au Canada, mais j'ai principalement grandi aux États-Unis, à Long Island, New-York. J'ai aussi passé beaucoup de temps en Inde. J'ai beaucoup de famille en Inde et au Canada et j'ai donc été régulièrement dans ces deux pays.

*Tu as été très influencé par la culture indienne ?*

Oui, j'ai grandi dans un foyer à la culture très indienne. Mes deux parents ont immigré d'Inde et nous parlions hindi à la maison, nous mangions de la cuisine indienne, je lisais des livres pour enfants indiens... et puis mon grand-père était professeur de Sanskrit. J'ai donc lu beaucoup de littérature sanskrite quand j'étais enfant, notamment des livres de mathématiques. Cela a été une grande source d'inspiration pour moi.

*Dans quelles universités as-tu étudié ?*

J'ai tout d'abord étudié à Harvard et je suis ensuite allé à Princeton pour mon doctorat.

*Ton directeur de thèse est Andrew Wiles. Étais-tu impressionné de débiter une thèse sous sa direction ?*

Oui, bien sûr, mon directeur de thèse est Andrew Wiles (sourire). Comme chacun sait, c'est un mathématicien extraordinaire. C'est aussi une personne merveilleuse. Je ne travaillais pas directement sur des problèmes sur lesquels lui

travaillait, mais il a toujours su me faire sentir ce qui importait, ce qui faisait de bonnes mathématiques. J'allais le voir avec différents projets et il a toujours été de très bon conseil, m'indiquant ce qui était plus important et ce qui l'était moins. Cela a été très utile pour moi. Et puis, il était tellement encourageant, toujours prêt à discuter, toujours excité d'entendre ce que j'avais à raconter... Non vraiment, cela a été une excellente expérience.

*Comment as-tu choisi la théorie des nombres ?*

La théorie des nombres est quelque chose que j'aime depuis que je suis enfant. Je crois qu'il a toujours été clair que si je faisais des mathématiques, ce serait pour travailler dans ce domaine. Oui, aussi loin que je me souviens. J'aime le genre de mathématiques que l'on peut expliquer à n'importe qui. C'est ce que j'aime dans la théorie des nombres. Les problèmes sont tellement concrets, on peut les expliquer à tout le monde, et pourtant les méthodes pour les résoudre sont si profondes.

*As-tu des héros mathématiques ou au moins des influences particulièrement importantes ?*

Bien sûr, il y en a beaucoup ! Tu veux dire... ceux qui sont contemporains ?

*Pas nécessairement.*

Comme je le disais, j'ai lu beaucoup de travaux mathématiques en Sanskrit. Ils m'ont beaucoup influencé lorsque j'étais enfant, en particulier Brahmagupta, Panini, Pingala. Ma mère, bien évidemment, a été mon premier professeur de mathématiques. Elle est probablement ma plus grande inspiration. Plus tard, à l'université, il y a eu mes professeurs Barry Mazur et Persi Diaconis, et des mentors comme Joe Gallian et David Cargo. Ensuite, il y a évidemment mon directeur Andrew Wiles. Mes autres professeurs à Princeton Peter Sarnak, John Conway. Il y en a beaucoup d'autres... j'ai passé du temps quand j'étais étudiant avec Hendrik Lenstra et Don Zagier... et aussi Benedict Gross avec qui je collabore maintenant beaucoup. De nombreux mathématiciens ont influencé ma façon de voir les mathématiques.

*Ramanujan ?*

Oui, Ramanujan aussi. Certains de mes travaux sont directement inspirés des siens. Oui, il est clairement dans la liste... et puis j'oubliais Gauß ! C'est probablement ma plus grande source d'inspiration mathématique. Je n'ai pas le droit de l'oublier !

*Tu es un théoricien des nombres, mais quels autres domaines des mathématiques t'intéressent particulièrement ?*

En fait, la théorie des nombres est souvent le principal objectif, mais pour cela je dois m'intéresser à de nombreux domaines voisins qui fournissent des outils nécessaires. Dans cet ordre d'idée, la théorie des représentations joue un rôle prépondérant dans mes travaux depuis de nombreuses années, tout comme la géométrie algébrique. La combinatoire est également un thème qui m'a toujours fasciné. Mais il y a aussi beaucoup d'analyse, d'algèbre, de théorie des anneaux... bref, il y a vraiment de nombreux domaines auxquels je m'intéresse. En général, la

finalité est de répondre à des questions de théorie des nombres... comme souvent avec moi. (sourire)

*Tu as reçu de nombreux prix prestigieux et ton nom circulait déjà bien avant l'annonce officielle des lauréats de la médaille Fields. Est-ce que cela a été quand même une surprise pour toi ?*

C'est vrai que beaucoup de gens en parlaient depuis longtemps. Ce n'était donc pas une énorme surprise, mais bien sûr lorsque l'on m'a prévenu c'était un sentiment très agréable et un grand honneur.

*Est-ce que tu crois que cela va changer ta vie ?*

J'espère que ça ne la changera pas trop. Il y a beaucoup de choses que je voudrais faire d'un point de vue mathématique et j'espère bien continuer activement mes recherches. Si cette reconnaissance me permet de faire quelque chose concernant l'enseignement des mathématiques à travers le monde, je profiterai sans aucun doute de cette occasion et je serai heureux de pouvoir apporter ma contribution grâce à cette reconnaissance. Mais sinon, je voudrais rester avant tout concentré sur mes travaux mathématiques.

*Pourrais-tu nous présenter tes travaux ?*

J'ai l'habitude de travailler sur plusieurs problèmes en même temps. Je ne considère jamais un seul problème. De cette façon, lorsque je suis bloqué avec l'un, je peux passer à un autre. Les polynômes sont des objets fondamentaux pour les mathématiques (et pour d'autres sciences). Les mathématiciens aiment approcher des fonctions par des polynômes, étudier des espaces de polynômes, et en particulier, ils veulent savoir des choses sur les valeurs prises par des polynômes. Les théoriciens des nombres s'intéressent aux polynômes à coefficients entiers et aux valeurs entières ou rationnelles de ces polynômes. Par exemple, un problème millénaire est la description des entiers qui sont la somme de deux carrés. Si deux entiers ont cette propriété alors leur produit l'a également. Une généralisation du mathématicien Brahmagupta, quelque chose que j'ai lu étant enfant, stipule que si deux entiers sont de la forme un carré plus  $n$  fois un carré, alors leur produit est également de cette forme. Ce résultat date du VII<sup>e</sup> siècle. Douze siècle plus tard, Gauß s'est demandé quand est-ce que le produit de deux nombres entiers étant chacun représenté par une expression quadratique, peut également être représenté par une troisième expression quadratique. C'est ce que l'on appelle maintenant la loi de composition de Gauß. Ce résultat est le point de départ de mon travail de thèse, mais je me suis intéressé à des objets plus généraux (expressions de plusieurs variables, de plus grand degré). J'ai commencé par chercher un moyen simple de comprendre cette loi de composition de Gauß. J'ai été inspiré par l'idée de matrice tridimensionnelle. J'avais l'habitude de jouer avec des cubes, par exemple des Rubik's cubes, et je me suis dit : on a l'habitude de travailler avec des matrices carrées à l'école, mais pourquoi ne pas considérer des matrices cubiques ? Rien qu'en considérant l'exemple des matrices  $2 \times 2 \times 2$ , j'ai pu trouver une description simple de la loi de composition de Gauß. Cette approche m'a permis de généraliser cette loi de composition à des contextes plus généraux et d'en décrire d'autres, quatorze en tout. C'est le sujet de mes travaux de thèse. Et c'est seulement après avoir

compris que la loi de Gauß n'était qu'un exemple d'une théorie plus générale, que je me suis demandé ce que l'on pouvait faire avec cette théorie. Cela m'a conduit à des questions de nature plus analytique à propos du comportement « typique » d'objets mathématiques, en me demandant quelles sont les propriétés d'un polynôme typique ou d'un corps de nombres typique. Et finalement, cela m'a conduit à des questions de géométrie arithmétique. Par exemple, si l'on considère un polynôme à coefficients entiers, on peut se demander combien de fois peut-il prendre une valeur qui est un carré parfait ? Un résultat récent issu de cette philosophie est que si le polynôme est de degré dix ou plus, la probabilité qu'il prenne pour valeur un carré parfait est inférieure à 1%. C'est juste un exemple du genre de question concrète que l'on peut traiter grâce à cette façon de penser en terme de matrices de dimension supérieure... combinée avec des techniques d'analyse et de géométrie.

*Quel est le résultat, s'il y en a un, dont tu es le plus fier ?*

Les mathématiciens ont coutume de dire que choisir un théorème préféré, c'est comme choisir un enfant préféré. Je n'ai pas encore d'enfant, mais je crois que je peux comprendre ce sentiment. Chaque théorème que l'on prouve est une nouvelle étape, à la fois mémorable et excitante. Je n'ai pas de théorème préféré, mais il y a un résultat particulièrement simple à expliquer aux gens qui n'ont pas de grandes connaissances mathématiques. Il s'agit du « théorème 290 ». C'est un résultat qui a été conjecturé par Conway au début des années 90. Je peux vous en parler ?

*Oui, bien sûr.*

Il y a un vieux théorème de Lagrange qui stipule que tout nombre entier positif peut s'écrire comme la somme de quatre carrés. Par exemple,  $19 = 16 + 1 + 1 + 1$ . Les répétitions sont permises. Parfois, certains sont un peu surpris car les carrés sont de plus en plus espacés (1, 4, 9, 16, ...) et pourtant aussi grand que soit le nombre choisi, on peut l'écrire comme la somme de quatre carrés. C'est là que Ramanujan arrive. Une façon d'énoncer le théorème de Lagrange est de dire que tout nombre entier positif est représenté par la forme quadratique  $a^2 + b^2 + c^2 + d^2$ . Et Ramanujan s'est demandé s'il y a d'autres expressions quadratiques qui représentent tous les entiers. Il a donné cinquante-quatre autres expressions de ce type. Par exemple,  $a^2 + b^2 + c^2 + 2d^2$ ,  $a^2 + b^2 + c^2 + 3d^2$  ou  $a^2 + b^2 + c^2 + 4d^2$ ... mais  $a^2 + b^2 + c^2 + 8d^2$  ne convient pas, car le nombre 7 ne peut pas s'écrire sous cette forme. Donc seulement certaines formes quadratiques de quatre variables font l'affaire. Ensuite, il n'y a guère eu de progrès sur cette question jusqu'à ce que Conway, au début des années 90, se mette à faire des calculs avec un de ses étudiants. Ceux-ci semblaient indiquer que pour qu'une forme quadratique définie positive à coefficients entiers représente tous les entiers positifs il suffit qu'elle représente tous les entiers de 1 jusqu'à 290 ! C'est devenu la « conjecture 290 » de Conway. Il y a quelques années<sup>1</sup>, dans un travail en collaboration avec Jonhatan Hanke, j'ai démontré ce résultat en utilisant une combinaison de méthodes théoriques et de calculs intensifs. Je trouve que c'est vraiment un résultat particulièrement adapté à être présenté à un large public. Et puis, il est valable pour un nombre quelconque de variables !

<sup>1</sup> NDLR : l'article est à paraître dans la revue *Inventiones Mathematicae*.

On dispose donc d'un test très simple pour savoir si une expression quadratique qui prend uniquement des valeurs entières positives prend chaque entier positif comme valeur. Par exemple, le théorème des quatre carrés de Lagrange est un cas spécial de ce résultat : il suffit de vérifier que les entiers  $1, 2, \dots, 290$  sont bien la somme de quatre carrés. Voilà ce qu'est le « théorème 290 » ! (sourire)

*Peux-tu nous parler un peu de tes travaux sur les courbes elliptiques ?*

Bien sûr ! Une courbe elliptique est une équation de la forme  $y^2 = x^3 + ax + b$ , où  $a$  et  $b$  sont des constantes et  $x$  et  $y$  les variables. Par exemple,  $y^2 = x^3 + 2x + 3$ . C'est également un thème très ancien qui remonte à plusieurs siècles. Ces objets sont rattachés à beaucoup de domaines des mathématiques. Pour les théoriciens des nombres, c'est une source d'intérêt depuis longtemps, notamment car les solutions  $(x, y)$  rationnelles (on considère  $a$  et  $b$  rationnels) ont une structure particulière. On peut prendre deux solutions et les « ajouter » pour en obtenir une troisième. Ce genre d'équations a une grande importance en mathématiques. Les théoriciens des nombres voudraient notamment savoir si, une courbe elliptique étant donnée, celle-ci a un nombre fini ou infini de solutions rationnelles. Pour des équations quadratiques, il est bien connu que l'on peut répondre à cette question. Mais pour les équations cubiques comme  $y^2 = x^3 + ax + b$ , il n'y a aucun algorithme connu permettant de décider si le nombre de solutions rationnelles est fini ou infini. C'est un peu gênant. (rire) Une façon de penser à la conjecture de Birch et Swinnerton-Dyer (BSD), est de la voir comme un moyen de fournir un tel algorithme pour les courbes elliptiques. En effet, si l'on suppose la conjecture BSD vraie, alors il y a bien un algorithme pour décider de la finitude des solutions rationnelles. C'est l'une des raisons pour lesquelles les théoriciens des nombres sont si intéressés par cette conjecture. Elle permet de passer du cas des équations quadratiques à certaines équations cubiques, ce qui correspond naturellement à l'étape suivante à comprendre. Puisque l'on ne sait pas traiter le cas d'une courbe elliptique donnée, j'ai essayé de regarder les choses sous un autre angle et de comprendre ce qui se passe pour une courbe « typique ». C'est-à-dire si on choisit une courbe elliptique « au hasard », quelle est la probabilité que cette équation ait un nombre fini de solutions rationnelles ? Un des résultats que j'ai prouvés avec Arul Shankar dit qu'une proportion positive de courbes elliptiques n'a qu'un nombre fini de solutions rationnelles.

Ce travail a ensuite été complété par un résultat obtenu avec Christopher Skinner qui montre qu'une proportion positive de courbes elliptiques a un nombre infini de solutions rationnelles. Les deux possibilités ont donc une probabilité non nulle. En réalité, la conjecture est que ces deux probabilités sont égales et qu'il y a donc 50% des courbes elliptiques qui ont un nombre fini de solutions rationnelles et 50% pour lesquelles ce nombre est infini. Il s'agit donc d'un premier pas en direction de cette conjecture. En fait, nous avons montré que chacune de ces probabilités est supérieure à 20%. Finalement, une conséquence de cette approche est en particulier que la conjecture BSD est vraie pour la plupart (plus de la moitié) des courbes elliptiques. C'est un autre aspect de mes travaux sur les courbes elliptiques de ces dernières années.

*Ces résultats sont inefficaces ?*

C'est vrai. Tous les résultats que j'ai mentionnés ne sont valables que pour une courbe « typique », c'est-à-dire choisie « au hasard ». Ils ne disent par contre rien sur une courbe elliptique particulière qui nous serait donnée. On dit par exemple qu'au moins 66% des courbes elliptiques satisfont à la conjecture BSD, mais on est incapable de dire pour quels paramètres  $a$  et  $b$  c'est bien le cas. C'est vraiment un énoncé de nature probabiliste.

*As-tu un espoir de démontrer cette conjecture des 50% ?*

En fait, les méthodes utilisées ne l'interdisent pas. Il semble qu'il y ait un moyen d'aller plus loin. Au moins pour dire que, pour toute courbe elliptique d'un certain type, la conjecture BSD est vraie. Même un énoncé prouvant que la conjecture est vraie pour 100% des courbes elliptiques ne semble pas impossible à obtenir. Attention, 100% ne veut bien sûr pas dire toutes les courbes elliptiques. Si ces méthodes nous permettent de continuer, on peut imaginer arriver à traiter 100% des courbes elliptiques, mais il y aura toujours un ensemble infini de 0% de courbes qui nous échapperont. Il y a d'autres arguments qui permettraient peut-être de tout démontrer, mais cela demandera des avancées majeures. Je n'ai pas encore abandonné! (rire) Ce serait vraiment un exploit formidable d'arriver à montrer le résultat pour toute courbe elliptique et pas seulement 100%. Mais certaines idées sont déjà là... alors nous ne devons pas abandonner.

*Les résultats de nature probabiliste semblent de plus en plus courant en théorie des nombres. Comment expliques-tu ce phénomène ?*

Oui, c'est vrai. Il y a eu énormément de calculs effectués à propos d'objets arithmétiques fondamentaux, comme les corps de nombres, les courbes elliptiques, les courbes hyperelliptiques... Il est clair, à partir de ces données, qu'il ne faut pas chercher de motif particulier. Par exemple, il ne faut pas chercher une explication simple en fonction de  $a$  et  $b$  indiquant si la courbe elliptique  $y^2 = x^3 + ax + b$  a un nombre fini ou non de solutions rationnelles. Ces courbes semblent se comporter comme un objet aléatoire. C'est pourquoi, ces dernières années, il y a eu cette tendance à les traiter vraiment comme tel et ainsi à essayer d'obtenir des énoncés de nature probabiliste. C'est sans doute parce qu'on ne s'attend pas à découvrir une formule (en termes de  $a$  et  $b$ ) permettant de savoir si une courbe elliptique a ou non une infinité de solutions rationnelles, ni une formule concernant la taille du groupe des classes d'un corps quadratique. Ces objets se comportent vraiment comme des objets aléatoires et l'idée de les considérer de la sorte remonte au moins aux heuristiques de Cohen-Lenstra. Ces heuristiques concernent la taille des groupes de classes des corps de nombres et sont obtenues en les modélisant par des objets aléatoires. Même si elles ne donnent aucune formule pour aucun corps de nombres fixé, elles ont une grande puissance de prédiction sur le comportement des groupes de classes. J'ai prouvé quelques cas de ces conjectures et l'idée est venue de regarder d'autres objets sous cet éclairage probabiliste. Puisque les objets individuels sont si difficiles à appréhender, l'idée est de traiter la collection de ces objets comme aléatoire et d'essayer d'obtenir alors des énoncés non triviaux.

*Tes travaux récents sur les courbes elliptiques sont en collaboration, notamment avec Shankar et Skinner, tandis que tu as travaillé seul pour généraliser la loi de composition de Gauß. Quel type de travail préfères-tu ?*

Je voudrais préciser que le résultat que j'ai mentionné concernant la conjecture BSD est également en collaboration avec Wei Zhang. Pour revenir à la question, je préfère le travail en collaboration. C'est une façon plus ludique de faire des mathématiques, avec plus d'interaction. Je crois que c'est une bonne idée que davantage de mathématiciens collaborent. Avant de préparer une thèse, on vous dit que vous devez la rédiger seul. C'est pourquoi je travaillais seul. Et comme j'ai mis quelques années à rédiger les résultats de ma thèse, j'ai donc travaillé seul pendant quelque temps, même après l'avoir soutenue. Mais quand l'occasion de travailler avec d'autres mathématiciens s'est finalement présentée, j'ai saisi cette opportunité. C'est très amusant d'apprendre certaines méthodes à d'autres et d'apprendre également des autres. Je crois que c'est non seulement plus amusant, mais aussi peut-être plus productif.

*Justement, que penses-tu de l'initiative de Polymath ?*

Polymath est une extension de cette idée que la collaboration permet d'échanger davantage d'idées et finalement d'être plus productif. Mais il est difficile pour un plus grand nombre de personnes de se rencontrer physiquement, ou même *via* des moyens comme Skype. Polymath est une façon de faire collaborer beaucoup de gens, même s'ils ne se trouvent pas réunis au même endroit. Je trouve que c'est une très bonne initiative. C'est plutôt nouveau et il faut donc attendre un peu pour voir si ça se révèle vraiment être un succès. Mais c'est vraiment une bonne idée : une extension de l'idée de collaboration, mais à grande échelle. Je pense que ça peut avoir un gros potentiel. Je n'ai encore participé à aucun projet Polymath, mais je suis tout à fait ouvert à le faire.

*Une question pour finir. Quel est le prochain problème auquel tu voudrais t'attaquer ?*

(sourire). Il y a beaucoup de choses. Comme je le disais, j'aime travailler sur plusieurs projets à la fois. La conjecture BSD est clairement un problème auquel je voudrais réfléchir. Je suis aussi intéressé par les méthodes de cribles. Il y a ce fameux résultat qui dit que si on choisit un entier au hasard, alors la probabilité qu'il soit sans facteur carré (dans sa décomposition en facteurs premiers, aucun nombre premier n'apparaît plus d'une fois) est  $6/\pi^2$ , soit plus d'une chance sur deux. Je suis intéressé par des généralisations de ce résultat depuis quelques mois. Si on choisit un polynôme au hasard, quelle est la probabilité que son discriminant soit sans facteur carré ? Il y a beaucoup de généralisations de ce type qu'on peut essayer de démontrer, mais qui sont toujours ouvertes. C'est une autre de mes questions favorites en ce moment, comprendre la probabilité que les valeurs des polynômes soient sans facteur carré. Voilà deux exemples de sujets pour des recherches futures.

## Martin Hairer

*Bonjour Martin Hairer.*

*Pourrais-tu commencer par nous décrire un peu ton parcours ?*

J'ai surtout grandi en Suisse, à Genève. C'est là que j'ai effectué une grande partie de ma scolarité et de mes études, notamment ma thèse. Il s'agit d'une thèse en physique théorique soutenue sous la direction de Jean-Pierre Eckmann.

J'ai ensuite obtenu une bourse du Fond National Suisse pour aller à l'université de Warwick où j'ai obtenu un poste permanent quelques années plus tard. À l'exception d'une année passée au Courant Institute de New York en 2009, je suis depuis resté à Warwick.



*Comment est venue ta vocation pour les mathématiques ?*

Mon père est mathématicien. Sa spécialité est l'analyse numérique. Enfant, j'ai donc toujours pu lui poser des questions et de son côté, il a su faire des efforts pour m'expliquer, autant que possible, en quoi consistait son travail. Adolescent, j'étais en fait intéressé par les sciences en général : mathématiques, physique, informatique. J'ai notamment fait beaucoup de programmation.

*Tu as une thèse en physique, comment s'est passée la transition vers les mathématiques ?*

Officiellement, ma thèse est en physique théorique, mais dans la plupart des universités mon directeur serait considéré comme mathématicien. Mon sujet de thèse était davantage un sujet de mathématiques que de physique.

*Quel en était le sujet ?*

Le comportement asymptotique d'équations différentielles partielles stochastiques.

*Tu as connu l'Autriche, la Suisse et maintenant le Royaume-Uni, quelles différences as-tu constaté entre ces systèmes éducatifs et de recherche ?*

Concernant le système éducatif, j'ai principalement fait l'expérience de la Suisse et du Royaume-Uni. Bien que cela ait semblé-t-il changé depuis, les élèves suisses étaient confrontés dès le secondaire à de vraies preuves mathématiques. Par exemple, des preuves classiques d'analyse. En revanche, les étudiants de première année à Warwick ne connaissent absolument pas la notion de preuve

mathématique. C'est là je crois la différence principale dans l'enseignement des mathématiques dans ces deux systèmes. En tout cas, c'est ce qui ressort de mon expérience personnelle.

*Connais-tu un peu le système français ?*

Seulement au niveau universitaire car j'ai beaucoup de contacts avec des collègues en France. Au niveau de la recherche, il y a bien sûr la spécificité du CNRS qui n'a pas d'équivalent ailleurs en Europe. Le système des grandes écoles est également assez unique, même si *de facto* Oxford et Cambridge jouent un rôle similaire en Angleterre.

*Parlons un peu mathématiques. Peux-tu nous présenter ton domaine de recherche : ces fameuses équations différentielles partielles stochastiques ?*

(Rires). Les EDP stochastiques sont des objets mathématiques permettant de décrire le comportement de systèmes qui dépendent non seulement du temps mais également de l'espace et qui incorporent de plus une composante aléatoire. Un exemple que l'on pourrait donner est celui d'un aimant. À température ambiante, l'aimant a un champ magnétique propre dirigé dans une certaine direction. Si maintenant on décide de chauffer cet aimant, il existe une température critique au-dessus de laquelle son champ magnétique va disparaître. L'aimant va alors se comporter comme un bout de fer banal. Le problème consiste alors à comprendre le comportement de l'aimant lorsque la température est proche de cette température critique. Le champ magnétique va alors faiblir et développer des fluctuations à la fois dans le temps et l'espace. Ce type de fluctuations est justement décrit par une EDP stochastique. Ma contribution vient du fait que pour certaines de ces équations (en particulier celle provenant de l'exemple de l'aimant), il est possible en quelque sorte de deviner l'équation décrivant le phénomène, mais cette équation contient un terme qui n'a aucun sens mathématique classique. Plus techniquement, ce terme fait intervenir des carrés ou des cubes de distributions, ce qui ne correspond *a priori* pas à des opérations licites. Ma contribution a été de développer une théorie générale qui permet de manière systématique de donner un sens mathématique à ces termes et ainsi aux solutions de telles équations.

