

# LIVRES

---

---

## Algorithms and Complexity

H. S. WILF

A K Peters Ltd., Natick, MA, 2002. (2<sup>nd</sup>e édition).

219 p. ISBN : 1-56881-178-0. \$39

---

Voilà un livre très déconcertant. Commençons par le contenu : c'est un premier cours d'algorithmique « pour mathématiciens », disons en dernière année de licence, mais qui pourra aussi bien inspirer des candidats à l'agrégation en quête de développements originaux. Le premier chapitre donne des rappels sur la croissance comparée des fonctions, les bases de numération, les opérations formelles sur les séries génératrices, la résolution de récurrences et de dénombrements simples, et le vocabulaire de la théorie des graphes. Malgré de curieux ménagements pour ne pas effrayer le lecteur, les énoncés sont élémentaires : écriture binaire des entiers, somme des termes d'une suite géométrique, théorème du binôme, estimation de  $\sum_{n=a}^b f(n)$  par une intégrale pour une fonction  $f$  monotone. . . Le deuxième chapitre introduit le concept de récursion et présente quelques algorithmes récursifs paradigmatiques : QuickSort, ensembles indépendants maximaux dans un graphe (analyse de l'algorithme récursif naïf), multiplication matricielle de Strassen, la FFT et son application à la multiplication rapide des polynômes. Le troisième est consacré au problème du flot maximal dans un graphe (algorithmes de Ford-Fulkerson et MPM). Le quatrième aux algorithmes arithmétiques : Euclide, pseudo-primalité, certificat de primalité (obtenu par factorisation de  $p - 1$  et preuve que  $\varphi(p) = p - 1$ ) et factorisation, ainsi que l'application attendue à la cryptographie (RSA). Le dernier est une introduction à la complexité, en particulier la classe NP et les problèmes NP-complets (machine de Turing, théorème de Cook, quelques réductions et algorithmes approchés).

Le livre s'articule sur la distinction entre usage polynomial et non polynomial de ressources, en général le temps ; les termes sont pris dans leur acception courante, *i.e.* en dehors de toute formalisation logique, y compris pour définir la machine de Turing. (Pour une première approche, c'est certainement une bonne chose.) Vu la variété de sujets traités, il est très court : sans prétention à la généralité, il présente une petite collection d'algorithmes intéressants et leur analyse, en se restreignant aux variantes les plus directes et aux preuves les plus élémentaires. Ainsi on multiplie des polynômes par FFT (implicitement à coefficients complexes, voire entiers), mais il n'est pas fait mention du problème d'interpolation général et le lecteur est renvoyé à la bibliographie pour la multiplication des entiers ; on multiplie des matrices mais on ne résout pas de système linéaire, etc. Les exercices sont nombreux (et faciles), avec solution, et les courtes bibliographies historiques de fin de chapitre sont soigneusement commentées. Le style est inhabituellement familier, ponctué de questions rhétoriques et de fausses naïvetés, cherchant continuellement à motiver l'étape à venir. Typiquement, pour annoncer le théorème de Cook (existence d'un

problème NP-complet) : « *Nous venons de discuter les avantages économiques de l'élevage des licornes sur celui des moutons. Si les licornes n'existent pas, la discussion est un peu ridicule.* »

Malheureusement, parfois cela ne va pas sans imprécisions : ainsi le premier exemple du texte énonce-t-il en substance que  $(\log x)/x \rightarrow 0$  quand  $x \rightarrow +\infty$  grâce à « la règle de l'Hospital », qui dit « on peut dériver numérateur et dénominateur et réessayer de faire tendre  $x \rightarrow +\infty$  » (des exemples sont donnés, mais on n'en saura pas plus). Toujours sur cette note négative, on rencontre de nombreuses typos ou remarques trompeuses, qui n'ont pas leur place dans une seconde édition. La plupart ne sont pas gênantes (erreurs d'indices ou de noms de variables, = à remplacer fréquemment par  $\neq$ , références décalées, problèmes T<sub>E</sub>X du type  $x \equiv 1 \pmod n$ , ...). Mais certaines le sont, en particulier dans le chapitre 4 : la section sur Euclide démontre que  $O(\log M)$  divisions euclidiennes suffisent à calculer le pgcd de deux entiers  $\leq M$  (ce qui est correct), dont on tire l'existence d'un algorithme en temps linéaire et l'équation conclusive 'Time = O(Bits)' (ce qui ne l'est pas). Autres exemples, la preuve de l'algorithme RSA écrit  $P^{\varphi(n)} \equiv 1 \pmod n$  pour tout  $P \in \mathbb{Z}/n\mathbb{Z}$ ; l'algorithme de Dixon est dit factoriser un entier  $n > 2$  en temps  $\exp((2 + o(1))\sqrt{\log \log n})$ . (La démonstration n'étant pas donnée, il n'est pas évident de remarquer l'erreur, ou de la corriger en remplaçant  $\log \log \log n$  par  $\log n \cdot \log \log n$ .)

Je recommande néanmoins cette introduction non-conformiste, pour le gros effort de motivation et les applications éclairantes, mais en conseillant une lecture critique du texte, et en le complétant par les premiers chapitres du classique de C. Papadimitriou (*Computational complexity*) pour une approche plus formelle des mêmes préoccupations.

Karim Belabas,  
Université de Paris-Sud Orsay

---

### La fonction zêta

J.-B. BOST, P. COLMEZ, P. BIANE  
Éditions de l'École Polytechnique, Palaiseau, 2003.  
206 p. ISBN : 2-7302-1011-3. 18 €

Issu de conférences données aux *Journées Mathématiques X-UPS* pour la formation continue des professeurs de classes préparatoires, ce volume de 193 pages se compose de trois textes indépendants, autour du thème de la fonction zêta de Riemann, au niveau du master.

Le texte de Bost, *Le théorème des nombres premiers* (35 pages, dont 3 pages pour la reproduction de la note d'Hadamard de 1896) démontre le dit théorème, sous la forme  $\pi(x) \sim x/\log x$ . L'argument, dû à Kahane et très clairement détaillé dans le texte, introduit de façon amusante la non-annulation de  $\zeta$  sur  $\Re s = 1$  : la fonction  $\ell(t) := \sum_p p^{-1-2\pi it}$ , issue du logarithme du produit eulérien pour  $\zeta(1 + 2\pi it)$ , a une singularité logarithmique en 0 associée au pôle simple de  $\zeta$  en 1, et des singularités logarithmiques aux zéros éventuels de  $\zeta(1 + 2\pi it)$ . C'est aussi la transformée de Fourier de la distribution  $\sum_p \delta_{\log p} p^{-1}$ . En appliquant ceci à des fonctions de type positif convenables, on voit que ces singularités logarithmiques

n'existent pas. C'est en substance le même argument que l'identité «miracle» de la Vallée-Poussin  $3 + 4 \cos t + \cos 2t \geq 0$ , du point de vue de l'analyse de Fourier.

Le texte de Colmez *L'arithmétique de la fonction zêta* est un tour d'horizon de grande ampleur (128 pages !) qui se décompose en deux groupes de trois chapitres, respectivement consacrés à la théorie complexe et à la théorie  $p$ -adique.

Le premier chapitre traite du prolongement analytique et de l'équation fonctionnelle de la fonction zêta de Riemann (puis des fonctions  $L$  de Dirichlet et de la fonction zêta de Dedekind), et de ses valeurs spéciales aux entiers : des résultats d'Euler aux polylogarithmes, en passant par le volume de  $SL_n(\mathbb{R})/SL_n(\mathbb{Z})$ , pour aboutir à la conjecture de Zagier vue comme généralisation de la formule du nombre de classe de Dirichlet (les liens avec la  $K$ -théorie algébrique sont évoqués mais pas développés). Le chapitre 2 est consacré aux propriétés diophantiennes des valeurs de  $\zeta$ , en particulier le théorème de Rivoal sur l'irrationalité d'une infinité de ses valeurs aux entiers impairs, et à une étude des relations entre nombres polyzêtas. Le chapitre 3 commence par une introduction aux formes modulaires pour  $SL_2(\mathbb{Z})$ , se poursuit par une nouvelle démonstration du prolongement analytique, de l'équation fonctionnelle de  $\zeta$  (la troisième depuis le début du texte) et de la non-annulation sur la droite  $\Re s = 1$  à l'aide de la série d'Eisenstein non-holomorphe  $\sum'_{m,n} y^s / |m+nz|^2$ . Viennent ensuite les opérateurs de Hecke, la théorie en niveau supérieur, quelques pages sur la fonction zêta de Hasse-Weil (associée à une  $\mathbb{Z}$ -algèbre de type fini), les «conjectures de Weil», et le chapitre se termine sur quelques cas particuliers célèbres (conjecture de Shimura-Taniyama-Weil, théorème de Fermat-Wiles). Le chapitre 4 commence par des généralités sur les corps complets ultramétriques, construit les nombres  $p$ -adiques puis le corps  $\mathbb{C}_p$ , et introduit le logarithme et l'exponentielle ( $p$ -adiques). Le chapitre 5 introduit les espaces de Banach  $p$ -adiques, puis les mesures et les distributions sur  $\mathbb{Z}_p$ , notamment plusieurs caractérisations des distributions tempérées. Finalement le dernier chapitre utilise ce matériel pour démontrer les congruences de Kummer, construire la fonction  $\zeta$  de Kubota-Leopoldt et la fonction  $L$   $p$ -adique associée à un caractère de Dirichlet, et introduire le théorème de Mazur-Wiles.

Comme le dit l'auteur, «tout ce qui est démontrable est démontré», souvent avec plusieurs variantes. Quelques preuves, «très loin de tenir dans la marge de ces pages», sont tout de même omises. Le matériel est souvent classique mais parsemé de points de vue éclairants, de questions ouvertes, et développé bien au delà de ce que l'on pense trouver dans un texte de ce niveau. L'ensemble est clair, vivant. C'est une belle introduction à l'arithmétique et on regrette que la bibliographie soit si sommaire.

Le texte de Biane *La fonction zêta de Riemann et les probabilités* (29 pages) se concentre sur deux exemples où des idées probabilistes interviennent dans la théorie de la fonction zêta. Ce texte est plus allusif; une grande partie des résultats est seulement esquissée, voire admise.