*Comment se lance-t-on dans l'élaboration d'une nouvelle théorie ?*

C'est une question difficile. Dans ce cas particulier, il existait déjà une théorie développée par Terry Lyons dite des « rough paths », ce qui a été traduit en français par chemins rugueux ou fonctionnelles rugueuses. Dans certaines situations, unidimensionnelles, par exemple lorsqu'un système ne dépend que du temps, elle permet de donner un sens à certains des produits illicites que je mentionnais. Cette théorie s'applique par exemple à l'étude de l'évolution des prix des actions en bourse. On a alors un système qui ne dépend que du temps mais qui présente des fluctuations aléatoires. Mais cette théorie est vraiment unidimensionnelle et il n'y avait *a priori* pas de moyen de la généraliser à des systèmes dont le comportement dépendrait aussi de l'espace. J'ai tout d'abord commencé par réfléchir à ce qui faisait l'essence de cette théorie. Il y a justement un énoncé dû à Massimiliano Gubinelli de l'université de Paris Dauphine qui peut être vu comme une sorte de condensé de cette théorie. Il a également l'avantage d'être très simple. Très

grossièrement, cet énoncé porte sur des fonctions de deux variables et la recherche de conditions sur une telle fonction, disons  $F(s, t)$ , garantissant qu'elle soit « proche » des incréments  $G(t) - G(s)$  d'une fonction d'une seule variable  $G$ , lorsque la distance entre  $t$  et  $s$  est petite. J'ai cherché à généraliser ce résultat au contexte suivant : on considère cette fois une fonction  $\xi(x, \cdot)$ , où  $x$  peut être un élément de  $\mathbb{R}^n$  et où, pour tout  $x$  fixé,  $\xi(x, \cdot)$  est une distribution sur  $\mathbb{R}^n$ . Le problème est alors d'obtenir des conditions sur la fonction  $\xi(x, \cdot)$  garantissant l'existence d'une unique distribution  $\eta$  sur  $\mathbb{R}^n$  telle que, pour tout  $x$ ,  $\eta$  est proche de  $\xi(x, \cdot)$  lorsque l'on considère les deux distributions au voisinage du point  $x$ . Mais ce n'est pas une mince affaire. Cette généralisation a été en quelque sorte le point de départ de l'élaboration de ma théorie. Et ensuite... on construit à partir de là ! (rires)

*Est-ce que tu as tout de suite eu l'intuition que ça allait marcher ?*

Non, pas vraiment. Il y a eu une première phase de tâtonnement dans laquelle j'ai essayé, à travers plusieurs articles, d'adapter la théorie de Lyons et le résultat de Gubinelli dans des cas simples. Mais ensuite, concernant le développement de la théorie générale, il y a eu un moment très précis où j'ai eu une sorte de déclic. Il s'agit d'un point relativement technique qu'il est difficile de décrire ici, mais j'ai su alors que cette approche mènerait assez loin.

*Tu mentionnais l'exemple du champ magnétique d'un aimant, tes travaux ouvrent-ils la voie à des applications dans d'autres disciplines, notamment en physique ?*

Personnellement, je me considère comme un mathématicien pur et ce sont avant tout les problèmes mathématiques qui m'intéressent. Mais la physique est bien sûr une source extraordinaire de problèmes mathématiques.

*Est-ce que des physiciens utilisent déjà tes travaux ?*

Non, je ne crois pas. En fait, ma contribution se situe vraiment à un niveau fondamental. Il ne s'agit par exemple pas d'un outil calculatoire dont les physiciens pourraient disposer. Mes travaux permettent de justifier et de rendre mathématiquement rigoureuses certaines intuitions des physiciens, mais je ne suis pas sûr que ce soit vraiment primordial à leurs yeux. (sourire)

*Une fois qu'on dispose de ces fameuses équations, j'imagine qu'on souhaite en trouver les solutions. Cela pose-t-il de nouveaux problèmes ?*

Cela dépend des équations considérées. Pour celles que j'ai étudiées pour le moment, la question de l'existence et de l'unicité est essentiellement triviale localement en temps et dans les domaines bornés. Mais savoir si des solutions existent pour tout temps, est une question de nature totalement différente. La situation est comparable à celle de l'équation de Navier-Stokes en dimension trois : obtenir des solutions locales pour des conditions initiales suffisamment régulières est complètement trivial, alors que trouver une solution globale est un problème à un million de dollars ! La théorie que j'ai développée permet de résoudre le premier type de problème (donner un sens aux équations, puis obtenir des solutions locales). Mais, d'une certaine façon, elle est un outil également nécessaire pour

étudier le deuxième type de problèmes (celui des solutions globales), puisqu'auparavant on ne pouvait même pas se poser la question dans ce contexte.

*Revenons un peu à la médaille Fields. As-tu été surpris de compter parmi les lauréats ?*

Je savais que j'étais dans la course, mais c'était le cas de beaucoup d'autres personnes. Je crois qu'il y a toujours une part d'aléatoire, de chance et de *timing* dans l'attribution de ce genre de prix. J'ai eu beaucoup de chance... Le *timing* a justement été très favorable, mais je n'aurais pas pensé que cela suffirait. Lorsque j'ai reçu le courriel d'Ingrid Debauchies, cela a quand même été une grande surprise.

*Tu sembles avoir un profil légèrement atypique, non ?*

J'ai un peu ce sentiment, effectivement. Au moins dans le sens où cela n'était absolument pas une ambition que ce soit durant mes études ou ensuite durant ma carrière de mathématicien. Je n'ai jamais travaillé dans l'optique d'avoir la médaille Fields ou un quelconque autre prix. C'est peut-être un peu atypique, mais cela dit je ne peux parler au nom des autres médaillés.

*Qu'est-ce que cette reconnaissance va changer pour toi ?*

J'espère que cela ne va pas changer ma façon de travailler, mais je ne sais pas encore vraiment ce qui m'attend. En tout cas, j'ai l'intention de continuer à faire de la recherche activement. Même si j'imagine bien que je serai amené à avoir de nouvelles responsabilités...

*On trouve dans tes travaux des termes comme « ergodique » ou « mesure invariante », ce qui est bien sûr également le cas pour Artur Avila et Maryam Mirzakhani qui sont tous deux dynamiciens. De façon un peu plus surprenante, les travaux de Manjul Bhargava ont également une saveur probabiliste. Que penses-tu de ce point commun dans les travaux des différents lauréats ?*

Bien sûr nos travaux sont très différents, mais c'est vrai que quelque part les probabilités sont dans l'air du temps. C'est un domaine qui a eu énormément de reconnaissance ces dix dernières années, en tout cas beaucoup plus qu'auparavant. Il faut se rappeler que les probabilités, lorsqu'elles ont été introduites, n'étaient pas considérées comme des mathématiques. On trouve encore quelques traces de ce passé dans certaines universités où les départements de mathématiques sont séparés de ceux de probabilités et statistique. Mais aujourd'hui les probabilités sont reconnues comme un domaine à part entière et extrêmement important des mathématiques. Maintenant, je ne peux pas dire s'il s'agit là d'une mode passagère ou au contraire d'une tendance amenée à s'amplifier.

*Te considères-tu davantage comme un probabiliste ou un analyste ?*

Je me considère tout autant probabiliste qu'analyste. Maintenant, sans doute un peu par hasard, j'ai eu davantage de contact dans ma carrière avec des probabilistes qu'avec des analystes. Et il semble, pour des raisons peu claires, sans doute historiques, que la communauté des chercheurs étudiant les EDP stochastiques soit plus en contact avec celle des probabilistes qu'avec celle des « EDPistes classiques ».

*As-tu un héros mathématique, ou du moins une influence particulièrement importante ?*

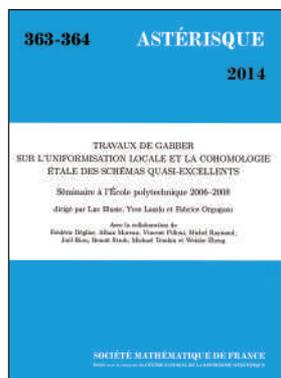
C'est difficile à dire et surtout de choisir un mathématicien en particulier. Dans mon domaine, il y a évidemment Kiyoshi Itô. Il a eu une influence énorme dans cette partie des probabilités. Et aussi Wiener... mais c'est vraiment trop difficile de choisir !

*Concernant ta façon de travailler, es-tu un travailleur solitaire ou plutôt un mathématicien social ?*

À vrai dire, un peu des deux. Un certain nombre de mes travaux sont en collaboration, mais j'ai également écrit plusieurs articles seuls. En particulier, celui dans lequel j'ai introduit cette théorie des structures régulières ou encore mon travail sur les équation KPZ. C'est vraiment partagé... Disons que cela dépend un peu du hasard et des circonstances.

*Dans le film de présentation des lauréats diffusé lors de la cérémonie d'ouverture du congrès, tu apparaissais aux fourneaux. Peux-tu nous en dire un peu plus sur tes hobbies ?*

(Rires) Oui, effectivement, mon épouse et moi adorons cuisiner ensemble et également nous promener dans la nature. Lorsque nous partons en vacances, nous privilégions des endroits où la nature est particulièrement intéressante, que ce soit dans la jungle, la montagne... J'aime également beaucoup le ski, mais je n'ai guère l'occasion de le pratiquer en Angleterre ! J'ai été un grand passionné d'informatique et de programmation, mais je n'ai malheureusement plus beaucoup de temps pour cette activité.



## Astérisque

### Dernières parutions

*Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents*

Luc Illusie, Yves Laszlo & Fabrice Orgogozo

avec la collaboration de F. Déglise, A. Morau, V. Pilloni, M. Raynaud, J. Raynaud, B. Stroth, M. Temkin, W. Zheng

Astérisque 363-364 - ISBN 978-2-85629-790-2

prix public\* : 140 € - prix membre\* : 98 €

*Theory of Hp-spaces for continuous filtrations in von Neumann algebras*

Marius Junge & Mathilde Perrin

Astérisque 362 - ISBN 978-2-85629-789-6

prix\* public\* : 36 € - prix membre\* : 25 €

*Séminaire Bourbaki, volume 2012/2013, exposés 1059-1073*

Astérisque 361 - ISBN 978-285629-785-8

prix public\* : 98 € - prix membre\* : 69 €

\*frais de port non compris



Institut Henri Poincaré  
11 rue Pierre et Marie Curie  
F-75231 PARIS CEDEX 05

<http://smf.emath.fr>

# THÉORIE DES TYPES ET MATHÉMATIQUES CERTIFIÉES

---

## Formalisation mathématique, certification logicielle, même combat !

Pierre-Louis Curien<sup>1</sup>

---

Qu'y a-t-il de commun entre les constructions mathématiques et les développements logiciels? Tout d'abord, le fait d'être souvent très complexes. On parle d'architectures logicielles, mais on pourrait aussi parler de l'architecture d'une preuve aussi complexe que celle du théorème de Fermat. On mesure aussi les prouesses dans les deux cas selon des critères assez similaires. On parle d'élégance pour une belle preuve, ou pour un beau programme. Dans le monde des langages de programmation, on recherche la portabilité et la réutilisabilité du code, qui font sens aussi dans le contexte des mathématiques : l'importance d'une théorie augmente considérablement lorsqu'elle est utilisée avec succès dans une autre branche des mathématiques, et des noms de mathématiciens sont souvent associés à des lemmes parfois « bêtes » mais tellement utiles, et utilisés à tout bout de champ.

En mathématiques et en informatique, il y a une tension, ou plutôt un va-et-vient, entre *sens* d'une part, et *langage formel* comme support du sens d'autre part (en linguistique, on parle de sémantique et de syntaxe). Un mathématicien communiquera généralement plus sûrement ses idées et résultats lors d'une présentation au tableau qu'à travers ses articles écrits, souvent arides. Un programme informatique est écrit pour répondre à une spécification (penser par exemple à la régulation des trains, qui de préférence ne doivent pas se percuter). Pour ce faire, les informaticiens préfèrent écrire leur code dans des langages de « haut niveau », qui sont reliés par une chaîne de compilations successives au langage machine, dont le code est exécuté par des processeurs parfaitement stupides, et en même temps totalement obstinés parce qu'obéissant exactement aux règles qu'on leur a demandé d'appliquer.

Dans les deux mondes, on cherche à être rigoureux : pas le droit à l'erreur, une preuve doit être juste, un programme ne doit pas contenir de bug. Seulement voilà, la liste des bugs informatiques est considérable, avec des coûts associés (financiers ou humains) parfois catastrophiques (pensons en particulier aux bugs

---

<sup>1</sup> Laboratoire Preuves, Programmes et Systèmes, équipe  $\pi r^2$ , CNRS, université Paris Diderot, et INRIA.

d'équipements médicaux informatisés). En mathématiques, les erreurs sont pratiquement inévitables, et sont particulièrement gênantes quand elles sont découvertes longtemps après que d'autres mathématiciens ont utilisé les « résultats » : « par le théorème X montré par Y dans la publication Z, nous pouvons conclure notre démonstration du théorème V, grâce à tous les résultats établis dans le présent article ». Vladimir Voevodsky raconte de telles mésaventures, qu'il a lui-même vécues (voir [www.math.ias.edu/~vladimir/Site3/Univalent\\_Foundations\\_files/2014\\_IAS.pdf](http://www.math.ias.edu/~vladimir/Site3/Univalent_Foundations_files/2014_IAS.pdf)).

Le besoin de correction est particulièrement important lorsque les preuves comportent des cas et des sous-cas en nombre si considérable qu'il faut faire appel à un ordinateur afin d'en faire l'étude exhaustive, comme pour le théorème des Quatre Couleurs, ou la conjecture de Kepler. Informatique et preuves donc, déjà ! Mais ce dont nous parlons ici est d'une autre nature : pour pouvoir faire confiance aux calculs de la machine, il faut pouvoir vérifier la validité des algorithmes sous-jacents – et tant qu'à faire *formaliser* la preuve toute entière, c'est-à-dire expliciter tous les détails et vérifier l'enchaînement logique des arguments. C'est ce qui a été réalisé, respectivement dans les assistants de preuve Coq (par Georges Gonthier, de Microsoft Research, Cambridge, Royaume-Uni) et HOL Light (par l'auteur de la preuve lui-même, Thomas Hales, de l'université de Pittsburgh, et par de nombreux collaborateurs, parmi lesquels en particulier l'auteur et le développeur de HOL Light, John Harrison, INTEL, Seattle).

Dans d'autres cas, c'est la longueur de la démonstration (et donc l'architecture dont nous parlions plus haut) qui pose question : un lemme partiellement fautif pourrait-il entraîner la chute de l'édifice ? Par exemple, dans le cas de la classification des groupes finis, des erreurs ont été détectées jusque dans les dernières semaines avant que la fin de ce vaste effort de recherche collectif ait été annoncé à la communauté mathématique. D'autres erreurs, heureusement mineures et sans conséquences, ont été repérées et corrigées au cours de la formalisation du Odd Order Theorem (une pièce importante de l'édifice), par Georges Gonthier et ses collaborateurs.

Le public est (malheureusement) plus habitué à l'idée que les bugs et autres failles informatiques font partie du paysage et sont « inévitables ». Le projet CompCert, dirigé par Xavier Leroy (INRIA Rocquencourt) marque une étape remarquable dans le développement d'outils pour garantir la sûreté des logiciels : pour la première fois, un compilateur complet d'un langage largement utilisé dans l'industrie (le langage C) a été entièrement certifié, c'est-à-dire vérifié, en Coq.

Ces tours de force réalisés en Coq, l'un de formalisation mathématique, l'autre de certification logicielle, tous deux achevés autour de 2012-2013, ont porté ce logiciel sur le devant de la scène, et ont certainement contribué à l'attribution par l'ACM, coup sur coup, du prix *Programming Languages Software 2013*, et du très prestigieux prix *Software System 2013*, décernés aux principaux auteurs et développeurs du logiciel (parmi lesquels Thierry Coquand, université de Göteborg ; Gérard Huet, INRIA Paris-Rocquencourt ; Christine Paulin-Mohring, université

Paris Sud et INRIA Saclay ; Bruno Barras, INRIA Saclay et École polytechnique ; Jean-Christophe Filliâtre, CNRS et INRIA Saclay ; Hugo Herbelin, INRIA Paris-Rocquencourt et université Paris Diderot ; Chet Murthy, Google Inc. ; Yves Bertot, INRIA Sophia ; et Pierre Castéran, université de Bordeaux). Le logiciel Coq, qu'une nouvelle génération de chercheurs continue de faire évoluer, rejoint ainsi une liste où figurent Unix, TeX, PostScript, TCP/IP, Java...

Mais qu'est-ce qu'un assistant de preuve ? C'est un logiciel (souvent interactif, c'est-à-dire permettant le développement progressif d'une preuve à partir de la conclusion) qui permet de vérifier d'autres logiciels, ou des preuves mathématiques, en explicitant toutes les étapes du raisonnement, ce qui suppose de ne laisser traîner aucun de ces « il est évident que », qui parfois cachent un lièvre. Le fait que ces assistants de preuve puissent être utilisés tant pour la formalisation de preuves mathématiques que pour la certification logicielle, au-delà des analogies esquissées plus haut, repose sur une correspondance très précise, connue dans le milieu spécialisé sous le nom d'*isomorphisme de Curry-Howard*, qui permet d'identifier les types ou les spécifications d'une part, les formules ou énoncés mathématiques d'autre part. Un programme d'un type donné ou satisfaisant à une certaine spécification correspond à une preuve formelle d'un théorème. Un troisième niveau relie enfin l'exécution des programmes à une notion de calcul sur les preuves, appelée élimination des coupures, qui joue un rôle fondamental pour prouver des résultats de cohérence, ou non-contradiction, des axiomes et des principes de raisonnement utilisés.

Le trimestre *Sémantique des Preuves et mathématiques certifiées*, qui s'est tenu à l'IHP au printemps 2014, que j'ai coorganisé avec Hugo Herbelin et Paul-André Melliès (chercheur CNRS, PPS), a mis à l'honneur ces assistants de preuve, à travers leur utilisation en mathématiques et en informatique, et a cherché aussi à mettre en lumière les développements théoriques qui ont permis de les concevoir : la théorie des types et la sémantique des langages de programmation, respectivement. Quelques-uns des grands pionniers à citer ici sont, sur le versant informatique :

- Dana Scott (émérite, Carnegie Mellon University), fondateur avec Christopher Strachey (université d'Oxford, 1916-1975) de la *sémantique dénotationnelle*, qui s'occupe d'associer aux programmes et aux preuves des objets vivant dans des structures mathématiques (typiquement des ensembles ordonnés, où la relation d'ordre modélise l'information partielle sur les données et les résultats) ;
- Gordon Plotkin (émérite, université d'Edimbourg), qui a amplifié considérablement ce programme et l'a complété en donnant ses lettres de noblesse à la *sémantique opérationnelle*, qui décrit le sens des programmes en spécifiant à haut niveau (c'est-à-dire en faisant abstraction des détails de l'implémentation) comment ils s'exécutent, à l'aide de règles formelles ;

et sur le versant logique :

- Jean-Yves Girard (émérite, CNRS et université de Marseille), créateur notamment du système  $F$  (voir ci-dessous), et de la *logique linéaire*, qui a profondément

transformé la sémantique dénotationnelle, en y incorporant l'analyse fine des ressources utilisées par les programmes (en temps, mais aussi en espace) ;

– Per Martin-Löf (émérite, université de Stockholm), auteur de la théorie des types dépendants, dont l'interprétation homotopique fait l'objet de ce dossier spécial pour la *Gazette*.

Pour revenir aux assistants de preuve, Coq est né du *Calcul des Constructions* de Huet et Coquand (1983), synthèse de la théorie de Martin-Löf et du système  $F$  de Girard (plus précisément son extension  $F\omega$  codifiant la logique propositionnelle d'ordre supérieur). Un exemple frappant montrant l'étroite interconnexion entre langages de preuves et langages de programmation, est le logiciel LCF de preuve de programmes conçu par Robin Milner (université de Cambridge, 1934-2010) dans les années 1970, et fondé sur les idées de la sémantique dénotationnelle. Milner avait développé pour ce système un langage de tactiques. Ce langage, appelé ML (pour *Meta-Langage*), a pris rapidement son indépendance et est devenu l'un des langages les plus utilisés dans la recherche sur les langages de programmation. Sa version la plus répandue est OCaml, dont l'implémentation est due principalement à Xavier Leroy.

Ces développements autour des preuves et des programmes, ainsi que les assistants de preuve eux-mêmes, sont à leur tour source d'idées nouvelles, comme celles de la théorie homotopique des types, qui suggère de nouvelles manières d'aborder les fondements des mathématiques, en reconnaissant le rôle prépondérant de la notion d'égalité, puis celle d'égalité entre preuves d'égalité, etc. Ils suggèrent également de nouvelles manières d'exercer l'activité de mathématicien : il est raisonnable de penser que les assistants de preuve, ou plutôt leurs futures versions, mieux pensées pour les non-spécialistes, seront dans quelque temps (dix, vingt ans ?), dans de nombreux domaines des mathématiques, des compagnons aussi naturels que (La)TeX ! Pas seulement pour leur confier des calculs (les logiciels de calcul formel offrent déjà pour cela une aide précieuse), ou des vérifications fastidieuses, mais aussi pour circuler dans une preuve complexe au fur et à mesure de sa construction, et enfin pour s'assurer de sa correction globale. Ceci allant de pair avec le développement d'outils permettant de développer des environnements sûrs pour les développeurs et utilisateurs des logiciels les plus divers.

## La bifurcation de Vladimir Voevodsky. De la théorie de l'homotopie à la théorie des types

Propos recueillis par Gaël Octavia<sup>1</sup>

---

*Le mathématicien Vladimir Voevodsky nous raconte ici comment il a fait le choix de quitter l'univers des mathématiques pures, qui l'avaient pourtant couronné de succès et lui avaient valu de remporter la médaille Fields en 2002, et d'embarquer pour de tout autres aventures : la logique et les fondements univalents, l'informatique fondamentale et les assistants de preuve. Cet entretien est disponible sous forme filmée à l'adresse suivante :*

*<http://www.icm2014seoul-blog.com/videos-en-preambule.html>*

Bonjour, je suis Vladimir Voevodsky. Je suis actuellement professeur à l'Institute for Advanced Study à Princeton dans le New Jersey. Je suis en poste là-bas depuis 2002. Pendant la première partie de ma carrière, j'ai surtout fait de la géométrie algébrique. J'ai travaillé sur l'application de diverses méthodes issues de la théorie de l'homotopie à des problèmes de géométrie algébrique. J'ai toujours été fasciné par la puissance de cet outil, à savoir la théorie de l'homotopie. J'ai presque envie de dire que c'est la nouvelle arithmétique. C'est une théorie qui peut être utilisée dans un large spectre de domaines mathématiques et qui peut être un outil de calcul très puissant. J'ai donc appliqué cette théorie à des questions complexes d'algèbre et de géométrie algébrique, en particulier à la *conjecture de Milnor* et à la *conjecture de Bloch-Kato*; ce sont des conjectures en algèbre pure mais les méthodes utilisées pour les démontrer appartiennent à la géométrie algébrique, avec des intuitions venant de la théorie de l'homotopie. Je trouve que c'est vraiment beau.



*Comment vous êtes-vous intéressé à la théorie des motifs ?*

À l'époque où j'ai commencé à faire des mathématiques de manière professionnelle, disons entre 1987 et 2002, date à laquelle j'ai obtenu la médaille Fields, j'ai construit ma carrière en mathématiques, et à cette époque, cette idée de motifs, introduite par Grothendieck, était un sujet très « tendance » dans la communauté

---

<sup>1</sup> Fondation Sciences Mathématiques de Paris.

mathématique russe. Alors évidemment, l'ambitieux jeune homme que j'étais a été attiré par ce sujet qui était le plus « tendance », le plus difficile et d'une certaine façon le plus ésotérique parmi les mathématiques de cette époque.