Le premier exemple, inspiré de la théorie des matrices aléatoires, est largement conjectural, et ses généralisations font l'objet de recherches actives. À partir du modèle du Gaussian Unitary Ensemble (qui suppose l'hypothèse de Riemann et prédit que les zéros critiques de  $\zeta$  suivent la même loi que les valeurs propres de matrices hermitiennes de grande taille, choisies suivant une loi gaussienne), il dérive la conjecture de corrélation de paires (de zéros critiques) de Montgomery,

et une conjecture de Keating et Snaith sur les moments de  $\zeta$  sur la droite critique  $\Re s = 1/2$ .

Le deuxième exemple est plus anecdotique, mais donne un point de vue élégant. Il réinterprète le prolongement analytique et l'équation fonctionnelle de  $\zeta$  en terme d'excursions browniennes. On étudie d'abord un modèle discret : dans un jeu équilibré de pile ou face où chaque partie (indépendante) se solde par le gain ou la perte d'une unité, soit  $T_1$  le premier temps de retour à 0 du gain total du joueur 1 ( $T_1$  est presque sûrement fini, et pair dans ce cas), et  $M_1$  son gain maximal jusqu'à ce moment. On obtient deux expressions explicites de la probabilité que  $M_1 < y\sqrt{n}$ , conditionnellement à  $T_1 = 2n$ , par dénombrement, puis par diagonalisation d'une matrice de transition. Elle tend vers la valeur d'une série théta en  $y$  quand  $n \rightarrow \infty$ , dont on obtient de ce fait l'équation fonctionnelle sans formule de Poisson ; la transformation de Mellin habituelle assure le passage à  $\zeta$ . Finalement, après une rapide introduction au mouvement brownien, le texte décrit un deuxième modèle continu, la norme euclidienne d'un mouvement brownien de dimension 3, dont la loi du maximum a pour densité de probabilité cette même série théta. En considérant la loi du couple  $(M, T)$ , où  $M$  est le maximum de l'excursion et  $T$  le temps de retour en 0, l'équation fonctionnelle de  $\zeta$  devient l'égalité des lois de deux variables aléatoires naturelles.

La conjonction de ces trois points de vue produit un beau livre, dont l'arithméticien que je suis a trouvé la lecture fort agréable.

Karim Belabas,  
Université de Paris-Sud Orsay

---

### Basic Hypergeometric Series

GEORGE GASPER, MIZAN RAHMAN

Encyclopaedia of Mathematics and its Applications (N° 96), Second edition,  
Cambridge University Press, 2004. xxvi + 428 p. ISBN : 0-521-83357-4. 120 €

---

Divers livres dans divers domaines des mathématiques ont acquis par l'affection et le respect de leurs lecteurs le nom de « bible » ; parmi eux, en bonne place, *le Gasper-Rahman* (je le nommerai **GR** dans la suite). Voici quelques unes des qualités objectives qui légitiment ce titre :

- 1) une quantité énorme de beaux énoncés, principalement des formules, probablement tous essentiellement justes et certainement presque tous tout à fait justes<sup>1</sup> ; le tout, accompagné d'explications fiables et souvent de preuves claires ;
- 2) encore d'autres énoncés et d'autres formules, répartis dans des centaines d'exercices ;
- 3) de très nombreuses références dans la bibliographie et de nombreuses notes bibliographiques et historiques à la fin de chaque chapitre ;
- 4) un formulaire résumé exhaustif en appendice ;
- 5) une table des matières rationnelle ;
- 6) un index complet et efficace.

---

<sup>1</sup> Des sites webs cités dans la préface tiennent le lecteur au courant des erreurs trouvées.

Quant aux qualités subjectives, chaleureusement évoquées dans l'avant-propos de Richard Askey, elles convaincront sans peine ceux qui sont déjà infectés par la *q-disease* et en contamineront bien d'autres. Une deuxième édition de ce livre (la première datait de 1990) vient de paraître, augmentée d'environ 50% : elle est passée de 287 à 428 pages ; on dira plus loin où s'est concentrée toute cette bonne graisse.

Le domaine du *q*-calcul remonte à Euler, Gauss, Heine, Jacobi, Ramanujan... Voir là-dessus, par exemple, **GR** lui-même (*i.e* le Gasper-Rahman), ou bien un article de survol paru il y a deux ans dans la *Gazette* [DVRSZ03]. Quelques exemples donneront une idée de son parfum. D'abord, les dénombrements de partitions et les identités arithmético-combinatoires [And86] ; ces dernières ont perdu un peu de leur fraîcheur naïve (mais gagné en profondeur) lorsqu'elles ont été reliées au jardin modulaire par Ramanujan, Hardy... jusqu'à Deligne (conjecture de Ramanujan).

Ensuite, les *q*-analogies ; l'une des plus anciennes est le théorème *q*-binomial, raconté dans [DVRSZ03]. La plupart d'entre elles disent que, lorsque  $q \rightarrow 1$ , une formule du *q*-calcul dégénère (par passage à la limite de ses coefficients) en une formule concernant des équations différentielles ou des fonctions spéciales. Notons que le calcul par Fermat de l'aire bordée par une parabole à l'aide de suites géométriques équivaut à la dégénérescence de la *q*-intégrale de Jackson (décrite dans **GR**, voir aussi [KC02]) en une intégrale de Riemann. Fermat nomme *adéquation* la substitution de *q* par 1, qu'il considère plus comme une spécialisation que comme un passage à la limite. À titre de curiosité, on peut également citer la formule donnant le nombre de sous-espaces de dimension donnée d'un espace vectoriel de dimension finie sur un corps fini. Dans le cas d'un corps à un élément (!), cette formule donne le nombre de parties de cardinal donné d'un ensemble fini.

*Last but not least*, la fonction (ou la série) hypergéométrique *basique* (de base *q*) introduite par Heine en 1848 :

$${}_2\Phi_1(a, b, c; q, x) = \sum_{n \geq 0} \frac{(a; q)_n (b; q)_n}{(c; q)_n (q; q)_n} x^n,$$

où l'on a posé, pour  $q \in \mathbf{C}^*$ ,  $|q| < 1$  et  $n \in \mathbf{N}$  :  $(a; q)_n = \prod_{i=0}^{n-1} (1 - aq^i)$ . Pour voir la *q*-analogie, on posera  $a = q^\alpha$ , etc... avant de faire tendre *q* vers 1.

Les aspects purement formels (algébriques) du *q*-calcul sont résumés dans [KC02], et ce n'est sans doute pas un hasard si la recension [Kas03] de ce livre pour la *Gazette* a été écrite par un spécialiste des groupes quantiques.

L'équivalent pour les fonctions hypergéométriques basiques de la théorie « classique », telle qu'elle est résumée par exemple par Goursat ou par Whittaker et Watson, constitue le contenu de **GR** et de son rival [Fin88] (qui est toutefois beaucoup moins complet). Il offre un aspect beaucoup plus calculatoire, en partie à cause de la variable supplémentaire *q*, mais surtout parce que *les fonctions hypergéométriques basiques admettent un prolongement méromorphe uniforme au plan complexe*. Ceci semble interdire la transposition du point de vue de Riemann, dont on sait pourtant l'importance pour la théorie moderne des fonctions ! On y reviendra.

Les 8 chapitres de la version classique (de 1990) de **GR** tournaient autour de 3 thèmes principaux :

1) formules de sommation, de contiguïté... bien plus intriquées que dans la théorie classique ;

2) représentations intégrales dans la lignée de Barnes, Mellin, Watson et formules de connexion ;

3) polynômes orthogonaux.

Ces 8 chapitres n'ont pas substantiellement évolué dans la nouvelle édition, sauf peut-être les notes historiques de fin de chapitre ; au total, ils ont gagné 28 pages. Il s'y est ajouté un chapitre 9 (de 23 pages) qui prolonge le thème des polynômes orthogonaux ; et surtout un chapitre 10 (de 20 pages) et un chapitre 11 (de 49 pages) abordant respectivement les fonctions de plusieurs variables et les fonctions hypergéométriques dites elliptiques, etc... Ces ajouts sont probablement motivés par des développements importants dûs notamment à « l'école russe » autour de l'équation KDV discrète, voir en particulier [TV97].

La bibliographie elle-même est passée de 28 à 48 pages, grâce à un considérable effort de mise à jour. Le choix de ces ajouts présente des aspects déconcertants. La bibliographie cite maintenant les résultats importants de L. Di Vizio, ainsi qu'un article de l'auteur de cette recension (= JS), bien que ces travaux soient assez éloignés de l'esprit du livre ; et elle omet totalement les travaux de Y. André, J.-P. Bézivin, B. Grammatikos et A. Ramani, J.-P. Ramis, C. Zhang ainsi que le livre de M. van der Put et M. Singer (par exemple) ; pourtant certains de ces auteurs sont de vrais experts de fonctions  $q$ -spéciales !

La raison indirecte de ces bizarreries tient sans doute à l'orientation résolument formaliste du livre (dans le sens où Hardy traitait Ramanujan de formaliste). Ce parti-pris, conscient ou non, se manifeste par les absences suivantes.

1) Le phénomène omniprésent de dégénérescence vers des formules classiques lorsque  $q \rightarrow 1$  (ou  $q$ -analogie) n'est pas vraiment expliqué : on dit parfois que les séries tendent terme à terme vers des séries classiques, rarement que les fonctions le font et encore plus rarement pourquoi ; et souvent en supposant inutilement que  $q$  est réel. Ce n'est pas vraiment de l'analyse !

2) On ne parle quasiment jamais d'équation fonctionnelle ; imaginez un livre sur la fonction hypergéométrique sans équation différentielle !

La raison évidente est que la notion de prolongement analytique n'est pas directement opérante ici. Cependant, Birkhoff a montré en 1913 comment formuler une correspondance de Riemann-Hilbert dans ce cas. *Mais Birkhoff n'est pas cité dans ce livre.* Pour un point de vue motivé sur ces points essentiels et les travaux récents auxquels ils ont donné lieu, je suggère donc au lecteur intéressé l'article de survol [DVRSZ03] et sa bibliographie.

Mais, bien sûr, ce n'était pas l'objet du Gasper-Rahman, et cette critique n'affectera pas le jugement final : c'est un livre extraordinaire, une intarissable source de plaisir et un beau cadeau pour vous-même ou un(e) collègue ami(e).

## Références

- [And86] G. E. ANDREWS – *q-series : their development and applications in analysis, number theory, combinatorics, physics and computer algebra*, CBMS Regional Conference lecture Series in Mathematics, vol. 66, Amer. Math. Soc., Providence, 1986.
- [DVRSZ03] L. DI VIZIO, J.-P. RAMIS, J. SAULOY & C. ZHANG – « Équations aux  $q$ -différences », *Gazette des Mathématiciens* **96** (2003), p. 20–49.