*Pour quels travaux avez-vous remporté la médaille Fields en 2002 ?*

J'ai eu la médaille Fields pour ma preuve de la conjecture de Milnor. J'avais trouvé la démonstration début 1995, j'en avais rédigé l'essentiel fin 1996 et elle a été publiée en 2000. C'était vraiment fascinant de travailler sur ce sujet qui faisait intervenir tant de domaines des mathématiques très en vogue. Je me suis vraiment beaucoup amusé et j'ai beaucoup travaillé aussi ! Ce que dit cette conjecture c'est que pour tout nombre entier naturel  $n$  et tout corps  $K$  « quelque chose » est vrai, sauf qu'il y a des cas particuliers... Pour certains  $K$ , cela ne marchait pas pour tous les  $n$ , et pour certains  $n$ , cela ne marchait pas pour tous les  $K$ . Et les démonstrations pour ces divers cas particuliers étaient différentes les unes des autres, il n'était pas possible de les combiner ensemble pour en faire une preuve générale. La preuve du cas particulier le moins trivial était très étrange. Beaucoup de gens avaient du mal à comprendre cette preuve comme la conséquence de principes généraux, ou à voir clairement quels principes généraux il y avait en fait derrière. C'était très mystérieux. Beaucoup de mathématiciens ont essayé d'établir la preuve générale. Beaucoup de conjectures dépendaient de celle-ci ou s'en déduisaient, ce qui fait que quand j'ai été en mesure de la démontrer, cela a permis de développer bien d'autres choses. Je ne passais pas le plus clair de mon temps à travailler spécifiquement sur la conjecture. J'étais en train de développer cette théorie générale de *l'homotopie motivique*, ou théorie de la cohomologie motivique. À un moment, j'ai senti que j'avais une boîte à outils qui contenait des objets nouveaux, alors j'ai cherché quelque chose de spectaculaire à faire, histoire de montrer que ces outils étaient intéressants. Et c'est comme cela que cette conjecture a attiré mon attention, c'était quelque chose à tenter avec mes nouveaux outils. Et quand la preuve a été claire, c'est encore le développement d'outils généraux sous-tendant cette preuve qui a été délicat. Donc le travail sur la conjecture proprement dite a peut-être représenté 20% de mon temps, tandis que 80% de mon temps était consacré au développement des outils généraux pour cet usage particulier qu'était la preuve de cette conjecture.

*Pouvez-vous nous en dire plus sur ces théories ?*

C'est difficile pour des non-spécialistes, et d'ailleurs le fait que ce soit difficile à expliquer est une des raisons qui m'ont poussé à changer de sujet de recherche. C'était extrêmement frustrant de me dire qu'il n'y avait que 10 personnes au monde à qui je pouvais raconter mon travail, et que pour toutes les autres, je devais utiliser des analogies très primaires, sans pouvoir expliquer ce que je faisais. Cette frustration a joué un grand rôle dans mon choix de ce que j'allais faire ensuite : je ne voulais plus d'un sujet aussi ésotérique. Par ésotérique, j'entends réservé à une toute petite communauté.

Mais on peut partir de là pour en venir à ce que je fais maintenant. J'ai eu des idées générales susceptibles de me permettre d'étendre cette boîte à outils de la théorie de l'homotopie motivique. Mais cela requerrait l'utilisation systématique de ce qu'on appelle les 2-catégories. Et j'étais très frustré par le fait que je ne voyais pas très clairement comment expliquer mes raisonnements à propos de ce

genre d'objets. C'est une chose que de faire des diagrammes et de réfléchir à ces 2-catégories d'un point de vue purement algébrique, mais c'est tout à fait différent de les utiliser comme outils pour calculer d'autres choses. Il y avait des parties de mon raisonnement où je sentais qu'il fallait en faire plus, mais je ne pouvais pas expliquer pourquoi. Cela n'avait pas de sens dans une approche classique du raisonnement mathématique. J'étais incapable d'expliquer pourquoi telle chose devait être faite de cette façon-ci, et surtout pas de cette façon-là. À ceci s'est rajoutée une autre frustration : celle de rédiger des articles remplis de raisonnements complexes dans un domaine où très peu de gens avaient les compétences pour vérifier si ce que j'avais fait était juste. La vérification de mes démonstrations pouvait prendre des années. Et j'ai senti que si j'amenais encore plus d'abstraction, de complexité, de constructions de haut niveau dans tout cela, il deviendrait tout simplement impossible à quiconque de contrôler ce qui se passait ! De plus, il m'était devenu difficile d'amener de nouvelles idées, car j'étais sans cesse préoccupé par la question de savoir si ceci était juste, si je pouvais m'appuyer sur cela. Comme je n'avais personne pour vérifier ce que je faisais ou ce que j'avais fait, c'était vraiment désagréable. C'est avant tout pour cela que j'ai arrêté la théorie de l'homotopie motivique, ce que j'ai fait effectivement après que mon dernier article sur la conjecture de Bloch-Kato a été accepté.

Je me suis vraiment dit : terminé, je vais faire autre chose. Il y avait en fait plusieurs possibilités. Je pouvais faire quelque chose qui fasse un lien entre mathématiques pures et appliquées, ou faire quelque chose autour de la vérification de preuves par ordinateur et les assistants de preuve. J'avais donc deux possibilités et dans un premier temps j'ai pensé que faire le lien entre mathématiques pures et appliquées était plus simple. J'ai donc essayé, et à un moment j'ai réalisé que j'avais perdu mon temps à faire n'importe quoi. Je me suis donc tourné vers la question de la vérification de preuves et là, cela a commencé à être fructueux. Et donc à partir de 2009, je me suis consacré entièrement à ce travail sur les assistants de preuve.

*Comment cette question de la possibilité d'une erreur (surtout quand un résultat n'est compris que par très peu de collègues) est-elle appréhendée par les mathématiciens ?*

Je pense que l'on comprend dans la communauté mathématique que c'est un problème, mais que c'est quelque chose dont on n'aime pas tellement parler. On se sent impuissant face à cela. C'est comme quand on n'a pas de remède à une maladie, on préfère ne pas mentionner cette maladie. Et puis il suffit qu'on trouve un remède pour que tout le monde se mette à en parler. C'est un peu pareil avec cette question des preuves et des erreurs en mathématiques. De même, publier un résultat intéressant, et voir que personne n'y réagit, parce que personne ne peut le comprendre, ou bien parce que tout le monde est occupé à faire publier ses propres résultats, pose problème. Les mathématiciens connaissent très bien ce phénomène d'absence de résonance d'un résultat que l'on publie. J'aimerais pourtant pouvoir en savoir plus sur les choses formidables que font d'autres mathématiciens. Le problème, c'est que quand je commence à lire un article, je n'arrête pas de tout vérifier. Donc lire un article devient quelque chose de fastidieux. On ne peut pas juste lire et faire confiance, apprécier. Et c'est pourquoi je pense que quand on aura établi une culture dans laquelle chaque résultat sera certifié par ordinateur,

alors on pourra juste lire, faire confiance, apprécier, au lieu de douter, de trouver ça fastidieux, voire de ne pas lire du tout.

### *Qu'est-ce que la théorie des types ?*

Il y a quelque chose d'une grande complexité derrière cette appellation de « théorie des types ». À l'origine, l'expression apparaît probablement dans l'œuvre de Russell, dans la première décennie du XX<sup>e</sup> siècle. Et à cette époque, l'idée des types était quelque chose qui servait à traiter, à éviter les paradoxes au sein de divers systèmes de logique formelle, c'était perçu comme quelque chose de contraignant<sup>2</sup>. Nous aurions adoré faire nos mathématiques dans le monde merveilleux des prédicats sans contraintes, en considérant que le monde entier est constitué d'objets et qu'il y a des prédicats qui sont en gros les propriétés de ces objets. En manipulant les prédicats de manière logique, nous aurions pu tout décrire, et plus particulièrement en mathématiques. Sauf qu'il y avait les paradoxes. C'est pourquoi on a introduit les types. Les types sont a priori restrictifs de par leur nature. Ils interdisent de faire certaines choses, et ces interdits, nous les intégrons dans notre manière de penser, sans quoi on produirait des paradoxes. Cela a été longtemps ainsi...

À quel moment exactement les types sont-ils passés d'un dispositif qui restreint à un dispositif qui ouvre des possibilités ? À un moment donné, dans les années 1960, je pense, les *types inductifs* ont été introduits dans les langages de programmation pour exprimer des concepts comme le filtrage. À la fin, les types sont devenus des dispositifs qui permettent de faire des choses. Il y a eu la théorie des types de Russell, puis la théorie des types de Church dans les années 1940, et enfin la théorie des types de de Bruijn et Martin-Löf des années 70 jusqu'au début des années 1980. Donc vous pouvez voir que le développement a été extrêmement lent. C'est ce qui s'est passé en 100 ans. Si on fait la comparaison avec le développement des mathématiques, avec la complexité, la variété, et la beauté des structures qui ont été découvertes en trois décennies, on peut dire que la théorie des types a rampé par rapport à l'extraordinaire prospérité des mathématiques. Mais elle a quand même fait du chemin. Elle est devenue un dispositif puissant pour combiner le raisonnement logique et l'informatique. Maintenant, avec l'idée de théorie des *types homotopiques*, une nouvelle dimension s'ajoute qui ne consiste plus simplement à combiner la logique et l'informatique, mais qui consiste aussi à faire ces deux choses dans le royaume des structures mathématiques en grandes dimensions, comme les catégories. On n'a pas encore trouvé de système complètement satisfaisant pour une telle synthèse, mais on a parcouru pas mal de chemin ces cinq dernières années pour se rapprocher de ce qui était alors un rêve lointain. Nous avons maintenant un système dans lequel travailler, système qui n'est pas parfait, mais qui est quelque chose de tangible.

### *Comment expliquer ce projet de « fondements univalents » sur lequel vous travaillez ?*

Le projet des *fondements univalents* a été pour moi quelque chose d'inattendu. Je ne m'attendais pas à ce qu'un tel projet puisse devenir réel si rapidement.

<sup>2</sup> Voir en particulier le paragraphe 2.1 de l'article de A. Pelayo et M. A. Warren.

Le point de départ est probablement l'article FOLDS de M. Makkai<sup>3</sup>. Makkai y examine l'idée de quelque chose qu'il appelle les « fondements univalents ». Dans ce cadre, l'univers n'est pas l'univers des ensembles dans lequel les mathématiciens travaillent, mais l'univers des  $\infty$ -catégories. Pour travailler avec des objets dans cet univers, nous avons besoin non pas de la logique du premier ordre, mais d'une logique à types dépendants, parce que nous voulons pouvoir parler de morphismes entre deux objets, plutôt que de parler de morphismes dont la source est égale au premier objet et dont la cible est égale au second objet<sup>4</sup>.

La percée qui a vraiment mené les fondements univalents à ce qu'ils sont aujourd'hui, a été de comprendre que le mot  $\infty$ -catégories pouvait être remplacé par *groupoïdes*, et que ce sont les groupoïdes et les  $\infty$ -groupoïdes qui sont fondamentaux, là où les catégories, qui sont des structures très utiles sur les groupoïdes, ne sont qu'une sorte de structures utilisables parmi d'autres. Les groupoïdes doivent être compris, non pas comme un cas particulier de catégories, mais comme quelque chose de fondamental, tandis que les catégories doivent être comprises comme des groupoïdes munis d'une structure additionnelle. Avec ce changement de perspective, les fondements univalents sont possibles, car si nous ne savons pas ce qu'est une  $\infty$ -catégorie, nous savons ce qu'est un  $\infty$ -groupoïde. C'est juste un type d'homotopie, on le sait grâce à Grothendieck. Nous savons donc ce qu'est cet univers de  $\infty$ -groupoïdes. C'est la même chose que l'univers des types d'homotopie. C'est beaucoup plus facile à définir précisément. Et de là, j'ai donc vraiment pu établir la construction d'un modèle au sens de la théorie des types de Martin-Löf, où tout est représenté dans la catégorie homotopique. J'ai commencé à m'amuser avec cela avec l'assistant de preuve Coq, car Coq est une implémentation de la théorie des types de Martin-Löf sur ordinateur, qui existe depuis plus de 20 ans. Donc j'ai commencé à jouer avec tout cela en pensant au modèle homotopique, et j'ai réalisé que je pouvais faire tout ce que je voulais faire auparavant, sans que cela ne nécessite plus d'investissement. Je me suis dit que nous avions désormais de nouveaux fondements pour les mathématiques.

*Utilisez-vous la théorie de l'homologie sur laquelle vous travailliez auparavant dans votre travail actuel ?*

De par ma façon de travailler en dessinant des figures, des diagrammes, cela m'est très utile. Je fais cela tout le temps : je formalise en Coq, je fais mes mathématiques en Coq, mais je continue à faire mes dessins sur le tableau noir, mes diagrammes, mes limites homotopiques. Cette intuition qui vient du fait de travailler avec des catégories de modèles, ces catégories homotopiques, m'est extrêmement utile et je continue à m'en servir. Sinon, mes connaissances en géométrie algébrique n'interviennent pas plus que cela jusqu'ici.

<sup>3</sup> « First-order logic with dependent sorts, with applications to category theory » <http://www.math.mcgill.ca/makkai/>

<sup>4</sup> Le point de vue traditionnel de la théorie des (multi-)graphes est d'avoir un ensemble de sommets  $V$  et un ensemble d'arêtes  $E$ , et d'indiquer pour chaque arête sa source et son but, ce qui donne deux fonctions « source » et « but » de  $V$  dans  $E$ . Mais le point de vue plus standard en théorie des catégories (qui ne sont rien d'autre que des graphes avec une opération de composition) est de fixer pour chaque paire de sommets  $a, b$  dans  $V$  un ensemble  $\text{Hom}(a, b)$  (les arêtes de  $a$  vers  $b$ ).

*Diriez-vous que votre vision des mathématiques, ou de votre métier de mathématicien, a changé ?*

Oui, elle a beaucoup changé, de même que la manière, en pratique, dont je fais des mathématiques. *Ma vision de ce qui est intéressant a changé.* Et les sensations que j'éprouve quand quelque chose marche ou ne marche pas, tout cela a changé !

*Est-ce que vous diriez que vous avez maintenant un point de vue plus constructiviste ?*

Ce qui est remarquable avec les fondements univalents, c'est qu'ils sont naturellement constructivistes. Et ils permettent de faire de manière constructive des choses que l'on ne pouvait pas faire de cette façon auparavant. Il est donc devenu tout à fait réaliste d'envisager des mathématiques constructives intéressantes, sans vouloir offenser les constructivistes. Mais je parle du point de vue de la communauté mathématique, de ceux qui utilisent les mathématiques de manière professionnelle. Je crois que nous avons toujours voulu quelque chose de plus, pouvoir utiliser plus d'objets, plus de constructions mathématiques. Si l'on considère les mathématiques constructives au sens restrictif, c'est-à-dire en empêchant quelqu'un d'utiliser quelque chose, c'est un peu étrange. Mais maintenant, avec les fondements univalents, on peut faire de bonnes mathématiques constructives. Pour moi, la *logique constructive* est beaucoup plus intéressante que la *logique classique* : elle est beaucoup plus proche du comportement réel. Par exemple, en logique classique, comme la double négation équivaut à l'identité, il n'y a aucune différence entre une proposition affirmative et une proposition négative. Nous y sommes habitués. Mais quand vous commencez à disposer de l'option qui consiste à vous dispenser de cette identification, vous comprenez que vous pouvez faire des mathématiques intéressantes dans un monde logique où une proposition positive n'équivaut pas à une proposition négative, et où il y a, de fait, une différence entre les choses positives et les choses négatives. Il me semble que c'est plus proche de la vérité. Maintenant je pense donc qu'il est vraiment très intéressant de faire les choses de manière constructive.

*Qu'en est-il des logiciels « assistants de preuve » ?*

Les *assistants de preuve* sont au cœur de mon approche des fondements univalents. Ceux-ci ne sont possibles qu'avec les assistants de preuve, ces fondements sont en effet beaucoup plus complexes si l'on ne dispose pas d'ordinateurs qui puissent manipuler les formules dont on a besoin. Mon but initial n'a jamais été de recréer les fondements des mathématiques. Mon but était, et est toujours, de contribuer à la création d'assistants de preuve utilisables pour qu'un jour, peut-être, j'aie la satisfaction de m'asseoir devant mon ordinateur et de me remettre à travailler sur mes théories mathématiques en faisant les choses comme je pense qu'elles devraient être faites, avec un assistant de preuve avec lequel je puisse travailler. Les assistants de preuve sont très importants. La partie la plus connue de leur histoire est probablement celle qui se situe de la fin des années 1960 au début des années 1970. À cette époque, deux assistants de preuve sont développés, *Automath* par de Bruijn, aux Pays-Bas, et *Mizar*, en Pologne. Mizar, qui est toujours en développement, repose sur la théorie des ensembles. C'était donc quelque chose de rassurant pour les mathématiciens habitués à travailler

dans ce cadre. Automath reposait sur un socle original que de Brouijjn avait inventé. Il y avait aussi LCF. Aujourd'hui, la situation est la suivante : il y a plusieurs assistants de preuve qui sont activement développés, et pour chacun d'entre eux, il y a un groupe de personnes qui s'y consacrent activement. Il y a aussi d'autres assistants de preuve qui apparaissent. Personnellement j'utilise habituellement Coq dans mon travail, et j'essaie d'y contribuer, de suggérer des améliorations inspirées de l'idéologie des fondements univalents. La question est de savoir quel assistant peut bénéficier des nouvelles idées explorées avec les fondements univalents. C'est une question complexe.

*On connaît des théorèmes dont la démonstration a été « certifiée par ordinateur », le théorème des quatre couleurs, par exemple...*

Le théorème des quatre couleurs est un bon exemple illustrant la question de l'intégration du calcul par ordinateur dans l'aide à la preuve. Car ce théorème a été démontré à l'origine en utilisant du calcul par ordinateur et les gens étaient dubitatifs. Ils n'étaient tout d'abord pas sûrs du calcul lui-même, ni du logiciel utilisé. Ensuite, il n'était pas clair qu'un calcul par ordinateur puisse être valable au même titre que le raisonnement logique. Ensuite, G. Gonthier a établi une preuve complète du théorème en Coq ; cette preuve comportait à la fois un raisonnement logique et des calculs par ordinateur, mais le tout était fait en Coq, dans un même système. Cette démonstration a donné naissance à un nombre intéressant que Tom Hales a évoqué, donc je l'ai appelé « nombre de Hales ».

Il existe un nombre nommé « nombre de de Brouijjn » qui sert à comparer la longueur d'une preuve formelle à celle d'une preuve écrite en langage humain. Et pour un assistant de preuve, ce nombre est un invariant. Un assistant de preuve est d'autant plus mauvais que ce nombre est grand. Pour le travail le plus long que j'aie effectué sur les fondements univalents, le nombre de de Brouijjn est inférieur à 1, donc cela aurait pris beaucoup plus de temps de faire cela à la main que cela n'en a pris sur Coq. Ce nombre est très important du point de vue de l'usage quotidien des assistants de preuve.

Il y a un autre nombre important qui est le suivant : considérons des calculs faits avec l'ordinateur, que ce soit ceux de la preuve du théorème des quatre couleurs ou ceux de la preuve de la conjecture de Kepler par Tom Hales. Dans les deux cas, une partie de la preuve utilise des calculs avec un logiciel de calcul numérique. Maintenant, prenons tout ce calcul, et au lieu de le lancer avec l'ordinateur, on en fait une partie d'une preuve certifiée. Au lieu de faire du calcul directement, on le fait donc avec un assistant de preuve tout en effectuant la procédure de certification de la preuve. La longueur du calcul fait directement par ordinateur et la longueur du même calcul fait avec l'assistant de preuve peuvent alors être comparées. Quand vous écrivez le code du programme nécessaire pour que l'assistant de preuve fasse un calcul et qu'ensuite vous faites le même calcul, mais en écrivant un programme en C, il y a une différence de temps entre les deux et c'est ce que j'appelle le nombre de Hales. Le nombre de Hales mesure à quel point la programmation avec assistant de preuve est plus lente que la programmation classique. Dans le cas de l'assistant de preuve que Thomas Hales a utilisé pour sa preuve de la conjecture de Kepler, le coefficient était de 2000. C'est un nombre très élevé. C'est fâcheux si vous voulez que le calcul certifié devienne la norme en calcul scientifique en général.

Or il me semble important de commencer à utiliser la certification dans les champs d'application des mathématiques, comme la physique, la biologie. Donc ce nombre de Hales va être déterminant dans l'acceptation de la certification. Il faudra réussir à passer de 2000 à un nombre proche de 1. C'est une frontière importante dans le développement des assistants de preuve.

Il reste, de plus, plusieurs problèmes à résoudre, plusieurs portes à ouvrir pour populariser l'utilisation des assistants chez les mathématiciens, leur installation sur un ordinateur pour commencer. Jusqu'à récemment Coq ne pouvait pas s'installer sur Mac OS. Se pose aussi la question des fondements des mathématiques sur lesquels on s'appuie. Par exemple, utiliser Coq suppose de s'appuyer sur quelque chose comme les fondements univalents, à mon avis, parce qu'utiliser Coq avec la théorie des ensembles me semble un peu incongru. Dans le cas de Coq, de mon point de vue, le principal défaut réside dans la faiblesse de la propriété de substitution dans les égalités. Parfois une partie de la démonstration semble évidente et vous vous dites que cela ne devrait pas prendre tant de place et être si complexe.

*Que dire à ceux qui imaginent ces logiciels comme des outils qui à terme « feront » les mathématiques tous seuls, ou remplaceront les mathématiciens ?*

L'idée que les assistants de preuve puissent mener les mathématiciens à être remplacés par les ordinateurs est d'une totale absurdité, de même que l'idée, en général, que les machines puissent remplacer les hommes. Les mathématiques sont un champ de création. Bien sûr, les ordinateurs ont remplacé les gens qui faisaient des calculs, quand le calcul faisait encore partie de grands projets dans les années 1940, par exemple. Les ordinateurs ne peuvent que servir, ils ne peuvent pas développer d'énergie humaine ou sociale par eux-mêmes. Ceci dit, certains mathématiciens sont en effet préoccupés par ces développements, pas du tout parce qu'ils ont peur d'être remplacés par des machines, mais peut-être par peur d'être mis en compétition avec d'autres mathématiciens, et plus particulièrement les mathématiciens plus jeunes, rompus à l'usage des assistants de preuve. Je peux aisément comprendre ce sentiment : on est en train de faire quelque chose que l'on aime faire, et soudain quelqu'un arrive et vous dit que maintenant il faut le faire en utilisant ce nouvel outil, vous devez apprendre à utiliser cet outil, ce qui va ralentir votre travail... Mon espoir est que le bénéfice de ces nouveaux outils sera supérieur au coût. Il y a certes cette tension, mais ce changement finira par être accepté par la communauté mathématique.

*À terme, l'utilisation des assistants de preuve va-t-elle se généraliser ?*

Je l'espère. Les assistants de preuve sont absolument nécessaires. Sinon nous allons rester séparés dans des sous-communautés. La question est d'essayer de ne pas les imposer à tout le monde. Je pense également qu'il est essentiel que l'on puisse disposer de plusieurs assistants de preuve fiables, qu'il n'y en ait pas un seul que tout le monde utilise, et que toute la communauté soit paralysée si quelque chose se passe avec un logiciel ou l'équipe qui le développe. Aujourd'hui il y a de plus en plus de discussions sur plusieurs assistants de preuve confirmés et il y a une certaine communication entre eux. Je suis donc certain que la généralisation de l'usage des assistants de preuve se fera.

Nous remercions Pierre-Louis Curien et Christian Retoré pour leur aide précieuse lors de la préparation de cet entretien.

# Homotopy type theory

Álvaro Pelayo<sup>1</sup>, Michael A. Warren<sup>2</sup>

---

*To Vladimir Voevodsky,  
whose Univalence Axiom has opened many mathematical doors*

We give a glimpse of an emerging field at the intersection of homotopy theory, logic, and theoretical computer science: *homotopy type theory*. One key ingredient of this approach is Vladimir Voevodsky's *Univalence Axiom*. It is the goal of this paper to provide a short introduction to some of the ideas of homotopy type theory and univalence. The approach taken here is to first develop some of the historical and mathematical context in which homotopy type theory arose and then to describe the Univalence Axiom and related technical machinery.

## 1. Introduction

The past decade has seen the birth of a new research field at the intersection of pure mathematics and theoretical computer science: *homotopy type theory*. It is in the framework of homotopy type theory, that Vladimir Voevodsky formulated his celebrated *Univalence Axiom* and stated his ideas regarding *univalent foundations*.

Homotopy type theory [4, 21, 12] is an emerging field which brings together insights from research in pure mathematics (higher-dimensional category theory, homotopy theory, mathematical logic, etc.) and computer science (type theory, programming languages, proof assistants, etc.). Whereas in the usual approach to the foundations of mathematics one takes sets as the basic entities from which mathematical structures are constructed, in homotopy type theory the basic entities are *spaces* (homotopy types), in the sense of homotopy theory, rather than sets. The key insight which led to the development of homotopy type theory is the realization that a direct axiomatization of spaces already existed in Martin-Löf's work on type theory. Because type theory, which plays an important role in mathematical logic, is the theoretical basis for many current programming languages and computer proof assistants (*Coq*, *Agda*, etc.), proofs in homotopy theory and other parts of pure mathematics can be formally verified in proof assistants using the ideas of homotopy type theory.

This approach is justified by the *homotopy theoretic interpretation* of type theory, which was independently discovered by Awodey and Warren [5, 30] and Voevodsky [27, 28], building on ideas of Hofmann and Streicher [11, 24], Moerdijk, Palmgren, and others. This interpretation relates structures arising

---

<sup>1</sup> University of California, San Diego Mathematics Department La Jolla, USA. Pelayo is partly supported by NSF CAREER Award DMS-1055897 and Spain Ministry of Science Sev-2011-0087.