- [Fin88] N. FINE – « Basic hypergeometric series and applications », *Math. Surv.* **27** (1988), Amer. Math. Soc., Providence.
- [Kas03] C. KASSEL – « Recension de Quantum calculus », *Gazette des Mathématiciens* **96** (2003), p. 123–125.
- [KC02] V. KAC & P. CHEUNG – *Quantum calculus*, Springer-Verlag, 2002.
- [TV97] V. TARASOV & A. VARCHENKO – *Geometry of q-hypergeometric functions, quantum affine algebras and elliptic quantum groups*, Astérisque, vol. 246, Soc. Math. Fr., 1997.

Jacques Sauloy,  
Université Paul Sabatier

---

### Automorphic Pseudodifferential Analysis and Higher Level Weyl Calculi

ANDRÉ UNTERBERGER

Progress in Mathematics, vol. 209, Birkhäuser Verlag, Basel, 2003.

viii + 246 p. ISBN : 3-7643-6909-4. \$ 114

---

Comme l'indique le titre, ce livre met en rapport l'analyse des fonctions automorphes et le calcul pseudo-différentiel — ou plutôt la description qu'avait donnée H. Weyl des opérateurs.

Décrivons-en d'abord les ingrédients (j'utilise ci-dessous des notations simplifiées qui ne sont pas celles du livre mais suffiront pour la description un peu sommaire ci-dessous — les notations d'Unterberger sont décrites minutieusement au cours du livre, et mieux adaptées à son contenu, mais plus longues à décrire).

**1. Fonctions modulaires.** Soit  $\mathbb{H}$  le demi-plan de Poincaré, ensemble des  $z = x + iy \in \mathbb{C}$  avec  $y > 0$ .  $\mathbb{H}$  est muni de la métrique  $ds^2 = y^{-2}(dx^2 + dy^2)$  et du laplacien  $\Delta = y^2(\partial_x^2 + \partial_y^2)$ . Le groupe  $SL(2, \mathbb{R})$  opère sur  $\mathbb{H} : z \mapsto \frac{az+b}{cz+d}$ .

Une fonction automorphe est une fonction sur  $\mathbb{H}$  invariante par le sous-groupe  $\Gamma = SL(2, \mathbb{Z})$  (pas forcément holomorphe). Une forme automorphe est une fonction automorphe qui est en plus fonction propre de  $\Delta$  (le cas  $SL(2, \mathbb{Z}) \subset SL(2, \mathbb{R})$  est le seul examiné dans ce livre, sauf au chapitre 4 où est indiqué comment les constructions du livre peuvent se généraliser à des sous groupes de congruence).

Un aspect important de l'analyse automorphe est l'étude de la décomposition spectrale du Laplacien  $\Delta$  dans l'espace  $L^2(\Gamma \backslash \mathbb{H})$  des fonctions automorphes de carré sommable : on a  $L^2(\Gamma \backslash \mathbb{H}) = S \oplus C$  où  $S$  correspond à la partie continue du spectre, et est bien décrit au moyen des séries d'Eisenstein ;  $C$  correspond à la partie discrète, et a une base orthonormale formée de fonctions propres qui sont des formes cuspidales, i.e. dont la série de Fourier en  $x : f = \sum f_k(y)e^{2i\pi kx}$  ne contient pas de terme constant ( $k=0$ ). Les valeurs propres de  $\Delta$  forment une suite tendant vers  $-\infty$ , mais on ne sait pas si elles sont toutes simples. On améliore la présentation en demandant à ces formes d'être aussi fonctions propres des opérateurs de Hecke (la série d'Eisenstein  $E_s$  est la somme des transformées distinctes de  $y^s$  par le groupe  $\Gamma : E_s(z) = \frac{1}{2} \sum_{(m,n)=1} (y/|mz+n|^2)^s$  ; elle converge pour  $\text{Res} > 1$  avec un prolongement méromorphe en  $s$  ; la partie continue de la décomposition spectrale de  $\Delta$  se décrit au moyen des  $E_{\frac{1+i\lambda}{2}}$ ).

**2. Groupe métaplectique.** Soit  $G$  le groupe des transformations unitaires de  $L^2(\mathbb{R})$  qui préserve l'ensemble  $V$  des opérateurs différentiels du premier ordre de la forme  $aD + bX$  ( $D = \frac{1}{i} \frac{\partial}{\partial x}$ ) : c'est un groupe de Lie, qui a pour l'algèbre de Lie

l'ensemble des opérateurs du second ordre  $i(\alpha D^2 + \beta(xD + Dx) + \gamma x^2 + \delta)$  ( $\alpha, \beta, \gamma, \delta$  réels) ( $G$  opère aussi sur l'espace de Schwartz  $\mathcal{S}$  des fonctions à décroissance rapide, et sur le dual  $\mathcal{S}'$ ).

L'application  $A \in G \mapsto \text{Ad}_{A|_V}$  ( $\text{Ad}(L) = ALA^{-1}$ ) est une surjection  $G \rightarrow \text{Sp}(V) = \text{SL}(V) \simeq \text{SL}(2, \mathbb{R})$  ( $\text{Ad}A$  préserve les commutateurs, qui définissent la structure symplectique ou  $\text{SL}$  de  $V$ ). Le sous-groupe (fermé) engendré par les opérateurs ci-dessus « sans terme constant » ( $\gamma = 0$ ) est le groupe métaplectique, revêtement à deux feuillets de  $\text{SL}(V)$ .

**3. Calcul de Weyl.** Il peut être décrit comme suit : à une fonction  $h(\xi, x)$  sur  $\mathbb{R}^2$  (symbole), on associe l'opérateur  $Op(h)$  défini par

$$(Op(h)u)(x) = \int h\left(\frac{x+y}{2}, \eta\right) u(y) e^{-i(x-y)\eta} dy d\eta \quad \text{pour } u \in \mathcal{S}(\mathbb{R})$$

En fait tout opérateur linéaire continu  $\mathcal{S} \rightarrow \mathcal{S}'$  est de la forme  $Op(h)$  avec  $h$  distribution tempérée sur  $\mathbb{R}^2$ .

Cette façon de repérer les opérateurs a la vertu suivante : si  $A$  est un opérateur métaplectique ( $A \in G$ ),  $a = \text{Ad}(A)$ , on a  $AOp(h)A^{-1} = Op(h \circ a^{-1})$ .

En particulier si  $\Im z > 0$ , on note  $e_z$  la fonction Gaussienne  $e_z(x) = e^{iz\frac{x^2}{2}}$ , solution de l'équation différentielle  $(D - zx)e_z = 0$ , de symbole  $\xi - zx : G$  permute les fonctions  $ce_z$  ( $c = \text{constante}$ ). Plus précisément si  $\text{Ad}_{A|_V}$  induit sur  $V$  la transformation  $\xi \mapsto a\xi + bx, x \mapsto c\xi + dx$ ,  $Ae_z$  est proportionnel à  $e_{z'}, z' = (az + b)(cz + d)^{-1}$ .

Une distribution automorphe est une distribution  $h$  invariante par le groupe  $\text{SL}(2, \mathbb{Z})$ . Il revient au même de dire que  $Op(h)$  est invariante par les opérateurs métaplectiques  $A$  tels que  $\text{Ad}_{A|_V} \in \text{SL}(2, \mathbb{Z})$ .

Si  $h$  est invariante par  $\text{SL}(2, \mathbb{Z})$  la fonction  $F(z) = \|u_z\|^{-2} \langle u_z | Op(h)u_z \rangle$  l'est aussi. Il est utile de lui adjoindre la fonction  $F^1(z) = \|xu_z\|^{-2} \langle xu_z | Op(h).xu_z \rangle$  : l'application  $h \mapsto (F, F^1)$  est injective (elle n'est pas surjective — ne serait-ce que parce que  $F$  et  $F^{-1}$  sont toujours des fonctions analytiques-réelles).

Dans cette correspondance le Laplacien  $\Delta$  de  $\mathbb{H}$  (le quart de l'opérateur de Casimir) correspond à  $\frac{Eu^2 - 1}{4}$  où  $Eu$  est l'opérateur d'Euler :  $Eu = \xi \frac{\partial}{\partial \xi} + x \frac{\partial}{\partial x} + 1$ , générateur du groupe des homothéties sur les demi-densités sur  $\mathbb{R}^2$ . L'étude de la décomposition en fonctions propres des fonctions automorphes est ainsi ramenée à l'étude de la décomposition en distributions homogènes des distributions automorphes.

Cette étude est faite de façon minutieuse dans le premier chapitre, où est établi un dictionnaire entre les deux situations. En particulier sont introduites les distributions d'Eisenstein, correspondant aux séries d'Eisenstein, celles qui correspondent aux formes cuspidales, ainsi que les opérateurs (sur les distributions automorphes sur  $\mathbb{R}^2$ ) correspondant aux opérateurs de Hecke.

La « distribution de Bezout »  $\mathcal{B}$  joue un rôle important (de série génératrice). Formellement c'est la somme des transformées distinctes par  $\text{SL}(2, \mathbb{Z})$  de la distribution  $e^{2i\pi x} \delta(\xi - 1)$  (en fait seule  $Eu\mathcal{B}$  est bien définie, ainsi que les distributions  $\mathcal{B}^\ell$  qui en dérivent :  $\mathcal{B}^\ell = \prod_{k=0}^{\ell-1} (k^2 - \frac{Eu^2}{4})$ , qui servent dans les « calculs de niveaux supérieurs » dans la suite) ; sa décomposition contient toutes les composantes utiles.

Une fois ces prémices établies, le livre se consacre principalement au problème suivant : construire un produit (non commutatif) sur l'ensemble des (couples de) fonctions automorphes dérivant du produit défini par la composition des opérateurs — ou au moins construire la table de multiplication pour les formes élémentaires (distributions d'Eisenstein, distributions cuspidales). Un tel produit bien maîtrisé fournirait un moyen intéressant pour générer de nouvelles formes modulaires à partir d'anciennes. C'est un problème compliqué parce que le composé de deux opérateurs automorphes n'est en général pas défini. Pour pallier cela Unterberger construit des substituts au calcul de Weyl : calculs de plus hauts niveaux où on modifie les opérateurs  $Op(h)$  en  $Op^p(h)$  opérant sur le sous-espace  $S_p = t^p S$  des fonctions nulles à l'ordre  $p$ . Le résultat principal (« *main formula* »), décrit le produit de deux distributions (opérateurs) d'Eisenstein en termes de la distribution de Bezout et des opérateurs de Hecke ; il est annoncé au chapitre 1 et démontré plus précisément dans la suite du livre.