<sup>2</sup> Los Angeles, CA, USA

in homotopy theory, such as Kan complexes and Quillen model categories, with Martin-Löf's [19, 17] dependent type theory. At around the same time, Gambino and Garner [7], van den Berg and Garner [6], and Lumsdaine [16] showed that this interpretation could be turned around to construct homotopy theoretic structures from the syntax of type theory. Crucial to this entire endeavor was Voevodsky's discovery of the *Univalence Axiom* which captures important features of his Kan complex model of type theory. (Kan complexes, which are especially nice combinatorial models of spaces and  $\infty$ -groupoids, are discussed more in Section 2.8 below.)

The following ingredients make homotopy type theory possible:

- (1) The homotopy theoretic interpretation of type theory.
- (2) The Univalence Axiom.
- (3) Higher-inductive types or other type theoretic encodings of homotopy theoretic data.

We have already encountered items (1) and (2) above. Item (3) is roughly the type theoretic analogue of combinatorial models of spaces such as models using CW-complexes or simplicial sets. In summary, item (1) shows that it is indeed consistent to view types as spaces. Item (2) forces types to behave more like spaces and item (3) makes it possible to describe familiar spaces and constructions on spaces (spheres, suspensions, etc.) in terms of types.

The goal of the present paper is to describe in an informal way some of the ideas which have made their way into homotopy type theory. In particular, we touch, in varying levels of detail, on all three of the ingredients mentioned above.

**Summary of the paper.** In Section 2 we develop some of the background material which, while not strictly necessary, should provide a clearer historical and mathematical context for homotopy type theory. In particular, we describe the development of type theory in parallel with developing some simple, but important, ideas from algebraic topology. These small “vignettes” are designed to help draw out some of the analogies between homotopy theory and type theory. In particular, both homotopy theory, especially when viewed from the perspective of higher-dimensional category theory, and type theory have made use of ideas related to annotating known mathematical structures with additional data. For example, up-to-homotopy, algebraic structures are the result of taking familiar equational theories (such as the theory of groups) and replacing the equations by “annotating” homotopies. On the other hand, Church's simple type theory can be seen as the result of annotating derivations in propositional logic.

In Section 3 we introduce the Univalence Axiom and other ideas of Voevodsky regarding the foundations of mathematics. This section is the heart of the paper.

In Section 4 we make some concluding remarks regarding connections between homotopy type theory and computer assisted proof. This is something which we do not treat in detail, but which is important since it has been one of the motivating factors for Voevodsky and others working in this area.

**Other relevant literature.** Although there is some overlap between the present paper and our papers [21, 4], the exposition here is focussed a bit more on the logical side of matters and we here include more detail of the historical context on

the logical side. For a very brief introduction to Voevodsky's Univalence Axiom we invite the reader to consult [4]. For a detailed look at homotopy type theory and univalent foundations with a view towards the formalization of mathematics in Coq we suggest [21]. The textbook [12] develops the theory more or less from first principles. Those readers interested in the semantics of homotopy type theory should look at [3, 26, 25]. A recent overview of a wider range of connections between category theory and logic can be found in [8]. Many of the ideas described in Sections 2.2 and 2.4 below are developed more fully in [9], which is one of the canonical references for type theory and its connection with logic. Voevodsky's own description of his Coq library can be found in [29].

We hope that this article will serve to persuade many readers to learn more about the fascinating emerging subjects of homotopy type theory and Voevodsky's univalent foundations program; we believe these subjects will be of mathematical interest in the long term, and that there is great potential that their further development will have a significant impact on the way working mathematicians read, write, and discover proofs.

## 2. A few mathematical vignettes

Although homotopy type theory is a new subject, there is a long history of connections between logic, topology and algebra. A brief survey of some of these connections should help to demystify some of the concepts of homotopy type theory and will allow us to develop some of the required background incrementally. Note though that we are not historians of mathematics and, as such, the sketch presented here is admittedly biased and incomplete.

### 2.1. Set theoretic antinomies and Russell's theory of types

Modern "abstract" mathematics arose at around the time of Riemann's *Habilitation* lecture in 1854 on the foundations of geometry. Subsequent mathematicians such as Cantor and Dedekind developed the kind of "naïve" theory of sets and functions needed for the then new mathematics to flourish.

In 1901, Russell discovered his well-known paradox: should we admit, for each property  $\varphi$ , the existence of a set  $\{x \mid \varphi\}$  of all elements satisfying  $\varphi$ , then we are led to consider the troublesome set  $R := \{x \mid x \notin x\}$ . In response to this and other paradoxes arising from the naïve view of sets, Russell introduced his *type theory*. In Russell's type theory, each set is to be associated with a natural number, which should be thought of as indicating the "level" at which it has been constructed. So we would write,  $x : 3, y : 13, \dots$  in such a way that the relation  $a \in b$  is allowed to hold *only* for  $a : n$  and  $b : n + 1$ .<sup>3</sup> The natural numbers annotating the sets are called their *types*. This theory is usually taken to be the historical origin of type theory, although some of the ideas undoubtedly go back much further and modern type theory is quite different from Russell's theory. Ultimately, Russell's type theory failed to attract much of a following and the *de facto* foundational system eventually became, and still remains, Zermelo-Frankel set theory with the Axiom of Choice. Nonetheless, it is worth mentioning Russell's theory as the idea

<sup>3</sup> The notation  $x : 3$  is not Russell's, but is closer to notation we will employ later. Also, we are simplifying matters: Russell in fact introduced several theories of types.

of *annotating* mathematical structures is present throughout the history of type theory.

## 2.2. Propositional logic

Although mostly known for his work in topology, Brouwer advocated an approach to foundations starkly at odds with the set theoretic trend of the time. Brouwer himself was against the formal codification of mathematical principles, but his student Heyting formalized his ideas as what is called *intuitionistic logic*. We will briefly recall the simplest form of intuitionistic logic which is called *propositional (intuitionistic) logic*.

Assume given a set  $\mathcal{V}$ . We refer to elements of  $\mathcal{V}$  as *propositional variables*. Usually these are thought of as representing declarative statements such as, “ $2+2=4$ ”, “The normal distribution is symmetric about its mean”, and so forth. A *proposition* is then either a propositional variable or is obtained by applying the *logical connectives* to other propositions. Here the logical connectives are summarized in Figure 1 below, where  $A$  and  $B$  denote propositions and  $\perp$  is the constant false proposition (i.e., a nullary connective). We can define the negation “not  $A$ ” of

	<i>name of connective</i>	<i>read as</i>
$\perp$	falsum	“false”
$A \wedge B$	conjunction	“ $A$ and $B$ ”
$A \vee B$	disjunction	“ $A$ or $B$ ”
$A \rightarrow B$	conditional	“If $A$ , then $B$ ”

FIGURE 1. Logical connectives.

a proposition  $A$  as  $\neg A := A \rightarrow \perp$ . The set  $\mathcal{P}$  of propositions is the smallest set containing  $\mathcal{V}$  and closed under the operations  $\neg$ ,  $\wedge$ ,  $\vee$  and  $\rightarrow$ .<sup>4</sup> In what follows we will restrict our attention to the portion of propositional logic concerned only with  $\wedge$  and  $\rightarrow$ .

We now define a set  $\mathcal{C}$  of what are called *contexts*. By definition a context, written  $\Gamma, \Delta, \Theta, \dots$ , is a finite list  $(A_1, \dots, A_n)$  of propositions where we allow  $n = 0$  (the *empty context*) and we allow  $A_i = A_j$  for  $i \neq j$ .<sup>5</sup> Given a context  $\Gamma$  and a proposition  $A$  we will write  $\Gamma, A$  for the result of appending  $A$  to the list  $\Gamma$ .

Next, we introduce a relation  $\Gamma \vdash B$  between contexts  $\Gamma$  and propositions  $B$ . This relation is the subset of  $\mathcal{C} \times \mathcal{P}$  determined by the *inference rules* of logic. For example, there is an inference rule, called  *$\wedge$ -introduction*, which says that if  $\Gamma \vdash A$  and  $\Gamma \vdash B$ , then  $\Gamma \vdash A \wedge B$ . It is often inconvenient to describe inference rules in such a verbose way so we use the common shorthand for such a rule as follows:

$$\frac{\Gamma \vdash A \quad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \wedge \text{ introduction}$$

<sup>4</sup> To be precise, we should also require some convention regarding the use of parentheses. However, we omit such logical arcana and refer the reader to any standard text in logic for a detailed treatment.

<sup>5</sup> The reader will notice that we should allow several operations (*structural rules*), such as rearranging the order of the propositions occurring in the context, on contexts. These issues are important, but we have chosen to avoid them in the interest of simplifying our presentation.

The idea being that the relation below the line holds when the relations listed above the line hold. The name of the rule is indicated on the right. The additional rules governing  $\wedge$  and the rules for  $\rightarrow$  are summarized in Figure 2. We also require the following rule,

$$\frac{}{\Gamma, A \vdash A} \text{Axiom}$$

which allows us to infer that  $A$  holds when it appears in the context. One usually

$$\begin{array}{c} \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \wedge \text{ elimination (left)} \\ \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B} \wedge \text{ elimination (right)} \\ \frac{\Gamma, A \vdash B}{\Gamma \vdash A \rightarrow B} \rightarrow \text{ introduction} \\ \frac{\Gamma \vdash A \rightarrow B \quad \Gamma \vdash A}{\Gamma \vdash B} \rightarrow \text{ elimination} \end{array}$$

FIGURE 2. Remaining rules of inference for  $\wedge$  and  $\rightarrow$ .

works with these rules by stacking one on top of another to form a tree. For example, to prove that the relation  $(A \rightarrow (B \wedge C)) \vdash ((A \rightarrow B) \wedge (A \rightarrow C))$  holds we simply construct the tree illustrated in Figure 3 where, for notational convenience, we set

$$P := A \rightarrow (B \wedge C),$$

and where the leaves are instances of the Axiom rule.

$$\frac{\frac{\frac{\frac{\frac{\frac{P, A \vdash A \rightarrow (B \wedge C)}{P, A \vdash B \wedge C} \wedge E}{P, A \vdash B} \wedge E}{P \vdash A \rightarrow B} \rightarrow I}{P \vdash (A \rightarrow B) \wedge (A \rightarrow C)} \rightarrow E \quad \frac{\frac{\frac{\frac{\frac{\frac{P, A \vdash A \rightarrow (B \wedge C)}{P, A \vdash B \wedge C} \wedge E}{P, A \vdash C} \wedge E}{P \vdash A \rightarrow C} \rightarrow I}{P \vdash (A \rightarrow B) \wedge (A \rightarrow C)} \rightarrow E}}{P \vdash (A \rightarrow B) \wedge (A \rightarrow C)} \wedge I$$

FIGURE 3. Derivation tree of  $A \rightarrow (B \wedge C) \vdash (A \rightarrow B) \wedge (A \rightarrow C)$ .

Remarkably, the system formalized by Heyting can be interpreted using the open sets of a topological space  $X$  by letting  $\wedge$  be intersection,  $\vee$  be union,  $\perp$  be the empty set, and by defining  $\rightarrow$  as follows:

$$U \rightarrow V := \bigcup \{W \mid U \cap W \subseteq V\} = ((X - U) \cup V)^\circ$$

for open sets  $U$  and  $V$ . Consequently, it is quite easy to prove that the law of excluded middle  $\vdash P \vee \neg P$ , which holds in *classical* propositional logic, does not hold in intuitionistic propositional logic. E.g., taking as our ambient space  $\mathbb{R}$  and letting  $P$  be the open set  $(0, +\infty)$  we see that  $P \vee \neg P = (0, +\infty) \cup (-\infty, 0)$ .

### 2.3. Weakening and annotating: a topological example

Interestingly, in both topology and logic several important structures have arisen by virtue of annotating known structures with an additional mathematical layer. In some cases, this process has allowed for the original intended structure to be weakened in the sense that, e.g., equations governing the structure are now relaxed and replaced by a relation other than equality.<sup>6</sup> The most natural setting for this kind of machinery is higher-dimensional category theory, but we will here constrain ourselves to examples of this phenomenon coming from topology and logic.

Let  $X$  be a topological space and let  $x_0 \in X$  be a point of  $X$ . The *loop space of  $X$  based at  $x_0$* , which we write as  $\Omega(X)$  when  $x_0$  is understood, is the space of continuous maps  $f: I \rightarrow X$  such that  $f(0) = x_0 = f(1)$ , where  $I = [0, 1]$  is the unit interval. We define a *concatenation  $f \cdot g$  operation* on  $\Omega(X)$  by letting

$$(f \cdot g)(t) := \begin{cases} f(2t) & \text{for } t \in [0, \frac{1}{2}] \\ g(2t - 1) & \text{for } t \in [\frac{1}{2}, 1] \end{cases}$$

for  $f, g \in \Omega(X)$ . Similarly, we have an inverse operation  $f^{-1}$  which traverses  $f$  in reverse. With the structure just described  $\Omega(X)$  is *almost* a group with multiplication  $(f \cdot g)$ , inverses  $f^{-1}$  and unit element the constant loop  $r(x_0)$  given by  $r(x_0)(t) := x_0$  for  $t \in I$ . However, it is easy to see that this is not a group. E.g., the multiplication is not associative since  $(f \cdot (g \cdot h))$  will still be traversing  $f$  at  $\frac{3}{8}$ , whereas  $((f \cdot g) \cdot h)$  will have already moved on to  $g$  at this point. One solution to this problem is to observe that although  $\Omega(X)$  is not a group, it is a group *up to homotopy*.

Recall that if  $f$  and  $g$  are continuous maps  $X \rightarrow Y$  for  $X$  and  $Y$  topological spaces, a *homotopy*  $\varphi$  from  $f$  to  $g$  (written  $\varphi: f \simeq g$ ) consists of a continuous map  $\varphi: X \times [0, 1] \rightarrow Y$  such that  $\varphi(x, 0) = f(x)$  and  $\varphi(x, 1) = g(x)$ . Coming back to the loop space  $\Omega(X)$  we see that we have homotopies

$$\begin{aligned} \alpha_{f,g,h} &: ((f \cdot g) \cdot h) \simeq (f \cdot (g \cdot h)), \\ \iota_f &: (f \cdot f^{-1}) \simeq r(x_0), \end{aligned}$$

and so forth, for  $f, g, h \in \Omega(X)$ .

So, we have *weakened* the group laws and replaced the equations specifying what it is to be a group by homotopies which provide a corresponding *annotation*. We sometimes say that the homotopies are *witnesses* of the algebraic laws in question. One can weaken many algebraic structures in similar ways and this has in fact been done. From our perspective the importance of this particular example will soon become clear.

<sup>6</sup> The terminology of *weak* versus *strict* is used frequently in the literature on higher-dimensional category theory, but is rarely clarified. In practice, a structure being strict usually refers to the case where the defining conditions of the structure are axiomatized using the smallest possible relation or relations satisfying certain constraints. Often the constraint is simply that the relation should be an equivalence relation and strictness then refers to the case where the structure is axiomatized in terms of equations. By contrast, the weak case occurs when the structure is axiomatized using a larger relation satisfying the constraints.

## 2.4. Annotating: a logical example

Following the early use of the locution “type theory” by Russell, the next major development in type theory came with Church’s *simple type theory*. Consider for a moment a derivation in propositional logic such as the derivation from Figure 3 above. Simple type theory can be regarded as an annotated version of the  $\wedge, \rightarrow$  fragment of intuitionistic propositional logic described above, where the annotations capture the structure of the derivation trees. We will write our annotations as

$$a : A$$

where  $A$  can, for now, be thought of as a proposition and  $a$  is regarded as a kind of “code” for the derivation tree of  $A$  (assuming  $A$  is derivable). For example, we would then annotate the introduction rule for  $\wedge$  as follows:

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash (a, b) : A \wedge B}$$

Here we use a tuple notation  $(a, b)$  for the annotation to indicate that a derivation of  $A \wedge B$  can be obtained by simply collecting a derivation of  $A$  together with a derivation of  $B$ . This notation is also reminiscent of elements of a cartesian product of sets  $A \times B$  and, in fact, this is the standard notation for  $A \wedge B$  in simple type theory. As such, we henceforth write  $A \times B$ .

In simple type theory we do not speak of propositions and annotations. Instead when faced with  $a : A$  we say that  $A$  is a *type* and  $a$  is a *term of type A*. A context  $\Gamma$  is now a list  $(x_1 : A_1, \dots, x_n : A_n)$  where the  $x_i$  are variables. The rules of inference, aside from the introduction rule for  $\times$  given above, for  $\times$  and  $\rightarrow$  in simple type theory are summarized in Figure 4. In the introduction rule for  $\rightarrow$ , the variable  $x$  in  $\lambda_{x:A}b$  is bound. Intuitively,  $\lambda_{x:A}b$  is an algorithm for transforming derivations of  $A$  into derivations of  $B$  using  $b$ . It is sometimes convenient to think of  $A \rightarrow B$  as being like the set of all functions from a set  $A$  to a set  $B$ . In this case,  $\lambda_{x:A}b$  is the function given by  $x \mapsto b(x)$ .

$$\begin{array}{ccc} \frac{\Gamma \vdash p : A \times B}{\Gamma \vdash \pi_1(p) : A} \times E \text{ (left)} & & \frac{\Gamma \vdash A \times B}{\Gamma \vdash \pi_2(p) : B} \times E \text{ (right)} \\ \frac{\Gamma, x : A \vdash b : B}{\Gamma \vdash \lambda_{x:A}b : A \rightarrow B} \rightarrow I & & \frac{\Gamma \vdash f : A \rightarrow B \quad \Gamma \vdash a : A}{\Gamma \vdash f(a) : B} \rightarrow E \end{array}$$

FIGURE 4. Rules of inference for  $\times$  and  $\rightarrow$  in simple type theory.

So we see that simple type theory can be viewed in (at least) two ways. In the first, we think of the terms as codes for derivation trees in propositional logic. This interpretation of simple type theory is sometimes called *propositions as types* or the *Curry-Howard correspondence*. In the second, we think of types as sets and terms as elements. There is actually a third way that is worth knowing about, even if we do not make use of it here, which is to think of types as objects in a cartesian closed category and terms as generalized elements. (Conversely, the morphisms of a cartesian closed category can be regarded as equivalence classes of proofs in a formal system and we refer the reader to [14] for a detailed exposition of these

<i>type former</i>	<i>name</i>	<i>logical</i>	<i>set theoretic</i>
$A \times B$	simple product	$A \wedge B$	cartesian product
$A \rightarrow B$	exponential	$A \rightarrow B$	function space $B^A$

FIGURE 5. Products and exponentials.

matters.) The first two of these interpretations are summarized in Figure 5. In addition to being able to construct terms of given types  $a : A$ , we can also reason about equality of terms and types in type theory. This is taken as two further relations in addition to the basic relation  $\Gamma \vdash a : A$ . Namely, we write  $\Gamma \vdash A = B$  to indicate equality of types and  $\Gamma \vdash a = a' : A$  equality of terms. Simple type theory then incorporates what are called *conversion* or *computation* rules such as

$$\frac{\Gamma \vdash a : A \quad \Gamma \vdash b : B}{\Gamma \vdash \pi_1(a, b) = a : A}$$

which describe the behavior of equality (which is of course also required to be an equivalence relation). The relation  $\Gamma \vdash a = a' : A$  between  $a$  and  $a'$  is sometimes referred to as *definitional* (or *intensional*) equality, as opposed to the *propositional* (or *extensional*) equality which we will now describe.

## 2.5. Dependent type theory

The form of type theory with which homotopy type theory is concerned is sometimes called *dependent type theory* and it is due to Martin-Löf [19, 17, 18], who built on related work by Curry, Howard, Tait, Lawvere, de Bruijn, Scott and others. From the logical point of view, dependent type theory extends the analogy between simple type theory and propositional logic to logic with quantifiers ( $\forall$  and  $\exists$ ). From the point of view of foundations and set theory, dependent type theory can be viewed as a theory in which indexed families of sets are manipulated.

Now, when we are given, say,  $x : B \vdash E$  we think of this as indicating that  $E$  is  $B$ -indexed or, in more geometric language, that  $E$  is fibered over  $B$ . In order to emphasize this intuition we will often write  $x : B \vdash E(x)$  which is reminiscent of the indexed set notation  $(E_x)_{x \in B}$ . A term  $x : B \vdash s(x) : E(x)$  would then be thought of as a  $B$ -indexed family of elements  $s_x \in E_x$ . From a category theoretic perspective it is common to think of this as describing a map  $E \rightarrow B$  (cf. [23]). Instead of just  $\times$  and  $\rightarrow$ , we now have indexed versions of these, written as  $\sum$  and  $\prod$  respectively, and we have rules governing when they can be introduced into a derivation. For example:

$$\frac{\Gamma, x : B \vdash E(x)}{\Gamma \vdash \sum_{x:B} E(x)}$$

The logical and set theoretic readings of these are summarized in Figure 6. We also consider notions of equality for types and terms.

In addition to  $\prod$  and  $\sum$ , Martin-Löf introduced what is known as the *identity type*. The rule for forming an identity type is as follows:

$$\frac{\Gamma \vdash A}{\Gamma, x : A, y : A \vdash \text{Id}_A(x, y)}$$

<i>type former</i>	<i>name</i>	<i>logical</i>	<i>set theoretic</i>
$\prod_{x:B} E(x)$	dependent product	$(\forall x \in B)E(x)$	$\prod_{x \in B} E_x$
$\sum_{x:B} E(x)$	dependent sum	$(\exists x \in B)E(x)$	$\sum_{x \in B} E_x$

where indexed products and sums of sets are given by:

$$\prod_{x \in B} E_x := \{f : B \rightarrow \prod_{x \in B} E_x \mid f(b) \in E_b\}$$

$$\sum_{x \in B} E_x := \{(x, e) \mid x \in B \text{ and } e \in E_x\}$$

FIGURE 6. Dependent products and sums.

The identity type captures a certain notion of equality between terms and it is often suggested that one should think of a term  $p : \text{Id}_A(a, b)$  as corresponding to a proof that  $a$  and  $b$  are equal. When such a  $p$  exists, we sometimes say that  $a$  and  $b$  are *propositionally equal*.

In the set theoretic interpretation,

$$\text{Id}_A(a, b) := \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise,} \end{cases}$$

and therefore propositional equality in this case coincides with definitional equality  $a = b : A$ . Nonetheless, it does not follow from the rules of type theory that these two notions of equality must be the same.<sup>7</sup> Indeed, this interpretation unnecessarily destroys the interesting structure present in the identity type.

## 2.6. Groupoids in topology

Earlier we saw that to each space  $X$  and point  $x_0$  we could associate the loop space  $\Omega(X)$  and that  $\Omega(X)$  is a kind of group, up to homotopy. It turns out that there is a good deal more structure lurking in this example. To see this, define a groupoid  $\Pi_1(X)$  called the *fundamental groupoid of  $X$*  as follows. Recall that a groupoid is a category in which every arrow is invertible. E.g., if  $G$  is a groupoid and  $x$  is an object of  $G$ , then the set  $\text{hom}_G(x, x)$  is a group. In our case, the objects of  $\Pi_1(X)$  are points of the space  $X$ . Given points  $x$  and  $y$  of  $X$ , an *arrow* from  $x$  to  $y$  is then defined to be an equivalence class  $[f]$  of paths  $f : I \rightarrow X$  with  $f(0) = x$  and  $f(1) = y$ . Here the equivalence relation is homotopy relative to endpoints. By considerations from Section 2.3 we see that this is indeed a groupoid. Moreover, for a point  $x$  of  $X$  we recover the Poincaré fundamental group  $\pi_1(X, x)$  as  $\text{hom}_{\Pi_1(X)}(x, x)$ .

In fact, there is no need to quotient at this stage. Instead we can follow Grothendieck and consider the entire graded set  $(X_n)_{n \geq 0}$  with  $X_0 := X$ ,  $X_1$  the

<sup>7</sup> There are many ways to see this. E.g., type checking in the form of type theory in which these notions of equality have been identified (i.e., the theory of [18]) is undecidable, whereas, by Martin-Löf's normalization theorem, it is decidable in the theory where they have not been identified.

paths in  $X$ ,  $X_2$  the homotopies of paths relative to endpoints,  $X_3$  the homotopies of homotopies of paths relative to endpoints, and so forth. The resulting structure is not a groupoid, but an  $\infty$ -groupoid: *the fundamental  $\infty$ -groupoid  $\Pi_\infty(X)$  of  $X$* . Moreover, Grothendieck noted that, when suitably defined,  $\Pi_\infty(X)$  should capture all of the homotopy theoretic content of  $X$ . This is something which is certainly *not* true of the usual  $\Pi_1(X)$ . Instead,  $\Pi_1(X)$  is only able to completely capture the  $X$  which are *homotopy 1-types*.