Ce livre contient une foison d'idées et de résultats ; il suggère aussi beaucoup de problèmes ouverts, à commencer par une meilleure compréhension de ces produits, et la généralisation à d'autres sous-groupes que  $SL(2, \mathbb{Z})$  ou d'autres groupes que  $SL(2, \mathbb{R})$ . Il ne peut qu'être recommandé aux doctorants et spécialistes qui désirent faire une étude approfondie de l'analyse des fonctions et distributions automorphes.

L. Boutet de Monvel,  
Université Pierre et Marie Curie, Paris VI

---

### Hecke Algebras with Unequal Parameters

GEORGE LUSZTIG

CRM Monograph Series 18, American Mathematical Society, Providence, RI,  
2003. vi+136 p. ISBN : 0-8218-3356-1. \$39

---

Ce livre, composé de 27 courts chapitres, débute par les définitions des concepts de base, résume l'essentiel des connaissances actuelles sur le sujet et introduit un grand nombre de résultats nouveaux. Le lecteur y trouvera des calculs explicites, de nombreux exemples, des théorèmes généraux ainsi que nombre de questions ouvertes et de conjectures.

Les *algèbres de Hecke* interviennent comme algèbres d'endomorphismes de représentations de groupes induites par des représentations de sous-groupes. L'auteur s'intéresse dans le livre à un type particulier de telles algèbres, celles apparaissant dans la théorie des représentations des groupes algébriques réductifs sur les corps finis ou  $p$ -adiques. Ces algèbres de Hecke sont des spécialisations de certaines algèbres de Hecke génériques (dites de *Hecke-Iwahori*), lesquelles peuvent être définies, sans référence aux groupes algébriques, par des générateurs et des relations explicites en termes d'un *groupe de Coxeter pondéré*.

Expliquons ce dont il s'agit. Soient  $S$  un ensemble fini et  $(m_{s,s'})_{(s,s') \in S \times S}$  une matrice à coefficients dans  $\mathbb{N} \cup \{\infty\}$ , satisfaisant  $m_{s,s} = 1$  pour tout  $s \in S$  et  $m_{s,s'} = m_{s',s} \geq 2$  pour tout  $(s, s')$  tel que  $s \neq s'$ . Nous supposons les relations suivantes satisfaites :  $(ss')^{m_{s,s'}} = 1$ , pour tout couple  $(s, s')$  d'éléments de  $S$  tel que  $m_{s,s'}$  soit fini. Le groupe  $W$  engendré par  $S$  est appelé un *groupe de Coxeter*. Pour

tout élément  $w$  de  $W$ , notons  $\ell(w)$  le plus petit entier  $i$  tel que  $w = s_1 s_2 \cdots s_i$ , avec  $s_1, s_2, \dots, s_i$  dans  $S$ . On dit alors que  $w = s_1 s_2 \cdots s_i$  est une *expression réduite* de  $w$  et l'entier  $\ell(w)$  est appelé la *longueur* de  $w$ . Les deux premiers chapitres décrivent des propriétés de ces groupes.

Un *groupe de Coxeter pondéré* est la donnée d'un groupe de Coxeter  $W$  et d'une application  $L$  de  $W$  dans  $\mathbb{Z}$  vérifiant  $L(w w') = L(w) + L(w')$ , pour tout couple  $(w, w')$  d'éléments de  $W$  tels que  $\ell(w w') = \ell(w) + \ell(w')$ . La *fonction poids*  $L$  est déterminée par ses valeurs sur les éléments de  $S$ , lesquelles sont seulement soumises à la condition  $L(s) = L(s')$  pour tout couple  $(s, s')$  d'éléments distincts tels que  $m_{s,s'}$  soit fini et impair. La fonction longueur  $\ell$  est clairement un exemple de fonction poids.

Soit  $v$  une indéterminée. Notons  $\mathcal{A}$  l'anneau  $\mathbb{Z}[v, v^{-1}]$ , et, pour tout élément  $s$  de  $S$ , posons  $v_s := v^{L(s)}$ . Soit  $\mathcal{H}$  l'*algèbre de Hecke-Iwahori générique* de  $(W, L)$ , i.e., la  $\mathcal{A}$ -algèbre définie par les générateurs  $T_s$  ( $s \in S$ ), avec les *relations quadratiques*

$$(T_s - v_s)(T_s + v_s^{-1}) = 0 \text{ pour tout } s \in S,$$

et les *relations de tresses*

$$\underbrace{T_s T_{s'} T_s \cdots}_{m_{s,s'} \text{ facteurs}} = \underbrace{T_{s'} T_s T_{s'} \cdots}_{m_{s,s'} \text{ facteurs}},$$

pour tout couple  $(s, s')$  d'éléments distincts de  $S$  tel que  $m_{s,s'} < \infty$ . Elle admet  $T_1$  comme élément unité. Pour tout élément  $w$  de  $W$ , on définit  $T_w \in \mathcal{H}$  par  $T_w := T_{s_1} T_{s_2} \cdots T_{s_i}$ , où  $w = s_1 s_2 \cdots s_i$  est une expression réduite de  $w$  (l'élément  $T_w$  est bien défini, car indépendant du choix de la décomposition réduite de  $w$ ). Les  $v_s$  sont appelés les *paramètres* de  $\mathcal{H}$ . Un cas particulièrement simple est celui où la fonction poids  $L$  est constante sur les éléments de  $S$ , ce cas est connu sous le nom de *cas de paramètres égaux*.