## 2.7. Groupoids in logic

The birth of homotopy type theory can be traced back to ideas of Hofmann and Streicher [11] (see also [24]). Hofmann and Streicher associated to any type  $A$  in dependent type theory a groupoid, which we now denote by  $\Pi_1(A)$  (Hofmann and Streicher did not use this notation), by letting the objects be terms of type  $A$  and the arrows be equivalence classes  $[f]$  where

$$\vdash f : \text{Id}_A(a, b)$$

and the equivalence relation  $\simeq$  is given by setting  $f \simeq g$  provided that  $f : \text{Id}_A(a, b)$  and  $g : \text{Id}_A(a, b)$ , for some  $a : A$  and  $b : B$ , and there exists some

$$h : \text{Id}_{\text{Id}_A(a,b)}(f, g).$$

Moreover, Hofmann and Streicher constructed a model of dependent type theory in the category of groupoids and observed that  $\Pi_1(A)$  does not seem to completely capture the content of the type  $A$ .

## 2.8. Early results in homotopy type theory

In 2001, Moerdijk conjectured, during the question session at the end of a talk he delivered at the Mittag-Leffler Institute, that there might be a connection between Quillen model categories, from homotopy theory, and type theory. Later, Awodey and Warren [5, 30], and Voevodsky [27, 28] independently realized how to interpret type theory using ideas from homotopy theory (in the former case, following Moerdijk's suggestion to make use of Quillen's machinery, and in the latter case using simplicial sets). We refer to our article [21] for further discussion of many of these topics, and especially regarding groupoids and homotopy  $n$ -types.

The basic idea of the homotopy theoretic interpretation of type theory, which is one of the ingredients making homotopy type theory possible, is to regard types neither as propositions nor as sets, but as spaces. In the dependent setting this means that a dependent type  $x : B \vdash E(x)$  would be interpreted as a fibration over  $B$ . A fibration is a continuous map which satisfies a certain homotopy lifting property. Identity types can then be interpreted using path spaces  $A^I$ . Interestingly, the features required to interpret type theory are sufficiently general that they can be validated in a wide range of settings where homotopy theory makes sense. In particular, Quillen introduced the notion of *model category* as an abstraction of the structure which makes the homotopy theory of spaces and simplicial sets possible. The result for type theory is then as follows:

**Theorem 2.1** (Awodey and Warren [5, 30]). *In any well-behaved Quillen model category there is a model of type theory.*

This perspective serves to clarify some features of dependent type theory which had previously been mysterious. Moreover, this opens the door to being able to manipulate spaces directly, without first having to develop point-set topology or even define the real numbers. That is, homotopy type theory interprets type theory from a homotopical perspective.

Voevodsky instead investigated a special model (sometimes called the *univalent model*) which he discovered in the category of simplicial sets:

**Theorem 2.2** (Voevodsky [28]). *Assuming the existence of Grothendieck universes (sufficiently large cardinals), there is a model of type theory in the category of simplicial sets in which types are interpreted as Kan complexes and Kan fibrations.*

Kan complexes are one model of the notion of  $\infty$ -groupoid and so this result is in line with the intuition of types as corresponding to spaces and  $\infty$ -groupoids. Indeed, from the point of view of homotopy theory, Kan complexes correspond precisely to spaces (in the technical sense that there is a Quillen equivalence between the category of spaces, with its usual model structure, and the category of simplicial sets with the Kan complex model structure). The work described above, together with theorems of Gambino and Garner, van den Berg and Garner, Lumsdaine, Moerdijk and Palmgren, Streicher, as well as further results from [27, 28] and [30] constitute the earliest results in homotopy type theory.

### 3. Homotopy type theory and foundations

With some of the relevant background covered, we are now in a position to describe Voevodsky's univalence axiom and some of the other ideas underlying his *univalent foundations* program.

#### 3.1. The univalence axiom

For spaces, a map  $f : X \rightarrow Y$  is a *weak equivalence* when it induces isomorphisms on the homotopy groups. Voevodsky realized that this notion could be captured type theoretically. In order to describe this approach let us first develop some notation and basic definitions. First, we will often omit explicit mention of contexts  $\Gamma$  in what follows in order to avoid notational clutter. Next, note that for types  $A$  and  $B$  which are not dependent (meaning they are not parameterized by one another) we can form the simple type  $A \rightarrow B$  as  $\prod_{x:A} B$  (cf. the set theoretic interpretation). Now, in homotopy type theory,  $A \rightarrow B$  is just the space of continuous maps from  $A$  to  $B$ .

**Definition 3.1.** Given  $f : A \rightarrow B$  and  $b : B$  we denote by  $f^{-1}(b)$  the type defined by

$$f^{-1}(b) := \sum_{a:A} \text{Id}_B(f(a), b).$$

This is sometimes called the *homotopy fiber of  $f$  over  $b$* .

**Definition 3.2.** Given types  $A$  and  $B$ , a term  $f: A \rightarrow B$  is a *weak equivalence* when there exists a term of the type

$$(3.1) \quad \prod_{b:B} \sum_{c:f^{-1}(b)} \prod_{a:f^{-1}(b)} \text{Id}_{f^{-1}(b)}(c, a).$$

It is perhaps useful to consider the logical analogue of (3.1):

$$(\forall b \in B)(\exists c \in f^{-1}(b))(\forall a \in f^{-1}(b))c = a$$

which is the same as

$$(\forall b \in B)(\exists c \in f^{-1}(b))(\forall a \in A)b = f(a) \rightarrow c = a.$$

This can be decomposed into the following observations:

- (1)  $f$  is *surjective*:  $(\forall b \in B)(\exists c \in A)f(c) = b$ .
- (2)  $f$  is *injective*:  $(\forall c \in A)(\forall a \in A)f(c) = f(a) \rightarrow c = a$ .

That is, being a weak equivalence is the homotopy theoretic version of being a bijective function.

**Definition 3.3.** Given types  $A$  and  $B$ , denote by  $A \simeq B$  the *type of all weak equivalences from  $A$  to  $B$* . That is,

$$A \simeq B := \sum_{f:A \rightarrow B} \prod_{b:B} \sum_{c:f^{-1}(b)} \prod_{a:f^{-1}(b)} \text{Id}_{f^{-1}(b)}(c, a).$$

Now, it is common in type theory to consider a type  $U$  which behaves as a kind of universe of “small types”. From the point of view of homotopy theory this corresponds to the assumption of a Grothendieck universe of “small spaces”. Voevodsky observed that, by virtue of the rules governing identity types, there exists a map  $\iota_{A,B}$  indicated as follows:

$$\text{Id}_U(A, B) \rightarrow (A \simeq B)$$

for small types  $A$  and  $B$ . Voevodsky then proved the following:

**Theorem 3.4.** (Voevodsky [28, 13]) *In the simplicial set model of type theory, the map  $\iota_{A,B}$  is a weak equivalence for all  $A$  and  $B$ .*

In the simplicial set model the identity type  $\text{Id}_U(A, B)$  is interpreted as the space of all paths in the space  $U$  from  $A$  to  $B$ . So this result characterizes such paths as corresponding to weak equivalences  $A \rightarrow B$ . Now, all of the parts of this theorem can be understood type theoretically and so Voevodsky turned this result around by adding it as an axiom to type theory:

**Axiom 3.5.** (Univalence Axiom, Voevodsky [28]) Given  $U$  the universal type, there exists a term  $v$  of type

$$\text{Id}_U(A, B) \simeq (A \simeq B)$$

such that the underlying term  $\text{Id}_U(A, B) \rightarrow (A \simeq B)$  of  $v$  is  $\iota_{A,B}$ .

We now consider consequences of the Univalence Axiom.

### 3.2. Univalent foundations

We will now describe what Voevodsky has called *univalent foundations*. To be clear, there is no implicit foundational claim made by homotopy type theory and some of the researchers in this area are satisfied with standard set theoretic foundations using Zermelo-Frankel set theory with the axiom of choice (ZFC) (and perhaps additional principles such as Grothendieck universes). So there is a sense in which homotopy type theory is entirely agnostic regarding matters of foundations. At the same time, Voevodsky has advocated for what he calls univalent foundations. Roughly, univalent foundations is simply the idea of taking homotopy type theory as a foundation for mathematics in place of alternatives such as ZFC. We will now describe some of the ideas which make this proposal reasonable.

We say that a type  $A$  is *contractible* when there exists a term of the following type:

$$\sum_{c:A} \prod_{a:A} \text{Id}_A(c, a).$$

Written logically this says  $(\exists c \in A)(\forall a \in A)c = a$ . I.e., it says that  $A$  is a singleton set. (Note that a map  $f: A \rightarrow B$  is a weak equivalence when all of its homotopy fibers are contractible.) From the point of view of homotopy theory though it merely states that the type  $A$  can be continuously deformed to a one point space. Following Voevodsky [28], let us say that a contractible type  $A$  has *h-level* 0. In general, we say that a type  $A$  has *h-level*  $(n + 1)$  when the type  $\text{Id}_A(a, b)$  has h-level  $n$  for any terms  $a$  and  $b$  of type  $A$ .

So, for example,  $A$  has h-level 1 when  $\text{Id}_A(a, b)$  is contractible for all terms  $a$  and  $b$ . This is true when  $A$  is the empty type (empty space)  $0$  and it is also easy to see that this is true when  $A$  is itself contractible. In fact, these are the only two possibilities. That is, the spaces of h-level 1 look like the boolean values 0 and 1 from the homotopical perspective. Moving up in dimension, we see that the  $A$  which have h-level 2 correspond to sets (discrete spaces). In general, the types of h-level  $(n + 2)$  correspond to homotopy  $n$ -types.

Now we are in a position to relate these ideas to foundational matters. The crucial point is that the sets sit among all of the types: we have carved them out as the types of h-level 2. The next important point here is that there are many types with h-level greater than 2. As such, if we adopt homotopy type theory as a foundational system, then our foundational system provides us access to more general spaces than just the discrete ones *at the outset*. This is in contrast with the situation in set theoretic foundations where one must build up all of the machinery of point set topology before having access to more general spaces. The final point worth making in this connection is that we have so far made no further assumptions regarding the properties of the types of h-level 2, but it is consistent that they obey the usual properties of sets in ZFC. In particular, the sets in Voevodsky's simplicial set model of type theory are indeed the classical sets of ZFC. Should we choose to adopt this perspective we should more properly see univalent foundations as being consonant with classical set theoretic foundations.<sup>8</sup> (We refer the reader to [22] for more regarding the properties of sets in a general model of homotopy type theory.)

<sup>8</sup> It is worth remarking that the authors prefer to remain agnostic about foundational matters such as these. We are merely clarifying some of the open possibilities.

### 3.3. Higher-inductive types

In algebraic topology it is often convenient to know that the spaces with which one is concerned have been constructed in a certain way. Consider for example CW-complexes. A *CW-complex* is a space which is built up inductively by “gluing cells”. Specifically, a space  $X$  is a CW-complex if there exists a sequence of spaces  $X_n$ , for  $0 \leq n$ , and a sequence of families of continuous maps  $f_i^n: S^{n-1} \rightarrow X_n$  called the *attaching maps* such that  $X = \bigcup_{i=0}^{\infty} X_i$ ,  $X_0$  is a discrete space, and either  $X_{n+1} = X_n$  or  $X_{n+1}$  is the pushout of the map  $\coprod_i S^n \rightarrow X_n$  induced by the attaching maps along the map  $\coprod_i S^n \rightarrow \coprod_i D^{n+1}$ . Working with CW-complexes as opposed to general spaces has the advantage that they have been constructed iteratively in a simple combinatorial fashion. Indeed, it is common in algebraic topology to take *space* to simply mean *simplicial set*, where simplicial sets can be understood as *purely* combinatorial descriptions of spaces (in terms of points, intervals, triangles and their higher-dimensional generalizations).

Therefore, in order to be able to manipulate familiar spaces in homotopy type theory one approach is to find a way to give a combinatorial description of spaces in type theory. This is exactly what is accomplished by higher-inductive types. In particular, using higher-inductive types it is possible to carry out all of the familiar constructions of and on spaces that one is familiar with from algebraic topology. Although we will not give a detailed description of higher-inductive types here, the idea is very simple. The combinatorial structure required to represent spaces as CW-complexes are spheres  $S^n$  and discs  $D^{n+1}$ , and the combinatorial structure required to represent spaces as simplicial sets are points, intervals, triangles, tetrahedra, *et cetera*. To represent spaces in type theory we use instead the kinds of combinatorial structure provided by identity types: paths, homotopies between paths, and so forth. The magic behind this is that the higher-inductive types are defined in such a way that they possess, by virtue of their type theoretic specifications (in terms of inference rules), universal properties which state that they are the smallest spaces possessing the required non-trivial paths, homotopies, and higher homotopies. We refer to [12] for a more detailed introduction to higher-inductive types.

## 4. Conclusion

In conclusion, we would like to make several remarks regarding the connection between homotopy type theory and computer proof assistants. In connection with his work in homotopy type theory and univalent foundations, Voevodsky has advocated for the formalization of mathematics in computer proof assistants, as well as for greater interaction between the developers of proof assistants and mathematicians. Voevodsky has himself written code documenting topics ranging from the homotopy theory, to the formalization of abstract algebra (see [29] for a survey of his library). In essence, there are two good reasons for doing so. First, as more mathematicians become engaged with the developers of computer proof assistants it is inevitable that the technology will adapt to better suit the needs of mathematicians. Second, it is likely inevitable that computer proof assistants will one day be as common as such tools as  $\text{\TeX}$  now are and we will reach this point sooner through greater engagement by the mathematical community. For

some mathematicians, these tools will already be of use. In the case of reasoning involving homotopy theoretic or higher-dimensional algebraic structures, which sometimes have large amounts of “book-keeping” involving complex combinatorial data, being able to make use of the computer to ensure that calculation errors have not been made is potentially quite useful. It is with these and like considerations in mind that Voevodsky and others have been making use of the proof assistants already to formally verify mathematical proofs in homotopy theory, algebra and other areas. Examples include the recent Coq proof of the Feit-Thompson odd order theorem [10], Voevodsky’s own Coq library, and [20].

Part of the reason that homotopy type theory is closely related to work in proof assistants is that Martin-Löf type theory provides the theoretical basis of both the Agda and Coq proof assistants. As such, it is easy to work in homotopy type theory in these systems. Examples of the kinds of results which have been formalized in this setting include [1, 2, 15] as well as further results which are mentioned in the textbook [12]. We encourage the interested reader to consult these and the other references mentioned throughout this paper in order to learn more about this exciting area.

*Acknowledgements.* The authors are grateful to the Editors of *La Gazette des mathématiciens* for their interest in this work, and their encouragement to write this contribution (in particular thanks to the former Chief Editors San Vũ Ngọc and Bernard Helffer, and to current Chief Editor Boris Admaczewski). We thank Steve Awodey for useful discussions on homotopy type theory. We also thank the referees for their helpful comments. Finally, we would like to thank Vladimir Voevodsky for many discussions on the topics of this paper, and for sharing with us his understanding and vision of the rapidly developing fields of homotopy type theory and univalent foundations.

## 5. References

- [1] B. Ahrens, C. Kapulkin, and M. Shulman, *Univalent categories and the Rezk completion*, to appear in *Math. Struct. in Comp. Science*, preprint on the arXiv as arXiv:1303.0584, 2014.
- [2] J. Avigad, K. Kapulkin, and P. L. Lumsdaine, *Homotopy limits in Coq*, preprint on the arXiv as arXiv:1304.0680, 2013.
- [3] S. Awodey, *Type theory and homotopy*, Epistemology versus Ontology: Essays on the Philosophy and Foundations of Mathematics in Honour of Per Martin-Löf (P. Dybjer, S. Lindström, E. Palmgren, and B.G. Sundholm, eds.), Logic, Epistemology, and the Unity of Science, vol. 27, Springer, Dordrecht, 2012, pp. 183–201.
- [4] S. Awodey, Á. Pelayo, and M. A. Warren, *Voevodsky’s univalence axiom in homotopy type theory*, Notices of the American Mathematical Society **60** (2013), no. 08, 1164–1167.
- [5] S. Awodey and M. A. Warren, *Homotopy theoretic models of identity types*, Mathematical Proceedings of the Cambridge Philosophical Society **146** (2009), no. 1, 45–55.
- [6] B. Berg van den Berg and R. Garner, *Types are weak  $\omega$ -groupoids*, Proceedings of the London Mathematical Society. Third Series **102** (2011), no. 2, 370–394.
- [7] N. Gambino and R. Garner, *The identity type weak factorisation system*, Theoretical Computer Science **409** (2008), no. 1, 94–109.
- [8] J. Gillibert and C. Retoré, *Category theory, logic and formal linguistics: some connections, old and new*, Journal of Applied Logic **12** (2014), no. 1, 1–13.
- [9] J.-Y. Girard, *Proofs and types*, 2003 web reprint ed., Cambridge University Press, Cambridge, 2003, translated and with appendices by P. Taylor and Y. Lafont.
- [10] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O’Connor, Sidi Ould Biha, Ioana Pasca,

- Laurence Rideau, Alexey Solovyeu, Enrico Tassi, and Laurent Théry, *A Machine-Checked Proof of the Odd Order Theorem*, ITP 2013, 4th Conference on Interactive Theorem Proving (Rennes, France) (Sandrine Blazy, Christine Paulin, and David Pichardie, eds.), LNCS, vol. 7998, Springer, 2013, pp. 163–179 (English).
- [11] M. Hofmann and T. Streicher, *The groupoid interpretation of type theory*, Twenty-five years of constructive type theory (Venice, 1995), Oxford Logic Guides, vol. 36, Oxford Univ. Press, New York, 1998, pp. 83–111.
- [12] The Univalent Foundations Program Institute for Advanced Study 2013, *Homotopy type theory: Univalent foundations of mathematics*, The Univalent Foundations Program, Princeton, NJ; Institute for Advanced Study (IAS), Princeton, NJ, 2013, <http://homotopytypetheory.org/book>.
- [13] C. Kapulkin, P. L. Lumsdaine, and V. Voevodsky, *Univalence in simplicial sets*, in preparation, on the arXiv as arXiv:1203.2553, 2012.
- [14] J. Lambek and P. J. Scott, *Introduction to higher-order categorical logic*, Cambridge Studies in Advanced Mathematics, no. 7, Cambridge University Press, Cambridge, 1988.
- [15] D. Licata and M. Shulman, *Calculating the fundamental group of the circle in homotopy type theory*, preprint on the arXiv as arXiv:1301.3443, 2013.
- [16] P. L. Lumsdaine, *Weak  $\omega$ -categories from intensional type theory*, Logical Methods in Computer Science **6** (2010), no. 3, 3:24–19.
- [17] P. Martin-Löf, *An intuitionistic theory of types: predicative part*, Proceedings of the Logic Colloquium (Bristol, July, 1973) (H. E. Rose and J. C. Shepherdson, eds.), Studies in Logic and the Foundations of Mathematics, vol. 80, North-Holland, Amsterdam, 1975, pp. 73–118.
- [18] ———, *Intuitionistic type theory*, Studies in Proof Theory. Lecture Notes, vol. 1, Bibliopolis, Naples, 1984.
- [19] ———, *An intuitionistic theory of types*, Twenty-five years of constructive type theory (Venice, 1995), Oxford Logic Guides, vol. 36, Oxford Univ. Press, New York, 1998, originally a 1972 preprint from the Department of Mathematics at the University of Stockholm, pp. 127–172.
- [20] Á. Pelayo, V. Voevodsky, and M. A. Warren, *A univalent formalization of the  $p$ -adic numbers*, to appear in *Math. Struct. in Comp. Science*.
- [21] Á. Pelayo and M. A. Warren, *Homotopy type theory and Voevodsky’s univalent foundations*, Bull. Amer. Math. Soc. **51** (2014), no. 4, 597–648.
- [22] E. Rijke and B. Spitters, *Sets in homotopy type theory*, to appear in *Math. Struct. in Comp. Science*, preprint on the arXiv as arXiv:1305.3835, 2014.
- [23] R. A. G. Seely, *Locally cartesian closed categories and type theory*, Math. Proc. Cambridge Philos. Soc. **95** (1984), no. 1, 33–48.
- [24] T. Streicher, *Investigations into intensional type theory*, Habilitationsschrift, Ludwig-Maximilians-Universität München, 1993.
- [25] ———, *Identity types and weak omega-groupoids*, slides from a talk at *Identity Types – Topological and Categorical Structure*, Uppsala University, November 2006.
- [26] ———, *A model of type theory in simplicial sets: a brief introduction to Voevodsky’s homotopy type theory*, Journal of Applied Logic **12** (2014), no. 1, 45–49.
- [27] V. Voevodsky, *A very short note on the homotopy  $\lambda$ -calculus*, unpublished note, available at [www.math.ias.edu/~vladimir](http://www.math.ias.edu/~vladimir), 2006.
- [28] ———, *Notes on type systems*, unpublished notes, available at [www.math.ias.edu/~vladimir](http://www.math.ias.edu/~vladimir), 2009.
- [29] ———, *Experimental library of univalent formalization of mathematics*, to appear in *Math. Struct. Comp. Sci.*, preprint available on the arXiv as 1401.0053, 2014.
- [30] M. A. Warren, *Homotopy Theoretic Aspects of Constructive Type Theory*, Ph.D. thesis, Carnegie Mellon University, 2008.

# CARNET

---

## Pierre Liardet

(1943-2014)

Jean-Paul Allouche, Hervé Daudé

---

Pierre Liardet nous a quittés. Il avait bien caché ou minimisé le fait qu'il était malade. Quelques jours avant sa disparition il tenait encore avec la passion mais aussi la modestie et la précision qu'on lui connaît, à expliquer des mathématiques, passant de questions d'équirépartition et d'anciens travaux de Jean Coquet, aux résultats récents de Green et Tao, comme si une chambre d'hôpital n'était qu'un des lieux possibles de séminaire. Il alla même jusqu'à rédiger des notes manuscrites qu'il fit scanner et envoyer par courriel.

La curiosité scientifique est loin d'être un défaut, surtout lorsqu'elle s'accorde avec la précision et la rigueur du raisonnement. Pierre a marqué nombre des chercheurs qui l'ont côtoyé, des plus aguerris aux plus néophytes. Par sa convivialité et sa disponibilité il savait instaurer un climat propice aux échanges, aux questionnements et aux avancées scientifiques. C'est ainsi qu'entre 1990 et 2010, au sein du Laboratoire d'Analyse Topologie et Probabilités, il a dirigé une petite équipe de recherche marseillaise. Le séminaire de l'équipe DSA (Dynamique Stochastique et Algorithmique) du jeudi matin a été fréquenté par de nombreux chercheurs que Pierre accueillait souvent pour plusieurs jours, et assez souvent chez lui à Saint-Cannat. Profitant d'une ambiance familiale et décontractée, qui devait beaucoup à Josy son épouse, l'activité scientifique était partagée dans un environnement provençal qu'il aimait faire découvrir. Lors des longues promenades sur la Sainte Victoire ou dans le Luberon, Pierre discutait avec passion et précision des sujets que ses invités affectionnaient ; sa grande culture mathématique et son sens de l'écoute faisaient souvent oublier les forts pourcentages des sentiers arpentés. À la fin du séminaire, Pierre savait aussi l'importance des pauses déjeuners, il connaissait très bien les petits restaurants de Château-Gombert que beaucoup de ses invités ont pu apprécier.

Maître-assistant (comme on disait alors pour ceux qu'on appelle maintenant les maîtres de conférence) puis Professeur à l'université de Provence, Pierre avait effectué sa thèse sous la direction de Gérard Rauzy. Avant de s'intéresser à l'étude des systèmes dynamiques et aux applications de la théorie des nombres, il avait publié une preuve remarquable d'une conjecture de S. Lang. Titulaire d'un baccalauréat E, Pierre avait une formation mathématique et technique qui lui permettait d'effacer les barrières entre mathématiques dites pures et mathématiques dites appliquées.

Inclassable et toujours porté par la curiosité, il s'est tourné vers l'application de la théorie ergodique à la théorie des nombres et en particulier à l'étude des systèmes de numération : nous n'avons pas la place de détailler dans ce bref article ses nombreuses contributions dans ces domaines. Inclassable ? on pourrait aussi citer ses collaborations avec le Laboratoire d'Informatique de l'université François Rabelais à Tours, équipe *Handicap et Nouvelles Technologies* et avec l'équipe TAO du LRI à Orsay sur les algorithmes évolutionnaires. Inclassable ? il n'y a pas beaucoup de chercheurs qui ont des articles, des communications ou même des cours aussi bien en mathématiques (*Acta Arithmetica*, *Israel Journal of Mathematics*, *Compositio Mathematica*, *Journal d'Analyse*, *Mémoires de la Société Mathématique de France*, *Ergodic Theory and Dynamical Systems*, *Journal of Number Theory*, *Annales de l'Institut Fourier*, etc.) qu'en informatique (*Proceedings Eurocode'92*, *Lecture Notes in Computer Science*, *Annals of Telecommunications*, *Designs, Codes and Cryptography*, etc.), qu'en physique (un cours sur Systèmes Dynamiques Discrets et Quasi-Cristaux aux Houches en 1994), qu'en médecine (Thèse de Médecine, Journée de Posturologie). En médecine ? Pas si nombreux sont les collègues mathématiciens qui savent que Pierre a passé une thèse de médecine en 1985 sur la médecine d'urgence. Il expliquait que dans le cas d'une intervention urgente on n'avait pas le temps de faire tous les examens nécessaires sans mettre la vie du patient en danger. Il fallait donc mettre au point (ce qu'il fit) un protocole de conduites à tenir prenant en compte les probabilités des différentes situations rencontrées, tout en sachant que ce protocole allait, dans des cas peu fréquents, être dangereux voire létal, mais qu'il sauverait des vies dans la grande majorité des cas (la ressource rare ici est *le temps* dont chaque minute compte). Puis, parallèlement à ses activités de recherche, d'enseignement et d'administration à l'université, Pierre a exercé comme médecin urgentiste, consacrant en particulier une journée par semaine au rôle de médecin régulateur (celui qui prend les appels téléphoniques et qui doit décider quel type de service appeler : médecine de ville, SAMU, pompiers, etc.).

Cette force de travail peu commune se voyait aussi dans les directions de thèse. C'est ainsi en encadrant simultanément plusieurs thèses au milieu des années 90, que Pierre a exploré certains liens étroits entre mathématiques et informatique, passant en particulier de domaines standards d'application de la théorie des nombres, comme le codage et la cryptographie, à des champs moins connus comme celui des algorithmes génétiques. Il aimait aborder des sujets nouveaux où il apprenait très vite les bases, repérait des problèmes intéressants et y entraînait un ou des thésards dans une sorte de courte échelle mutuelle. On peut remarquer qu'il y a dans la quinzaine de thèses qu'il a dirigées une parité quasi-parfaite entre doctorantes et doctorants.

Pierre prenait soin d'apprendre, d'interroger, de se documenter, de collaborer, de publier et de valoriser. Organisateur de nombreux colloques et écoles, il aimait prendre part à la dynamique de la recherche mathématique et transmettre ses connaissances. Il était membre des comités de rédaction du *Journal de Théorie des Nombres de Bordeaux* et de la revue *Uniform Distribution Theory*. Point d'orgue de cet engagement pour la communauté mathématique, Pierre avait organisé à Marseille, en juillet 2005, les XXIV<sup>e</sup> Journées Arithmétiques. Pour l'organisation

de cet événement, Pierre avait su fédérer les énergies des membres de son équipe et de sa famille. Certains se souviendront longtemps et avec émotion des nuits courtes et de l'activité intense, tant administrative que scientifique, qui régnait dans le couloir SDA du CMI pendant les quinze premiers jours de juillet 2005. Grâce à Pierre, 250 participants ont ainsi pu profiter pleinement des exposés et des conférences de très haut niveau international. Comme on peut le constater sur la photo de ces journées, Pierre était heureux au sein de la communauté scientifique. Il prenait soin d'associer ses proches collaborateurs, ses invités et aussi sa famille à des projets innovants, comme la recherche de générateurs aléatoires ou l'amélioration des performances des cartes à puce. Pierre voyageait aussi beaucoup et avait des collaborateurs en Autriche, aux Pays-Bas, au Japon, en Chine, en Roumanie, en Hongrie, en Slovaquie, aux États-Unis, au Canada et en Pologne. Il est parti loin de nous le vendredi 29 août 2014.

Comme à toutes celles et tous ceux qui ont pu apprécier tes qualités scientifiques et humaines, Pierre, tu nous manqueras.



*XXIV<sup>e</sup> journées arithmétiques à Marseille, campus de Château-Gombert.*



Mémoire 137

**Abstract Analogues of Flux  
as Symplectic Invariants**  
P. Seidel

We study families of objects in Fukaya categories, specifically ones whose deformation behaviour is prescribed by the choice of an odd degree cohomology class. This leads to invariants of symplectic manifolds, which we apply to blowups along symplectic mapping tori.

*(Analogues abstraits du flux comme invariants des variétés symplectiques)*

*Nous étudions des familles d'objets dans des catégories de Fukaya, en particulier celles dont le comportement infinitésimal est déterminé par une classe de cohomologie de degré impair. Cette étude aboutit à des invariants des variétés symplectiques; nous en tirons des conséquences pour les éclatements de tores d'applications symplectiques.*

ISBN : 978-2-85629-788-9

prix public : 30 € - prix membre : 21 €  
frais de port non compris



Institut Henri Poincaré  
11 rue Pierre et Marie Curie  
F-75231 PARIS CEDEX 05

<http://smf.emath.fr>

# VIE DE LA SOCIÉTÉ

---

## La Gazette et vous

---

Afin d'améliorer la formule actuelle de la *Gazette* et de mieux comprendre vos attentes, nous avons lancé un questionnaire entre mars 2014 et mai 2014. Vos réponses nous ont fourni des indications précieuses et nous vous en remercions vivement. Le questionnaire ainsi que les chiffres correspondant aux réponses sont donnés à la fin de ce texte.

Ce questionnaire, ainsi que ce texte, ont été conçus avec l'aide de B. Adamczewski, V. Berthé, A. Bonami, B. Helffer, B. Mallein, M. Peigné, P. Pansu, et S. Seuret.

### Quelques chiffres

Vous avez été 281 à répondre à ce questionnaire. Il convient donc bien sûr de rester prudent quant à la significativité des chiffres. À titre de comparaison, il y a eu 534 votes lors des élections 2014 au conseil de la SMF. Parmi ces 281 retours, on compte 237 hommes et 44 femmes ; on compte également 267 adhérents, dont 48 sont également adhérents de la SMAI ; enfin on compte 239 retours de membres de l'enseignement supérieur et de la recherche. La répartition selon les tranches d'âge est la suivante : 22 réponses dans la tranche  $< 30$  ans, 108 réponses dans la tranche 30-45 ans, 89 réponses dans la tranche 45-65 ans, et enfin 62 dans la tranche  $> 65$  ans.

### La Gazette et vous

Le lecteur de la *Gazette* fait plus que simplement parcourir la *Gazette* ; la lecture n'est pas exhaustive, le lecteur se concentre sur certains articles. La *Gazette* se lit surtout chez soi. Les numéros spéciaux sont lus. Les attentes concernant la *Gazette* sont multiples : la *Gazette* doit à la fois être une revue scientifique, un bulletin interne de la SMF, une source d'informations sur la vie de la communauté mathématique et un lieu de découverte de thèmes mathématiques. Un examen plus attentif des réponses permet de penser que les lecteurs attendent d'abord de la *Gazette* qu'elle soit un lieu d'information sur la vie de la communauté mathématique, mais aussi de découverte de nouveaux thèmes mathématiques. Ils ne la voient pas comme une source classique d'information scientifique.

## L'organisation par rubriques

L'organisation par rubriques est appréciée et leur choix actuel est jugé pertinent. Parmi les rubriques proposées, un souhait se dégage concernant le fait d'avoir régulièrement une rubrique « Actualités mathématiques ». Le retour concernant une rubrique régulière « Problèmes, jeux et énigmes » est moins tranché.

### Quelles rubriques souhaiteriez-vous voir dans la Gazette ?

Vous êtes nombreux à citer la rubrique *WHAT IS...* des *Notices* l'American Mathematical Society. Parmi les suggestions de rubriques, citons des rubriques d'ouverture, par exemple vers l'histoire des mathématiques, la philosophie mathématique ou les liens entre mathématiques et art. Notons également comme suggestion « l'ouverture des colonnes de la *Gazette* aux non mathématiciens (journalistes, scientifiques, juristes etc. » ainsi que des entretiens afin d'entendre des « mathématiciens sur le (leur) travail de recherche mathématique et sa signification. »

### Mot du président, éditorial, tribune libre

Le mot du président, l'éditorial et la tribune sont souvent, voire toujours, lus. La tribune libre est en particulier jugée intéressante.

## Enseignement

Il s'agit d'une rubrique qui est lue dont le contenu est considéré comme intéressant (178) et utile (170) mais pas forcément adapté (116 oui et 126 sans avis). Nous avons une marge de manœuvre concernant cette rubrique par rapport à vos attentes : vous êtes 130 à avoir trouvé que son contenu correspond à vos attentes, mais 114 sans avis. Vous êtes 115 à souhaiter voir dans la rubrique Enseignement des articles de nature pédagogique, vous êtes 194 à souhaiter y trouver des articles de réflexion liés aux évolutions en cours, et enfin 174 à souhaiter des articles d'information sur ces évolutions.

### Vos suggestions

Vous aimeriez y trouver des compte-rendus des réunions organisées par la SMF (par exemple autour du CAPES ou des ESPE<sup>1</sup>), des exemples pédagogiques concrets, des informations sur ce qui se passe à l'étranger, des débats. Vous trouvez que cette rubrique est beaucoup tournée vers le milieu universitaire. Vous aimeriez y voir « traiter l'apprentissage/l'enseignement des mathématiques dans son ensemble en proposant des articles de synthèse, de suggestion, d'analyse, transcendant les échelons primaire/secondaire/supérieur », et plus particulièrement les liens entre secondaire, CPGE, université et grandes écoles. Vous soulignez également que « l'importance de l'enseignement des mathématiques est cruciale, à cause d'un phénomène de désaffection des étudiants », thème que vous êtes plusieurs à évoquer.

---

<sup>1</sup> Écoles Supérieures du Professorat et de l'Éducation.

## Articles de mathématiques

Le contenu est un peu spécialisé, tout en étant de longueur appropriée. Vous ne lisez pas que les articles de votre domaine. À la question suivante : « Pensez-vous que votre domaine est bien représenté ? », vous n'êtes que 68 à répondre oui (avec 75 non et 132 sans avis). La couverture thématique pourrait être étendue : vous n'êtes que 112 à la trouver suffisante.

### Quels sujets ou champs thématiques vous paraissent insuffisamment représentés ?

On retrouve le plus souvent cités ici l'histoire des mathématiques, la physique mathématique, et les liens avec l'informatique (logique combinatoire, graphes, aspects algorithmiques des mathématiques).

Un thème qui revient souvent dans vos retours concerne la « mise en œuvre de mathématiques dans d'autres sciences », « les interactions entre les disciplines mathématiques ou les liens avec les autres disciplines (physique, biologie, informatique, économie etc.) ». Vous citez ainsi les mathématiques expérimentales, l'influence du numérique sur les mathématiques, la modélisation mathématique, les « mathématiques appliquées même si la SMAI existe ».

L'actualité mathématique vous tient également à cœur.

À noter un sujet qui revient souvent dans les divers retours libres, à savoir, celui du niveau des articles de mathématiques. Vous notez ainsi que « le problème n'est pas celui des thèmes, mais principalement celui du niveau. Il faut garder des articles de fond, mais en faisant un GROS effort pour vulgariser. Le lecteur de la *Gazette* ne paraît pas être prêt, pour la lire, à faire un effort équivalent à celui qu'il fait pour lire un article technique ».

### Quels domaines des mathématiques et des disciplines connexes souhaiteriez-vous voir abordés ?

Le spectre que vous souhaiteriez voir couvert est large. Voici des domaines que vous suggérez d'aborder : physique (théorique, quantique, expérimentale, appliquée), mécanique théorique, mécanique céleste et astronomie, mécanique des fluides, philosophie mathématique, histoire des mathématiques, épistémologie des sciences, mathématiques discrètes, informatique (pour l'enseignement et pour la recherche, vous citez en particulier le classique problème Clay  $P=NP$  ?).

Vous citez ici encore beaucoup les liens avec d'autres disciplines : « lorsque les mathématiques abordées sont très liées à des problèmes issus de la physique, il serait très intéressant d'avoir l'éclairage de physiciens sur les mêmes questions (sous forme d'un article "jumeau" ou d'encarts), de même éventuellement pour la biologie. » Vous aimeriez voir des « articles introductifs sur les mathématiques utiles en physique fondamentale, par exemple en géométrie riemannienne, en lien avec la théorie de la relativité, ou en théorie des représentations avec la physique des particules. » Vous constatez que « nous savons très peu comment les autres disciplines utilisent les mathématiques. Par exemple, on pourrait reprendre toutes les idées qui ont émergé pour MPT2013<sup>2</sup>, et parler des mathématiques faites ou utilisées par des physiciens, des hydrologues, des économistes. » Les liens entre mathématiques et le

<sup>2</sup> Mathématiques de la planète terre 2013, <http://mpt2013.fr/>

monde vous intéressent. Vous citez ainsi les « mathématiques et applications grand-public : GPS, LTE-4G , vidéo, cartes à puce », les « mathématiques et applications professionnelles, les liens avec le HPC, le Big-Data, les simulations numériques intensives », « l'évolution des mathématiques pour la sécurité et le respect de la vie privée », et vous souhaiteriez plus généralement trouver « une information et une réflexion sur la responsabilité des mathématiciens dans la société ».

Enfin, vous suggérez des articles sur « l'histoire de l'enseignement des mathématiques, l'histoire des institutions d'enseignement du point de vue des mathématiques, l'histoire des communautés mathématiques », sur des sujets d'actualité mathématique, par exemple en lien avec l'ICM<sup>3</sup>, mais également sur les politiques de publication (Open Access).

### Actualité, carnet, recensions

Si la *Gazette* apparaît comme suffisamment connectée à l'actualité de la communauté mathématique nationale, il semble que c'est moins évident pour ce qui concerne l'actualité internationale (113 non, 69 oui, 89 sans avis à la question « Trouvez-vous la *Gazette* suffisamment connectée à l'actualité de la communauté mathématique internationale ? »).

Rien ne semble se dessiner nettement concernant vos attentes éventuelles sur les informations sur les colloques et rencontres à venir, ou bien sur les informations sur la vie locale.

Le carnet est lu. À noter la suggestion suivante concernant le carnet : « Il faudrait qu'entre le site web et la *Gazette* les membres de la SMF trouvent l'information qu'ils souhaitent sur les décès, avec de brefs récapitulatifs de carrières ».

Le lectorat est ouvert à l'ouverture des recensions vers d'autres supports. Considérant les recensions, on peut noter une demande pour les livres autour des mathématiques destinés à un plus large public, les sites web et les expositions.

### Sur la forme

La *Gazette* est perçue comme intéressante (203), lisible (147) et utile (148), mais notons néanmoins une proportion non négligeable de réponses qui la considèrent parfois ennuyeuse (69) et parfois inadaptée (56). Elle n'est perçue comme attrayante que par 49 personnes. Vous n'êtes pas hostiles au fait de voir publier occasionnellement des articles en anglais. Majoritairement les lecteurs apprécient de pouvoir lire cette revue sur papier comme un journal ou un magazine traditionnel. L'idée de voir regroupés au sein d'un même numéro plusieurs articles sur un même sujet paraît bonne, en particulier dans le cadre d'un dossier thématique. Dans les commentaires libres, on trouve enfin que « les articles un peu plus courts permettraient plus de variété dans le choix des thèmes ».

<sup>3</sup> International Congress of Mathematicians.

## Retours libres

### Qu'aimez-vous le plus dans la Gazette ?

Vos réponses reflètent bien la variété et la diversité de vos attentes. Il n'est pas une rubrique qui ne soit pas citée. On sent également un attachement sincère à la *Gazette* avec beaucoup de bienveillance dans les retours.

On trouve plusieurs commentaires concernant l'aspect vivant de la *Gazette* : vous aimez les « biographies, les hommages et récits de vie », « la partie vivante, humaine », « les souvenirs et rétrospectives des vieux mathématiciens », « les articles parlant (quelques fois après leur décès) des mathématicien-ne-s en tant qu'êtres humains ».

L'actualité est également importante pour vous, qu'elle soit mathématique ou qu'elle concerne la communauté au sens large : vous aimez « les articles de débat ou de point de vue sur les sujets d'actualité de notre communauté (enseignement, recrutement, publications, disparitions et hommages) », « les débats, sur les nouvelles formations, sur les évolutions du métier, sur les publications », « le point de vue et les actualités », le fait que la *Gazette* soit une « source d'information en français de haut niveau sur la profession dans tous ses aspects ». Vous aimez « les articles courts et ouvrant la réflexion sur tous les sujets des mathématiques (formation, recherche, enjeux, etc.) » ; vous citez aussi « la diversité des sujets abordés », « la variété des articles (recherche, recensions, informations sur la politique de l'enseignement et la recherche...) qui rassemble de façon efficace tous les principaux aspects de la vie de la communauté mathématique ».

Vous êtes attachés à la lisibilité et au fait de découvrir de nouvelles choses. Vous soulignez ainsi « le fait que la *Gazette* ne se contente pas d'être un bulletin de liaison d'une société savante et qu'au contraire elle a une véritable ambition de contenu, » et que la *Gazette* « donne ainsi une idée de l'actualité mathématique à laquelle on n'a pas toujours accès, parce que les discussions entre les collègues de champs disciplinaire différents ne sont pas systématiques ».

### Qu'aimeriez-vous voir dans la Gazette ?

Vous aimeriez y voir des articles concernant des aspects sociétaux, « des réflexions approfondies sur la situation des femmes en mathématiques, et plus généralement sur le manque de diversité sociale de notre profession », vous aimeriez y voir traiter des sujets généraux comme une réflexion sur la désaffection et la disparition des étudiants.

L'histoire des mathématiques est souvent citée, et vous souhaiteriez également « un peu plus d'articles intégrant des aspects historiques sur l'évolution des idées ».

Sur la forme, vous aimeriez « un style plus enjoué », « qu'on parle un peu plus, sous une forme non forcément figée (interviews, reportages, enquêtes) ». Vous êtes plusieurs à également souhaiter trouver une part d'images plus importante. Notons que de nombreux retours insistent sur l'importance de la lisibilité pour les articles mathématiques, et sur le fait d'avoir des articles plus courts. Dans le même esprit, vous souhaitez « plus d'articles de synthèse peu techniques, mais donnant un aperçu sur un domaine et les problématiques importantes qu'il porte ». Enfin, vous aimeriez « davantage de dossiers thématiques, à l'occasion d'hommages, d'événements ou tout simplement lorsque des idées neuves apparaissent dans un domaine des mathématiques ».

La vulgarisation est un sujet qui vous mobilise et vous souhaiteriez des retours sur les diverses expériences menées. L'international est également un sujet qui vous mobilise : vous aimeriez trouver des articles sur les mathématiques en Europe, en Afrique, et plus généralement, plus d'informations sur l'actualité mathématique internationale. Vous aimeriez enfin trouver des analyses politiques des réformes en cours sur l'enseignement et la recherche. Vous aimeriez voir accordée une « plus grande place à des articles de nature transdisciplinaire, ou centrés sur des applications industrielles, professionnelles, ou grand public », ainsi que trouver des portraits de « mathématicien(ne)s exerçant en dehors du monde académique ».

### Vos remarques et suggestions

Parmi vos remarques et suggestions, on y trouve le fait de regarder ce qui se fait ailleurs, à l'international où « il y a d'excellents articles dans les équivalents étrangers de la *Gazette*, la SMF pourrait avoir une politique consistant à en traduire certains dans la *Gazette* », au niveau des liens avec les autres sociétés savantes, SMAI et SIF<sup>4</sup> en particulier, ainsi que le développement des liens avec « Images des mathématiques ». Dans le même esprit, plusieurs retours concernent une demande pour des articles de vulgarisation, « vulgarisation de haut niveau », « vulgarisation en interne, pour des mathématiciens professionnels, mais d'horizons divers dans le but d'avoir un aperçu culturel d'autres domaines ».

On retrouve plusieurs fois une demande d'ouverture vers les divers acteurs de la communauté : « Ce serait utile d'avoir plus d'ouverture sur l'enseignement des maths en lycée/collège, sur les carrières de mathématiciens dans l'industrie etc... » ; il serait bien que la *Gazette* « ouvre une tribune courte mais annoncée plus clairement sur les politiques en cours sur la recherche et l'enseignement en mathématiques, avec des intervenants les plus variés, pas que parisiens, témoignages directs d'enseignants, chercheurs, élus dans les conseils, syndicats, responsables de départements, laboratoires, écoles doctorales » ; vous citez enfin une demande pour « plus de présence des acteurs de terrain (vie de la société, vie des départements de maths, vie des labos, etc.) ».

**Remerciements.** On trouve plusieurs retours avec des remerciements pour celles et ceux qui font vivre la *Gazette*, ainsi que plusieurs retours concernant un attachement pour la qualité typographique. Nous en profitons donc pour remercier très chaleureusement Claire Ropartz pour son travail d'édition minutieux ainsi que Frédérique Petit, pour sa relecture attentive.

## Questionnaire

Voici les chiffres correspondant aux réponses du questionnaire.

### La *Gazette* et vous

- Quelles sont vos habitudes de lecture ?
- Je lis l'ensemble des rubriques/articles 60
- Je ne lis que les articles qui m'intéressent 192
- Je ne fais que parcourir la revue 36

<sup>4</sup> Société Informatique de France.

• Dans quelles circonstances lisez-vous la <i>Gazette</i> ?	
– Au coin café de mon laboratoire	24
– À la bibliothèque	9
– Dans mon bureau	66
– Chez moi	226
– Dans les transports en commun	69
• Lisez-vous les numéros spéciaux ?	
– Oui	203
– Non	59
• Vous percevez actuellement la <i>Gazette</i> comme	
– Une revue scientifique	
– Principalement	56
– En partie	185
– Pas du tout	35
– Le bulletin interne de la SMF	
– Principalement	90
– En partie	160
– Pas du tout	21
– Une source d'informations sur la vie de la communauté mathématique	
– Principalement	110
– En partie	164
– Pas du tout	3
– Un lieu de découverte de thèmes mathématiques	
– Principalement	40
– En partie	209
– Pas du tout	29
• Quels rôles devrait jouer la <i>Gazette</i> selon vous ?	
– Être une revue scientifique	
– Principalement	35
– En partie	175
– Pas du tout	60
– Être le bulletin interne de la SMF	
– Principalement	86
– En partie	167
– Pas du tout	17
– Être une source d'informations sur la vie de la communauté mathématique	
– Principalement	138
– En partie	138
– Pas du tout	0
– Être un lieu de découverte de thèmes mathématiques	
– Principalement	88
– En partie	177
– Pas du tout	9

**L'organisation par rubriques**

- Le choix actuel des rubriques de la *Gazette* vous semble-t-il pertinent ?
  - Oui 172
  - Non 13
  - Sans avis 87
- Aimez-vous le principe de l'organisation par rubriques de la *Gazette* ?
  - Oui 203
  - Non 7
  - Sans avis 61

Si oui

- Aimez-vous retrouver les mêmes rubriques d'un numéro à l'autre ?
  - Oui 146
  - Non 15
  - Sans avis 96
- Diriez-vous que l'idée d'une rubrique régulière « Actualités mathématiques » est
  - Excellente 128
  - Bonne 126
  - Sans grand intérêt 10
- Diriez-vous que l'idée d'une rubrique régulière « Problèmes, jeux, énigmes » est
  - Excellente 55
  - Bonne 111
  - Sans grand intérêt 98

**Mot du président, éditorial, tribune libre**

Lisez-vous le mot du président

- Toujours 95
- Souvent 131
- Rarement 46
- Jamais 8

Trouvez-vous le mot du président intéressant ?

- Oui 161
- Non 13
- Sans avis 101

Lisez-vous l'éditorial

- Toujours 83
- Souvent 135
- Rarement 53
- Jamais 7

Trouvez-vous l'éditorial intéressant ?

- Oui 141
- Non 10
- Sans avis 123

## Lisez-vous la tribune libre ?

– Toujours	76
– Souvent	151
– Rarement	44
– Jamais	5

## Trouvez-vous la tribune libre intéressante ?

– Oui	176
– Non	8
– Sans avis	86

### Enseignement

- Vous lisez la rubrique Enseignement

– Toujours	69
– Souvent	136
– Rarement	64
– Jamais	11

- Trouvez-vous le contenu de la rubrique Enseignement

– intéressant ?	
– Oui	178
– Non	16
– Sans avis	76
– utile ?	
– Oui	170
– Non	24
– Sans avis	75
– adapté ?	
– Oui	116
– Non	20
– Sans avis	126

- Est-ce que ce contenu correspond à vos attentes ?

– Oui	130
– Non	17
– Sans avis	114

Si non, avez-vous des suggestions ?

- Aimerez-vous voir dans la rubrique Enseignement des articles de nature

– pédagogique ?	115
– de réflexion liés aux évolutions en cours ?	194
– d'information sur les évolutions en cours ?	174

**Articles de mathématiques**

• Trouvez-vous que le contenu des articles de mathématiques est en général	Oui	Non
– ouvert à destination d'un public varié	128	101
– un peu spécialisé	178	38
– trop spécialisé	76	118
– trop élémentaire	6	172
– adapté en difficulté	122	67
– trop difficile	72	108
• Les articles de mathématiques vous paraissent-ils		
– trop courts		10
– de longueur appropriée		198
– trop longs		62
• Lisez-vous seulement les articles de votre domaine ?		
– Oui		45
– Non		277
• Pensez-vous que votre domaine est bien représenté ?		
– Oui		68
– Non		75
– Sans avis		132
Quel est votre domaine ?		
• Trouvez-vous la couverture thématique		
– suffisante		112
– insuffisante		34
– appropriée		83

**Actualité, carnet, recensions**

• Trouvez-vous la <i>Gazette</i> suffisamment connectée à l'actualité de la communauté mathématique nationale ?		
– Oui		175
– Non		35
– Sans avis		62
• Trouvez-vous la <i>Gazette</i> suffisamment connectée à l'actualité de la communauté mathématique internationale ?		
– Oui		69
– Non		113
– Sans avis		89
• Souhaiteriez-vous trouver des informations dans la <i>Gazette</i> sur des colloques et rencontres à venir ?		
– Oui		115
– Non		94
– Sans avis		62
• Souhaiteriez-vous trouver des informations dans la <i>Gazette</i> sur la vie mathématique locale ?		

– Oui	123
– Non	71
– Sans avis	71
• Lisez-vous le Carnet	
– Toujours	53
– Souvent	110
– Rarement	89
– Jamais	14
Avez-vous des suggestions concernant le Carnet ?	
• Souhaiteriez-vous voir recensés	
– des livres de recherche ?	
– Oui	192
– Non	36
– Sans avis	36
– des livres autour des mathématiques destinés à un plus large public ?	
– Oui	203
– Non	32
– Sans avis	34
– des livres des disciplines connexes ?	
– Oui	119
– Non	77
– Sans avis	66
– des films ?	
– Oui	110
– Non	81
– Sans avis	71
– des sites web ?	
– Oui	171
– Non	45
– Sans avis	51
– des expositions ?	
– Oui	152
– Non	48
– Sans avis	65

### Sur la forme

• D'une manière générale, vous diriez que la <i>Gazette</i> est	
– Intéressante	203
– Lisible	147
– Utile	148
– Attrayante	49
– Parfois ennuyeuse	69
– Parfois inadaptée	56

● Pensez-vous que la <i>Gazette</i> peut publier occasionnellement quelques articles en anglais ?	
– Oui	151
– Non	80
– Sans avis	40
● Souhaiteriez-vous voir regroupés au sein d'un même numéro plusieurs articles sur un même sujet dans le cadre	
– d'un hommage ?	
– Oui	199
– Non	25
– Sans avis	44
– d'un dossier thématique ?	
– Oui	227
– Non	16
– Sans avis	27
– d'un dossier événementiel (par exemple ICM) ?	
– Oui	195
– Non	28
– Sans avis	44
● Appréciez-vous de pouvoir lire cette revue sur papier comme un journal/magazine traditionnel ?	
– Oui	231
– Non	14
– Sans avis	23

### **Votre profil**

● Vous êtes	
– un homme	237
– une femme	44
● Votre tranche d'âge	
– < 30 ans	22
– 30-45	108
– 45-65	89
– > 65	62
● Secteur d'activité	
– Administration/Services	3
– Enseignement	23
– Enseignement supérieur/Recherche	239
– Industrie	7
– Autre	9
● Discipline	
– Économie	3
– Informatique	9
– Mathématiques	263

– Industrie	2
– Autre	4
• Grade	
– Agrégé(e) préparateur(trice)	1
– Assistant(e)	2
– ATER/Post-doc	8
– Chargé(e) de recherche	12
– Directeur(trice) de recherche	18
– Instituteur/Professeur des écoles	1
– Maître(sses) de conférences	71
– PRAG	4
– PRCE	1
– Professeur(e)	99
– Professeur(e) agrégé(e)	9
– Professeur(e) certifié(e)	1
– Professeur(e) des Classes Préparatoires aux Grandes Écoles	12
– Professeur(e) de chaire supérieure	6
– Thésard(e)	15
– Autre	21
• Vous êtes adhérent de la SMF	
– Oui	267
– Non	14
• Vous êtes adhérent d'une autre société	
– APMEP	16
– SFdS	7
– SIF	4
– SMAI	48
– UPS	14
– Autre	77

## Les prix d'Alembert et Anatole Decerf 2014

Pierre Pansu<sup>1</sup>

---

Le 20 juin 2014, à l'issue de la journée annuelle de la SMF, a eu lieu la remise des prix d'Alembert et Decerf.

« Le Prix d'Alembert, d'un montant de 2000 euros, récompense une personne ou un groupe étant parvenu, par la réalisation d'un ouvrage, d'un film, d'une émission de radio ou de télévision, d'une exposition ou de tout autre moyen, à intéresser le public aux développements des mathématiques et à les relier aux préoccupations de nos contemporains. Le prix d'Alembert est décerné par la SMF. »

« Le Prix Anatole Decerf, d'un montant de 2000 euros, récompense des travaux d'enseignement ou de vulgarisation de la pédagogie des mathématiques. Le Prix Anatole Decerf est décerné par la Fondation Anatole Decerf (sous l'égide de la Fondation de France). »

Le Prix d'Alembert a été fondé par la Société Mathématique de France en 1984, et a été attribué tous les deux ans depuis cette date. L'édition 2014 a bénéficié d'un soutien apprécié de la Fondation Mathématique Jacques Hadamard. Avis aux mécènes pour la prochaine édition, en 2016 ! Le site<sup>2</sup> de la SMF indique les lauréats des 12 éditions et la composition des jurys successifs.

En 2014, la SMF a reçu 31 candidatures, dans des registres très divers : 3 sites internet à caractère institutionnel, 6 sites internet individuels, 3 cycles de conférences, 1 émission de radio, 2 films, 7 livres, 3 collections de livres, 1 troupe de théâtre, 1 artiste, 5 personnes ou groupes de personnes impliqués dans l'animation sur le terrain. Devant cette profusion d'initiatives, souvent excellentes, le jury composé de 12 personnalités (N. Anantharaman, M. Andler, P. Bellingeri, A. Bonami, V. Chauveau, P.-A. Chérix, A. de Bouard, M. Fréchet, C. Imbert, D. Larousserie, F. Letué, P. Pansu (président)) a choisi de partager le prix d'Alembert et de donner des accessits à trois candidatures remarquables.

Le prix d'Alembert 2014 a été décerné au réalisateur Olivier Peyon et à l'association *Maths pour tous*. Le prix Anatole Decerf a été décerné au groupe Jeux de l'Association des Professeurs de Mathématiques de l'Enseignement Public (AP-MEP).

Le film *Comment j'ai détesté les maths*, d'Olivier Peyon, représente un travail de longue haleine, sur 4 ans. Il aborde de front les aspects les plus rébarbatifs des mathématiques (enseignement vécu comme une contrainte par de nombreux élèves, implication de la recherche dans la crise financière de 2008), tout en révélant au public de multiples facettes de notre discipline, de façon profondément humaine. Nommé aux Césars 2014, il a d'indéniables qualités cinématographiques. Le sujet était risqué, la sortie en salles un pari qui a été remarquablement réussi. Olivier Peyon fait état de 85 000 entrées depuis la sortie en novembre 2013. Le film a donné lieu à de multiples débats dans toute la France, c'est un outil exceptionnel pour parler de mathématiques avec le public.

---

<sup>1</sup> Université Paris-Sud.

<sup>2</sup> <http://smf.emath.fr/content/prix-dalembert-et-prix-anatole-decerf>

L'association *Maths Pour Tous* porte les mathématiques au-devant du grand public dans tous les coins des régions Provence-Alpes-Côte-d'Azur et Corse. En s'appuyant sur les réseaux de clubs et d'ateliers, elle organise des forums, sur le continent et en Corse, où les élèves se font médiateurs des mathématiques pour un public toujours plus nombreux (plusieurs milliers de visiteurs aux éditions récentes). Elle irrigue les manifestations scientifiques plus larges, lors de la fête de la science ou de souks des sciences dans les petites villes des Alpes. La qualité des travaux d'élèves présentés est attestée par de nombreuses récompenses nationales et internationales.

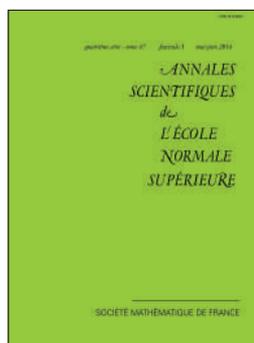
Depuis sa création, il y a 35 ans, le Groupe *JEUX de l'APMEP* s'est investi pour faire entrer le jeu et les activités ludiques dans les ateliers puis en classe de mathématiques avec de très nombreuses fiches pour un travail individuel, par petit groupe ou en classe entière. La diffusion de ses 14 brochures éditées par l'APMEP est large comme en témoignent les nombreuses rééditions. Ce matériel de haute qualité couvre une grande variété de sujets, et s'adresse à tous les niveaux, de l'école élémentaire au lycée. Les fiches les plus récentes propagent dès l'école maternelle le plaisir ludique que chacun peut prendre à faire des mathématiques. Cette ressource est particulièrement précieuse au moment où la communauté fait une priorité de la popularisation des mathématiques dans les écoles.

Le jury a pris plaisir à lire le joli livre *C'est mathématique*, de Carina Louart et Florence Pinaud, aux éditions Actes Sud Junior, qui montre de façon plaisante comment les mathématiques imprègnent notre vie quotidienne. Il encourage les éditions Actes Sud Junior à persévérer sur le créneau des ouvrages scientifiques destinés aux petits et aux tout-petits.

Il a souhaité aussi saluer l'engagement d'un professeur qui emmène les élèves de son club dans une aventure sans cesse renouvelée, Hubert Proal. Familier des compétitions et des récompenses internationales, le club du Lycée d'Altitude de Briançon est présent dans d'innombrables manifestations, y compris en altitude.

Enfin, il a décerné une mention spéciale à une sorte d'alchimiste qui sait tout transformer en mathématiques, François Sauvageot. Engagé simultanément sur tous les fronts de la communication des mathématiques, tous les moyens lui sont bons, jusqu'au théâtre et à la danse, seul ou entouré d'élèves. Chacun de ses spectacles combine une réflexion approfondie sur les moyens de faire passer un message mathématique et une capacité d'improvisation sidérante.

De nombreux projets de qualité portaient sur la mise en ligne de ressources pédagogiques. Bien qu'aucun d'entre eux n'ait pu être primé, le jury a observé avec intérêt l'émergence de ces nouveaux outils.



## Annales Scientifiques de l' ÉNS Dernières parutions

### Volume 47, fascicule 4 (2014)

- M. EMERTON, D. HELM - The local Langlands correspondence for  $GL_n$  in families  
 M. CHEN - Composantes connexes géométriques de la tour des espaces de modules de groupes  $p$ -divisibles  
 Y. HARPAZ, Alexei N. SKOROBOGATOV - Singular curves and the étale Brauer-Manin obstruction for surfaces  
 H. DARMON, V. ROTGER - Diagonal cycles and Euler systems I: A  $p$ -adic Gross-Zagier formula  
 B. BHATT, A. J. DE JONG - Lefschetz for Local Picard groups

### Volume 47, fascicule 3 (2014)

- P. GERMAIN & N. MASMOUDI – Global existence for the Euler-Maxwell system.  
 S. SAITO & K. SATO – Zero-cycles on varieties over  $p$ -adic fields and Brauer groups.  
 C. E. KENIG, G. PONCE & L. VEGA – A theorem of Paley-Wiener type for Schrödinger evolutions.  
 F. BERNICOT & S. KERAANI – On the global well-posedness of the 2D Euler equations for a large class of Yudovich type data.  
 S. HOFMANN & J. M. MARTELL – Uniform rectifiability and harmonic measure I: Uniform rectifiability implies Poisson kernels in  $L^p$ .

prix public\* : 77 € (frais de port non compris)

Revue disponible aussi par abonnement :

prix public : [smf.emath.fr/tarifs-abonnements-prix-public-2014](http://smf.emath.fr/tarifs-abonnements-prix-public-2014)



Institut Henri Poincaré  
 11 rue Pierre et Marie Curie  
 F-75231 PARIS CEDEX 05

<http://smf.emath.fr>

# INFORMATIONS

---

## Quelques nouvelles de l'Insmi

Sinnou David et Clotilde Fermanian Kammerer

---

### Délégations CNRS 2014

La campagne des délégations 2014 s'est achevée pour l'Insmi avec un bilan de 102,5 années de délégations sur un total de 480 années. À titre de comparaison, le bilan était de 107,5 sur 500 en 2013. La baisse du nombre total de délégations offerte par le CNRS est liée à la réévaluation de la compensation financière versée aux universités.

Ainsi, comme les années précédentes, bien qu'il soit le plus petit des dix instituts du CNRS, l'Insmi bénéficie d'un cinquième des délégations mises en jeu. En effet, la communauté mathématique est très universitaire et a donc davantage recours aux délégations que d'autres disciplines.

Ces 102,5 années se répartissent en 14 délégations d'un an à temps plein et 177 délégations d'un semestre ou d'un an à temps partiel (22 et 171 en 2013). Ce sont donc 191 collègues qui bénéficieront d'une délégation durant l'année universitaire 2014/2015. Sachant que l'institut avait reçu 285 demandes, le pourcentage de satisfaction est de 67% (305 demandes, soit 63% de satisfaction en 2013).

Depuis la campagne 2013, l'étape finale de l'attribution des délégations se fait au niveau des « sites » et est arbitrée par son délégué scientifique référent (DSR). Celui-ci recueille les avis élaborés par les sections du comité national puis dialogue avec les directions d'établissements et les Instituts. Pour nous, l'expertise scientifique des dossiers a été faite par la section 41 du comité national qui a examiné tous les dossiers de l'Insmi en s'appuyant sur la liste de critères élaborée par le comité national et l'Insmi, liste qui a été publiée sur le site de la section.

Comme toujours, le projet scientifique a été l'élément déterminant de l'évaluation du dossier. Rappelons aussi que la fiche synthétique demandée par l'Insmi doit être renseignée clairement. En particulier, les informations concernant les services faits lors des années précédentes, les décharges, les CRCT et les délégations auprès d'autres organismes de recherche (INRIA par exemple) doivent y apparaître. Enfin, concernant les accueils en UMI, il faut penser à se signaler auprès du directeur scientifique adjoint en charge de l'international ; pour mémoire, un appel d'offre spécifique est envoyé aux laboratoires durant l'automne.

### **Postes de chercheurs associés 2014**

Chaque année, lors des demandes effectuées par les unités dans le cadre du dialogue de gestion, il est possible de demander des postes de chercheurs associés (postes rouges). Ces postes permettent de faire venir dans nos unités (UMR, UMS, FR) des chercheurs venant de l'étranger qui sont embauchés sur un contrat à durée limitée et rémunérés à un échelon correspondant à leur expérience.

Dans ce cadre, à l'automne 2013, l'Insmi a reçu 62 demandes : 35 DR, 19 CR, 6 post-doctorants et 2 doctorants. Comme les années précédentes, l'Insmi a affecté tous ses crédits de CDD chercheur pour les invitations de chercheurs étrangers confirmés. Les dossiers scientifiques ont été évalués par le comité national et 30 de ces demandes ont été acceptées, 24 DR et 6 CR. Ces postes de chercheurs associés correspondent annuellement à 7,25 emplois à temps plein. Parmi ces demandes, 1,5 années concernent l'organisation des semestres à l'IHP, et 1,5 années des chercheurs issus de nos UMI/LIA.

## LIVRES

---

---

### **Cryptologie et Mathématiques. Une mutation des enjeux**

SOUS LA DIRECTION DE MARIE-JOSÉ DURAND-RICHARD ET

PHILIPPE GUILLOT

L'Harmattan, 2014. 312 pp. ISBN 978-2-343-02522-3, 32€

---

Contrairement à d'autres ouvrages sur l'histoire de la cryptologie, les éditeurs du livre *Cryptologie et Mathématiques. Une mutation des enjeux* se focalisent sur la relation entre la cryptologie et les mathématiques. Si on regarde la longue durée, la cryptologie met en œuvre une diversité de savoirs et techniques, certains tirés des domaines du langage, d'autres de l'écriture et sa transmission, de l'analyse logique ou formelle etc. Ce n'est qu'avec l'automatisation et les communications digitales du XX<sup>e</sup> siècle que la cryptologie est entrée dans une relation privilégiée avec les mathématiques. Le livre est consacré à la mutation de cette relation. Il contient des analyses historiennes, des témoignages d'acteurs et des traductions de textes importants, tous arrangés en ordre chronologique. Le recueil est le résultat d'un enseignement et d'une recherche en histoire de cryptologie menés au sein du laboratoire de mathématiques et histoire des sciences de l'université Paris 8 qui, depuis 2003, organise une spécialité « Mathématiques appliquées et protection de l'information ».

Une partie du livre peut être considérée comme une excellente introduction à l'histoire de la cryptologie et ses trois époques. La périodisation suit à peu près celle proposée par Jacques Stern dans son livre *La science du secret* (1998) : d'abord un âge artisanal, puis un âge technique et finalement un âge paradoxal où la science du secret devient un outil public. Le premier chapitre, écrit par les éditeurs, « L'ancrage de la cryptologie dans les jeux d'écriture », décrit l'époque littéraire et diplomatique en cryptologie qui s'étend de l'Antiquité jusqu'au milieu du XIX<sup>e</sup> siècle. Même si des mathématiciens comme Viète ou Wallis sont parfois impliqués, la cryptologie à cette époque utilise encore surtout l'analyse linguistique et sémantique et repose sur des procédés manuels ou mécaniques. Ce chapitre est complété par la traduction en fragment du premier traité connu sur la cryptologie, un texte de Al-Kindi datant du IX<sup>e</sup> siècle, « Sur l'extraction de l'obscur ». Le chapitre suivant, « Du message chiffré au système cryptographique » signé par Marie-José Durand-Richard, s'intéresse à l'époque industrielle et militaire en cryptologie, du milieu du XIX<sup>e</sup> siècle à nos jours. Cette époque voit l'introduction des mathématiques en cryptologie, en parallèle avec l'établissement des réseaux de communication (téléphone, télégraphe, radio etc.) et avec les processus de mécanisation. Les guerres y figurent comme les catalyseurs dans le développement de nouvelles techniques. La troisième époque, celle de la cryptologie publique qui ne commence que dans les années 1970 et où l'ordinateur va jouer un rôle primordial, est ici représentée par une traduction du texte classique de Diffie et Hellman, « Les nouvelles orientations de la cryptographie » (1976) qui introduit l'idée d'une cryptologie asymétrique.

Une autre partie du livre informe sur quelques épisodes de la cryptologie en France. Sophie de Lastours écrit sur « Les travaux de la Section du Chiffre pendant la Première Guerre Mondiale » expliquant le système allemand et son décryptement, qui est illustré par des exemples fameux comme le télégramme de Zimmermann ou le radiogramme de la victoire. André Cattieuw montre comment la cryptologie gouvernementale en France se modernise après la Seconde Guerre mondiale avec l'introduction de l'électronique et l'établissement d'une formation mathématique. Louis Guillou finalement raconte le succès des systèmes cryptologiques dans le domaine public sous la forme de la carte à puce, de ses débuts en France jusqu'au cartes bleues et cartes SIM qu'on trouve partout dans le monde aujourd'hui.

Enfin, d'autres articles creusent les relations entre les mathématiques et la cryptologie dans les dernières décennies du XX<sup>e</sup> siècle. Il s'agit en particulier de l'influence réciproque entre la théorie des nombres et la cryptologie depuis l'avènement de la cryptographie asymétrique, qui repose sur des questions de factorisation, d'indices modulo un nombre premier, etc. Cette influence se traduit entre autres par des questions d'institutionnalisation et de formation disciplinaire. Catherine Goldstein questionne ces relations sous plusieurs angles : par une analyse de l'évolution des mots-clé et rubriques qui sont utilisées pour classer les articles « cryptologiques » et par des cas ponctuels. Même si l'importance de la cryptologie en théorie des nombres est récente, les cas ponctuels, du XVII<sup>e</sup> siècle au XX<sup>e</sup> siècle, montrent que la négociation sur les problèmes et questions à aborder ne l'est pas. Les contributions de Jean-Louis Nicolas et de Neal Koblitz (ce dernier traduit de l'anglais) étudient l'institutionnalisation de la cryptologie au sein des universités (qui a été stimulée par des mathématiciens) ainsi que l'identité disciplinaire de la théorie des nombres qui se transforme (non sans discussions !) sous l'influence de la cryptologie. Ces contributions falsifient amplement les fameux propos de G.H. Hardy (1940) selon lesquels la théorie des nombres demeure « éloignée des activités humaines ordinaires » et reste « noble et propre », en montrant au contraire que les mathématiques ne peuvent pas éluder les enjeux économiques, politiques et sociaux.

Les éditeurs ont fait un excellent travail dans l'annotation des chapitres, même si une bibliographie commentée pour approfondir certains aspects et thèmes aurait pu être un atout. Le livre souffre d'un défaut regrettable, il contient encore un nombre non-négligeable de coquilles.

Avec les deux chapitres des éditeurs et les textes traduits, ce recueil contient tous les éléments pour un cours d'introduction à l'histoire de la cryptologie. Le livre offre de plus des contributions fascinantes sur l'histoire plus récente de la cryptologie, en particulier sur la contribution française ou sur la cryptologie publique, et une réflexion poursuivie sur le statut même de la cryptologie.

Maarten Bullynck  
Université Paris 8

---

**Classical and Multilinear Harmonic Analysis (vol. I)**

C. MUSCALU, W. SCHLAG

Cambridge University Press, 2013. 387 pp. ISBN 978-0521882453, 47€

---

J'ai lu avec délices le volume I de « Classical and Multilinear Harmonic Analysis » de C. Muscalu et W. Schlag. Ces deux volumes dans le fond se présentent un peu comme « le Zygmund du XXI<sup>e</sup> siècle » dans la mesure où ils présentent l'état de l'art en analyse harmonique commutative jusqu'aux dernières années, avec, au tome II (que je n'ai pas lu en détail), des morceaux de bravoure comme le théorème de convergence presque partout de Carleson ou les résultats de Lacey et Thiele sur la transformée de Hilbert bilinéaire. Dans la forme, ils pourraient se comparer (tout en portant sur des questions mathématiques plus difficiles) aux quatre tomes du cours de Princeton de Stein et Shakarchi, avec des exercices significatifs en cours de chapitre (pas du type « complétez les détails »), et des problèmes instructifs en fin de chapitre.

Ce n'est pas souvent que des mathématiciens jeunes et en pleine activité prennent la peine et le temps de rédiger des ouvrages à la fois de haut niveau et accessibles à un large public. C'est le cas ici, grâce au souci constant des auteurs d'expliquer les idées principales et de « dévisser » les difficultés techniques. D'ailleurs, la couleur est annoncée dans la préface : « our book is designed as a teaching tool... » Relativisons, il s'agit d'un livre de niveau M2-recherche ! Mais le lecteur, spécialiste ou non du domaine, apprendra une foule de résultats généraux en analyse, probabilités, et théorie des opérateurs. De plus, un jeune chercheur débutant dans ce domaine, et désireux de s'initier aux techniques avancées de l'analyse harmonique, ne pourra que gagner un temps précieux en lisant de façon approfondie l'ouvrage en question.

Une chose m'a frappé, la clarté et la beauté des preuves (par exemple au chapitre sur les principes d'incertitude, où le théorème de Amrein-Berthier est particulièrement bien expliqué, et où le théorème de Logvinenko-Sereda permet une approche du théorème de Malgrange-Ehrenpreis sur les solutions d'EDP linéaires à coefficients constants). Cela suppose de la part de C. Muscalu et W. Schlag une maîtrise impressionnante de sujets d'analyse harmonique variés. Citons par ailleurs, outre des résultats de base sur les transformées de Fourier, de Hilbert et les probabilités, une présentation remarquablement claire de la théorie de Calderon-Zygmund des intégrales singulières et de celle de Littlewood-Paley.

J'ai aussi particulièrement aimé, sans être expert sur la question, la preuve donnée du difficile théorème  $T(1)$  de David-Journé, dans laquelle les outils viennent naturellement quand on en a besoin : la décomposition de Calderon-Zygmund en « bonne et mauvaise » fonctions pour se ramener à  $p = 2$ , l'utilisation des para-produits pour se ramener à  $T(1) = 0$ ,  $T^*(1) = 0$  et enfin l'emploi des lemmes de Schur et Cotlar pour estimer les termes restants. On a vraiment l'impression d'apprendre sur le tas, ce qui correspond certainement à la volonté des auteurs.

En conclusion, je recommande donc chaleureusement la lecture de cet excellent cours d'Analyse Harmonique, et son acquisition par toutes nos bibliothèques de recherche.

Hervé Queffélec  
Université Lille 1

---

**The Blind Spot. Lectures on logic**

J.-Y. GIRARD

European Mathematical Society, 2011. 550 pp. ISBN 978-3-03719-088-3, 68€

---

En dépit de son sous-titre, ce livre n'est pas un cours de logique standard (du reste la *Gazette* ne recense pas les livres d'enseignement), mais une présentation de la majeure partie des recherches menées par Jean-Yves Girard depuis plus de quarante ans, exception faite de ses travaux sur les ordinaux des années 80.

L'essentiel des trois premières parties (sur six) correspond à peu près à *Proofs and Types* [18]. Elles contiennent des résultats standards et peuvent bien sûr être utilisées pour un cours de M2 de logique ou d'informatique théorique. Le reste, soit plus de la moitié de cet ouvrage, est consacré aux travaux de l'auteur sur la logique linéaire [8, 9], sur la relecture linéaire des logiques intuitionniste et classique, ainsi que sur les programmes de recherche dérivés de la logique linéaire que sont la géométrie de l'interaction (initiée par [10]) et la ludique (apparue avec [13]).

Cet ouvrage développe un point de vue sur la nature de la logique, qui aboutit à un questionnement sur la question des fondements, elle-même à l'origine de la logique *mathématique* – tandis que la logique en général a au moins vingt-trois siècles. Plutôt que d'étudier la logique à l'œuvre dans les mathématiques, il s'agit plutôt d'étudier, grâce à des mathématiques relativement standard, les preuves, voire les mécanismes de raisonnement de la logique ordinaire, ainsi que les notions informatiques fondamentales de calcul, de ressource, de donnée, de changement d'état, d'interaction etc. Riche en explications et en commentaires, évitant le formalisme excessif de bien des livres de logique, cet ouvrage est vif et plaisant à lire.

Nous allons présenter ce livre en suivant son organisation en six parties chacune composée de trois à cinq chapitres :

- I *The basics*
- II *Around Curry-Howard*
- III *Linear logic*
- IV *Polarized interpretations*
- V *Iconoclasm*
- VI *Geometry of interaction*

**The basics.** La première partie de cet ouvrage présente les origines de la théorie de la démonstration contemporaine. L'auteur commence avec la chute du programme de Hilbert : le théorème d'incomplétude de Gödel. Tandis qu'Hilbert pensait que toutes les mathématiques pouvaient se ramener à des méthodes finitistes et que la cohérence des mathématiques en résultait, le théorème d'incomplétude de Gödel a anéanti tout tel espoir : il est impossible de démontrer la cohérence d'un système contenant l'arithmétique sans faire appel à un système plus puissant. Après une réflexion sur ce théorème de Gödel, ce livre présente les systèmes déductifs modernes qui ont été introduits pour démontrer syntaxiquement la cohérence des mathématiques : le calcul des séquents – qui est

particulièrement adapté à la logique classique – et la déduction naturelle – qui est plus particulièrement adapté à la logique intuitionniste. La logique classique est la logique usuelle des mathématiques, et la logique intuitionniste s'obtient en laissant de côté le principe du tiers exclus (*tertium non datur*). Cette variante de la logique classique issue de réflexions philosophiques a depuis montré son importance cruciale en informatique comme base de la programmation fonctionnelle typée (cf. la partie II du présent ouvrage) et pour les mathématiques constructives, dans lesquelles on se soucie de construire les objets et les solutions dont l'existence est démontrée [21, 22].

Concernant la logique classique, le résultat central est l'élimination des coupures, lequel vaut aussi pour la logique intuitionniste. La règle de coupure correspond à l'utilisation d'un lemme dans une preuve mathématique : de  $A \Rightarrow B$  et  $B \Rightarrow C$  on peut déduire  $A \Rightarrow C$ . Éliminer les coupures, c'est à la fois dire que ce qui est démontrable l'est directement par des méthodes élémentaires et transformer une preuve en une preuve élémentaire (souvent d'une taille considérable). Cette dynamique des preuves sera au cœur des parties IV, V et VI du présent ouvrage. L'existence de preuves sans coupures pour un système incluant la  $\omega$ -règle (si  $P(0), P(1), P(2), \dots$  alors  $\forall n P(n)$ ) permet d'établir une preuve de la cohérence de l'arithmétique, due à Gentzen : il est aisé de voir qu'il n'existe pas de preuve élémentaire du faux. Cela ne contredit en rien le théorème de Gödel. En effet, pour établir l'élimination des coupures avec des preuves finies en hauteur, mais infinies en largeur à cause de la  $\omega$ -règle, Gentzen utilise une induction transfinie jusqu'à l'ordinal  $\varepsilon_0$ , c'est-à-dire une théorie bien plus puissante que la théorie dont il démontre la cohérence : l'arithmétique est essentiellement l'induction jusqu'à  $\omega$ , qui est bien plus petit que  $\varepsilon_0$ .

Concernant la logique intuitionniste cette première partie ne fait que donner les règles et les premières propriétés de cette logique, le plus intéressant faisant l'objet de la partie suivante.

**Around Curry-Howard.** La seconde partie est consacrée à l'isomorphisme de Curry-Howard [19, 18, 20]. Cet isomorphisme établit une correspondance entre programmes informatiques et preuves formelles de la logique intuitionniste, que l'on peut résumer ainsi :

- un **type** au sens informatique (comme entier, liste d'entiers, arbres etc. fonction des entiers dans les entiers, fonction des listes d'entiers dans les entiers,...) est vue comme une **proposition** ;
- une **donnée de type  $T$**  (par exemple l'entier 2 de type entier ou la liste  $\langle 2, 1, 4 \rangle$  de type liste d'entiers) est vue comme une **preuve de la proposition  $T$**  ;
- les programmes sont des données particulières de type  $X \Rightarrow Y$  : par exemple, la fonction qui associe à une liste d'entiers sa longueur sera une preuve de la proposition « liste d'entiers »  $\Rightarrow$  « entier » ;
- la règle de coupure représente l'application d'un programme à un argument, un programme de type  $X$  implique  $Y$  est appliqué à un argument de type  $X$  ;
- la **normalisation** – l'élimination des coupures – représente le **calcul** : tant qu'une preuve (donnée, programme) n'est pas normale, on ne peut savoir de quel

objet il s'agit, par exemple on ne peut savoir si deux objets non normaux sont égaux.

Par exemple, la formule  $\mathbf{Nat} := \forall X.(X \Rightarrow X) \Rightarrow (X \Rightarrow X)$  correspond au type des entiers naturels en représentation unaire. Une preuve (sans coupures) de  $\mathbf{Nat}$  prend un argument, une preuve  $f$  de la formule  $X \Rightarrow X$ , et produit une nouvelle preuve de  $X \Rightarrow X$ , obtenue en itérant  $f$ . La preuve  $\pi_i$  qui produit  $f^i$  à partir de  $f$  représentera l'entier  $i$ . La formule  $\mathbf{Nat} \Rightarrow (\mathbf{Nat} \Rightarrow \mathbf{Nat})$  représente alors les fonctions  $\mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ ; par exemple il existe une preuve  $\rho$  de cette formule qui représente l'implémentation `sum` de la somme sur les entiers. Une règle de coupure entre  $\rho$  et les deux preuves  $\pi_2$  et  $\pi_3$  produit alors une preuve (avec coupure)  $\text{cut}(\text{cut}(\rho, \pi_2), \pi_3)$  de la formule  $\mathbf{Nat}$ . La normalisation de cette preuve correspond alors *pas à pas* au calcul du programme `sum` appliqué aux arguments 2 et 3, c'est-à-dire l'entier 5, et produit la preuve sans coupures  $\pi_5$  de la formule  $\mathbf{Nat}$ .

Les programmes ainsi définis sont sûrs : il a été démontré que les programmes extraits des preuves calculent ce qu'ils sont supposés calculer, s'ils ne font appel qu'à la logique et aux équations satisfaites par la fonction définie [18, 20]. Les fonctions sont alors vues ici comme des termes dotés d'un mécanisme de calcul, mais on peut aussi chercher à les voir comme d'habitude, c'est-à-dire comme l'ensemble statique des couples  $(x, f(x))$  : c'est ce que font les **sémantiques dénotationnelles**, des modèles mathématiques des programmes qui interprètent une fonction avant et après réduction (la fonction peut elle-même être un terme complexe) comme un même morphisme dans une catégorie dont les objets interprètent les propositions.

Toute cette partie du livre repose sur le fait qu'une preuve de  $A \Rightarrow B$  en logique intuitionniste, c'est une fonction des preuves de  $A$  dans les preuves de  $B$ , et qu'on peut considérer qu'une formule est un type et que les preuves de cette formule sont les programmes de ce type [19] – ce qui a pour effet que les types correspondant à des formules non démontrables sont inhabités, sans interprétation, et remédier à ce défaut est l'une des motivations de la ludique, exposée dans la quatrième partie de l'ouvrage.

Ces chapitres relativement standards sur la logique intuitionniste incluent un résultat important de l'auteur du livre, la résolution de la conjecture de Takeuti : les preuves de la logique d'ordre supérieur (système  $F$  et  $F_\omega$ , [3, 4]) admettent une forme normale. La méthode dite des candidats de réductibilité est depuis couramment utilisée pour des systèmes logiques plus puissants incluant par exemple les types dépendants.

**Linear Logic.** La logique linéaire est née de l'étude d'un modèle mathématique – une « sémantique quantitative » – des programmes [2] dans lequel ces derniers sont interprétés par des foncteurs – dit *normaux* – pour lesquels l'auteur montre l'existence d'un développement en série entière. Ainsi, une preuve de  $A \Rightarrow B$  – un programme de type  $A \Rightarrow B$  – est naturellement interprétée comme une fonction *linéaire* d'un espace  $!A$ , une sorte d'algèbre tensorielle  $\bigoplus_{n \in \mathbb{N}} A^{\otimes n}$ , dans  $B$ . La *logique linéaire* est alors obtenue en inscrivant cette décomposition dans la syntaxe. C'est donc un raffinement de la logique usuelle dans laquelle l'implication

$A \Rightarrow B$  est traduite par la formule  $!A \multimap B$ , où  $\multimap$  est une implication *linéaire*, qui utilise une et une seule fois son argument, et  $!$  est un connecteur dit *exponentiel*, qui marque la possibilité de réutiliser une hypothèse.

Cette sémantique quantitative à l'origine de la logique linéaire a également donné lieu à une sémantique dénotationnelle – les *espaces de cohérences*, un modèle plus simple que l'auteur utilise afin d'introduire le sujet. La troisième partie commence donc par décrire cette interprétation catégorique concrète des preuves modulo normalisation.

La logique linéaire [8] dont les différents aspects constituent les chapitres de cette partie peut se voir de diverses manières :

- la logique linéaire est une logique classique (avec une négation qui satisfait les lois de De Morgan  $\neg\neg A \equiv A$ ) qui inclut la logique intuitionniste et en garde le caractère constructif : les preuves d'une même formule ne sont pas toutes identifiables et elle peuvent se voir comme des programmes ;
- la logique linéaire permet de voir les formules comme autant de ressources et permet donc de parler de changement d'état et de modéliser des processus informatiques plus finement que ne le fait la logique intuitionniste.

En combinant ces différents aspects, la logique linéaire jouit de propriétés dont certaines lui sont propres :

- la logique linéaire admet un théorème de normalisation ;
- une sémantique des preuves est naturellement fournie par les espaces cohérents dont la logique linéaire est issue ;
- la logique linéaire peut s'interpréter usuellement dans des structure algébrique ordonnées (sémantique des phases) qui sont l'analogie des algèbres de Boole pour la logique classique.

Outre ces propriétés qui garantissent son statut de logique à part entière, la logique linéaire permet de nouveaux points de vue sur l'objet preuve. En particulier, la logique linéaire est introduite avec deux systèmes de déduction qui se correspondent : le premier est un calcul des séquents où les preuves sont définies intuitivement par des règles et le second est une syntaxe graphique – les « réseaux de preuves », où les preuves sont définies comme les graphes finis satisfaisant à un « critère de correction », une propriété topologique. Cette dernière syntaxe se distingue des systèmes de déduction usuels en cela qu'elle permet de généraliser la notion de preuve : il est possible d'écrire des graphes – des pseudo-preuves, ou « épreuves » – qui ne correspondent pas à des preuves en calcul des séquents (et ne satisfont donc pas au « critère de correction »). Ce dernier aspect, associé à l'étude du processus de normalisation de la logique linéaire, est le point de départ de la géométrie de l'interaction et de la ludique qui sont développées dans les parties suivantes.

Au passage l'auteur présente un résultat peut-être moins connu et repris que la résolution de la conjecture de Takeuti par les candidats de réductibilité, mais qui vient aussi résoudre un problème ouvert : la construction d'un modèle catégorique concret – les espaces de cohérence [7] – des preuves de la logique intuitionniste

propositionnelle du second ordre (système  $F$ ) dans lequel il est possible de quantifier sur des variables de type. Ce travail en rapport avec les travaux de l'auteur sur les ordinaux [5, 6], résout aussi une conjecture en informatique théorique et en sémantique dénotationnelle des programmes.

**Polarized Interpretations.** L'auteur y aborde dans un premier temps la question de la polarisation. La séparation des connecteurs logiques dits positifs et négatifs n'est pas nouvelle, mais elle refait son apparition dans le contexte de la logique linéaire dans les années 1990 au travers de travaux sur la recherche de preuves [1] d'un côté et d'une étude de la logique classique [11] d'un autre côté. Cette partie sur la polarisation mène l'auteur à discuter des sémantiques de jeux, qui étudient les preuves d'une formule  $A$  comme des stratégies gagnantes dans un jeu dont les règles dépendent de  $A$  : le changement de polarité – la négation – revient à échanger les rôles entre joueur et opposant. Ce point de vue permet donc d'envisager que les formules  $A$  et  $\neg A$  peuvent être toutes deux habitées : il existe des stratégies pour le joueur et pour l'opposant, même si seul l'un des deux (au plus) dispose de stratégie(s) gagnante(s). Cette discussion mène donc l'auteur à la description de sa relecture des sémantiques de jeux, la *ludique* [13]. Celle-ci se distingue des sémantiques de jeux traditionnelles du fait que les formules sont issues des stratégies qui, elles, existent en dehors de toute règle du jeu. Les stratégies (non nécessairement gagnantes) pour le jeu  $A$  correspondent à une notion de preuve généralisée – les épreuves – et définissent des tests pour les stratégies gagnantes du jeu  $\neg A$ . C'est alors l'interaction – l'élimination des coupures, ou (via Curry-Howard), l'exécution des programmes – et une notion de terminaison qui permettent de définir les formules : un ensemble de tests  $A$  définit la formule  $\neg A$  comme l'ensemble des épreuves  $a'$  telles que l'élimination des coupures de  $a'$  appliquée à un test  $a \in A$  – une épreuve également – termine. Les différents connecteurs de la logique linéaire (sans exponentielles) peuvent alors être définis à partir d'opérations portant sur les preuves/programmes : par exemple, une épreuve  $\pi$  est dans  $A \multimap B$  si pour chaque épreuve  $\rho$  dans  $A$ , l'épreuve  $\text{cut}(\pi, \rho)$  est dans  $B$ . Le dernier chapitre de cette partie est consacré à une discussion sur les connecteurs exponentiels de la logique linéaire et présente le travail de l'auteur concernant la logique classique [11].

**Iconoclasm.** Le premier chapitre est consacré aux connecteurs exponentiels de la logique linéaire. Une modification des règles régissant ces connecteurs permet d'obtenir des systèmes logiques restreints qui permettent de caractériser des classes de complexité [12]. Ainsi, une remise en question des principes régissant traditionnellement les duplications – la réutilisation d'hypothèses – en logique permet une approche des classes de complexité reposant sur l'idée que celles-ci correspondent à des différents infinis<sup>1</sup>. Via la correspondance de Curry-Howard, il existe des formules **Nat** et **Nat**  $\Rightarrow$  **Nat** correspondant respectivement aux types des entiers naturels et des fonctions des entiers dans les entiers. Ceux-ci, lorsque l'on considère la logique linéaire, contiennent des preuves correspondant à toutes les fonctions calculables. Dans un système logique restreint, ou « borné », comme

<sup>1</sup> Il faut comprendre ici une classification des infinis différente de celle de Cantor, plus fine, puisqu'il s'agit de distinguer des infinis qui ne contiennent pas une infinité d'infinités.

les systèmes ELL ou LLL présentés dans l'ouvrage, la restriction des règles de construction des preuves impose une restriction de l'ensemble des preuves d'une formule donnée. On peut alors montrer que les preuves de la formule  $\mathbf{Nat} \Rightarrow \mathbf{Nat}$  dans ELL (resp. LLL) correspondent aux fonctions calculables en temps élémentaire (resp. polynomial).

Le chapitre suivant décrit une relecture de la logique inspirée de la mécanique quantique. Une formalisation alternative des espaces de cohérence permet d'étendre ceux-ci afin d'interpréter les formules de la logique comme des ensembles de fonctions à valeur réelle positive (espaces de cohérence probabilistes) ou des ensembles de matrices auto-adjointes (espaces de cohérence quantiques). Ce travail est cependant limité car cette interprétation ne se généralise pas aux opérateurs agissant sur des espaces de dimension infinie. Le dernier chapitre reprend alors des résultats provenant d'une étude des réseaux de preuves et leur critère de correction datant de plus de trente ans. Ce travail est le point de départ de la *géométrie de l'interaction*, qui fait l'objet de la dernière partie de l'ouvrage et qui permet de passer outre les limitations apparues dans le chapitre précédent. L'auteur y expose comment les réseaux mènent à une interprétation des preuves par des permutations qui partage des points communs avec la *ludique*. En effet, les réseaux de preuves sont représentés par des unions disjointes de transpositions ; les autres permutations correspondent donc à la notion plus générale d'*épreuve*, et peuvent être comprises comme des *tests* traduisant les critères de correction.

**Geometry of Interaction.** La géométrie de l'interaction propose une interprétation des preuves/programmes par des opérateurs agissant sur un espace de Hilbert séparable de dimension infinie. Cette modélisation des preuves est dans la continuité du chapitre précédent, où l'interprétation des preuves par des permutations (finies) était insuffisante pour représenter les connecteurs exponentiels. Le premier chapitre de cette partie contient une exposition de l'*équation de rétroaction*, une équation fonctionnelle faisant intervenir deux opérateurs qui traduit la règle de coupure. La résolution de cette équation revient donc à éliminer les coupures dans une preuve ou, de manière équivalente, à *calculer* – exécuter un programme. Le résultat principal obtenu par l'auteur [14] et contenu dans ce chapitre, avec une nouvelle preuve, est l'existence et l'unicité d'une solution à cette équation, à condition que les opérateurs  $a, b$  considérés aient une norme inférieure ou égale à 1. Cette solution, noté  $\text{Ex}(a, b)$ , est alors un opérateur de norme au plus 1 dans l'algèbre de von Neumann engendrée par les deux opérateurs  $a, b$ . Cela permet d'envisager la boule unité d'une algèbre de von Neumann comme un *monde clos* pour l'interprétation des preuves/programmes : si  $a, b$  sont dans la boule unité de l'algèbre  $\mathfrak{N}$ , alors l'exécution  $\text{Ex}(a, b)$  existe et est un élément de la boule unité de  $\mathfrak{N}$ . Les deux chapitres suivants présentent alors la *géométrie de l'interaction hyperfinie* [17], l'un des résultats les plus récents de l'auteur. En fixant une algèbre de von Neumann (ici, le facteur hyperfini de type  $\text{II}_1$ ) et en restreignant l'interprétation des preuves à des opérateurs éléments de celle-ci, l'auteur y propose une reconstruction des connecteurs de la logique linéaire (comme c'était le cas en ludique) qui lui permet de recouvrir le système borné ELL. La notion de *test* entre permutations se traduit ici par le calcul d'une quantité faisant intervenir

le déterminant de Fuglede-Kadison. Cette notion explicite la condition de terminaison et permet de définir la notion de formule comme cela était fait en ludique.

**En guise de conclusion** Dans ce livre, les définitions, théorèmes et démonstrations ne sont pleinement formalisées que si cela est véritablement nécessaire à la compréhension du lecteur. Cette facilité de lecture est renforcée par de nombreuses explications intuitives et réflexions personnelles qui donnent le point de vue de l'auteur ; les commentaires sur les approches concurrentes sont souvent drôles, parfois piquants.

Il existe une version française de ce livre parue cinq ans auparavant [15, 16]. La version anglaise que nous présentons ici diffère de celle-ci grandement sur les derniers chapitres, en incluant une mise à jour bienvenue de ceux-ci. En effet, la partie *géométrie de l'interaction* de la version anglaise présente des résultats extrêmement récents qui, lorsque parut la version française, étaient encore en pleine évolution.

Il s'agit donc d'un livre de logique doublement original puisqu'il présente des résultats originaux d'une manière originale. L'un de ses intérêts est de poser des questions d'ordre épistémologique et de réintroduire la question des fondements qui est à l'origine même de la logique mathématique.

Surtout, cet ouvrage montrera au lecteur de la *Gazette* qu'il est possible de faire des mathématiques relativement standards sur ces objets inhabituels que sont formules et preuves formelles, mais aussi qu'une présentation de la logique mathématique et une étude des preuves formelles n'a pas à être plus formaliste qu'un autre traité de mathématiques. Les auteurs de cette recension espèrent que ces deux qualités, hélas peu courantes pour un ouvrage de logique, stimuleront l'intérêt des mathématiciens pour la logique mathématique.

## Références

- [1] Jean-Marc Andreoli. Logic programming with focusing proofs in linear logic. *Journal of Logic and Computation*, 1992.
- [2] Jean-Yves Girard. Normal functors, power series and  $\lambda$ -calculus. *Annals of Pure and Applied Logic*, 37(2) :129–177, February 1988.
- [3] Jean-Yves Girard. Une extension de l'interprétation de Gödel à l'analyse et son application : l'élimination des coupures dans l'analyse et la théorie des types. In Jens Erik Fenstad, editor, *Proceedings of the Second Scandinavian Logic Symposium*, volume 63 of *Studies in Logic and the Foundations of Mathematics*, 63–92, Amsterdam, 1971. North Holland.
- [4] Jean-Yves Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*. Thèse de doctorat d'état, Université Paris 7, 1972.
- [5] Jean-Yves Girard.  $\Pi_2^1$ -logic, part 1 : Dilators. *Annals of Mathematical Logic*, 21(2–3) :75 – 219, 1981.
- [6] Jean-Yves Girard. Une théorie géométrique des ordinaux. *Pour La Science, Edition Française de « Scientific American »*, 93, 1985. Repris dans “*Les mathématiques aujourd'hui*”, Belin, 97–108, 1986.
- [7] Jean-Yves Girard. The system F of variable types : Fifteen years later. *Theoretical Computer Science*, 45 :159–192, 1986.
- [8] Jean-Yves Girard. Linear logic. *Theoretical Computer Science*, 50(1) :1–102, 1987.

- [9] Jean-Yves Girard. La logique linéaire. *Pour La Science, Edition Française de "Scientific American"*, 150, April 1990.
- [10] Jean-Yves Girard. Towards a geometry of interaction. In *Categories in Logic and Computer Science-Boulder, June 1987*, volume 92 of *Contemporary Mathematics*, 68–109. AMS, 1990.
- [11] Jean-Yves Girard. A new constructive logic : classical logic. *Mathematical Structures in Computer Science*, 1(3) :255–296, 1991.
- [12] Jean-Yves Girard. Light linear logic. In *Selected Papers from the International Workshop on Logical and Computational Complexity, LCC '94*, 145–176, London, UK, 1995. Springer-Verlag.
- [13] Jean-Yves Girard. Locus solum : From the rules of logic to the logic of rules. *Mathematical Structures in Computer Science*, 11(3), 2001.
- [14] Jean-Yves Girard. Geometry of interaction IV : the feedback equation. In Stoltenberg-Hansen and Vaananen, editors, *Logic Colloquium '03*, 76–117, 2006.
- [15] Jean-Yves Girard. *Le point aveugle. Cours de logique. 1 : Vers la perfection. 1*. Paris : Hermann, Éditeurs des Sciences et des Arts. xvi, 280 p. , 2006.
- [16] Jean-Yves Girard. *Le point aveugle. Cours de logique. 2 : Vers l'imperfection*. Paris : Hermann, Éditeurs des Sciences et des Arts. xii, 281-567., 2007.
- [17] Jean-Yves Girard. Geometry of interaction V : Logic in the hyperfinite factor. *Theoretical Computer Science*, 412 :1860–1883, 2011.
- [18] Jean-Yves Girard, Yves Lafont, and Paul Taylor. *Proofs and Types*. Number 7 in Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1988.
- [19] William A. Howard. The formulae-as-types notion of construction. In J. Hindley and J. Seldin, editors, *To H.B. Curry : Essays on Combinatory Logic,  $\lambda$ -calculus and Formalism*, 479–490. Academic Press, 1980.
- [20] Jean-Louis Krivine. *Lambda Calcul – Types et Modèles*. Études et Recherches en Informatique. Masson, Paris, 1990.
- [21] Anne Troelstra and Dirk van Dalen. *Constructivism in Mathematics (vol. 1)*, volume 121 of *Studies in Logic and the Foundations of mathematics*. North-Holland, 1988.
- [22] Anne Troelstra and Dirk van Dalen. *Constructivism in Mathematics (vol. 2)*, volume 123 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, 1988.

Christian Retoré  
Université de Montpellier

Thomas Seiller  
IHÉS