Des définitions ci-dessus, il résulte que

$$T_s T_w = \begin{cases} T_{sw} & \text{si } \ell(sw) = \ell(w) + 1, \\ T_{sw} + (v_s - v_s^{-1}) T_w & \text{si } \ell(sw) = \ell(w) - 1. \end{cases}$$

En particulier, le sous- $\mathcal{A}$ -module de  $\mathcal{H}$  engendré par  $\{T_w : w \in W\}$  est un idéal à gauche de  $\mathcal{H}$ . Comme il contient  $T_1$ , il est donc égal à  $\mathcal{H}$ . Autrement dit l'ensemble  $\{T_w : w \in W\}$  engendre  $\mathcal{H}$  en tant que  $\mathcal{A}$ -module. La démonstration du fait que  $(T_w)_{w \in W}$  est une  $\mathcal{A}$ -base de  $\mathcal{H}$  est l'objet du court chapitre 3.

Pour tout  $s$  dans  $S$ , l'élément  $T_s$  est inversible dans  $\mathcal{H}$ , d'inverse  $T_s^{-1} = T_s - (v_s - v_s^{-1})$ . Il s'ensuit que  $T_w$  est inversible pour tout  $w \in W$  : si  $w = s_1 s_2 \cdots s_i$  est une expression réduite de  $w$ ,  $T_w^{-1} = T_{s_i}^{-1} \cdots T_{s_2}^{-1} T_{s_1}^{-1}$ . Soit  $\bar{\cdot} : \mathcal{A} \rightarrow \mathcal{A}$  l'involution d'anneau qui envoie  $v^n$  sur  $v^{-n}$  pour tout  $n \in \mathbb{Z}$ . Il existe un unique homomorphisme d'anneaux  $\bar{\cdot} : \mathcal{H} \rightarrow \mathcal{H}$ ,  $\mathcal{A}$ -semi-linéaire relativement à  $\bar{\cdot} : \mathcal{A} \rightarrow \mathcal{A}$  et vérifiant  $\bar{T}_s = T_s^{-1}$  pour tout  $s \in S$ . Cet homomorphisme est involutif et envoie  $T_w$  sur  $T_{w^{-1}}^{-1}$  pour tout  $w \in W$ . L'élément  $\bar{T}_w$  s'écrit  $\bar{T}_w = \sum_{y \in W} r_{y,w} T_y$ , où  $r_{y,w} \in \mathcal{A}$  est non nul pour un nombre fini de  $y$  seulement. Le chapitre 4 décrit des propriétés des  $r_{y,w}$ .

Dans le cas de paramètres égaux, l'on dispose de la théorie de Kazhdan-Lusztig qui définit une nouvelle base  $(c_w)_{w \in W}$  de  $\mathcal{H}$  ainsi que des partitions de  $W$  en

cellules à gauche, cellules à droite et cellules bilatères, respectivement. Le but du livre est d'étendre cette théorie autant qu'il est possible au cas général (de paramètres non nécessairement égaux).

Posons  $\mathcal{A}_{\leq 0} := \bigoplus_{m \leq 0} \mathbb{Z}v^m$  et  $\mathcal{H}_{\leq 0} := \bigoplus_w \mathcal{A}_{\leq 0} T_w$ . Le chapitre 5 démontre l'existence, pour tout  $w \in W$ , d'un unique élément  $c_w$  de  $\mathcal{H}_{\leq 0}$  invariant sous  $\bar{\cdot} : \mathcal{H} \rightarrow \mathcal{H}$  tel que  $c_w$  soit égal à  $T_w$  modulo  $\bigoplus_w \mathcal{A}_{< 0} T_w$ . Les  $c_w$  ( $w \in W$ ) forment une  $\mathcal{A}_{\leq 0}$ -base de  $\mathcal{H}_{\leq 0}$  et une  $\mathcal{A}$ -base de  $\mathcal{H}$ . L'élément  $c_w$  s'écrit

$$c_w = \sum_{y \in W} p_{y,w} T_y$$

dans la base des  $T_w$ , avec  $p_{y,w} \in \mathcal{A}_{\leq 0}$ ,  $p_{w,w} = 1$ , et  $p_{y,w} \neq 0$  implique  $y \leq w$  (où  $\leq$  est la relation d'ordre usuelle sur  $W$ ). Les  $p_{y,w}$  jouent le rôle des polynômes de Kazhdan-Lusztig. Le chapitre 6 étudie les multiplications à gauche et à droite de  $c_w$  ( $w \in W$ ) par  $c_s$  ( $s \in S$ ).

Pour tout couple  $(x, y)$  d'éléments de  $W$ , notons  $h_{x,y,w}$  le coefficient du produit  $c_x c_y$  dans la base des  $c_w$  et  $f_{x,y,w}$  celui de  $T_x T_y$  dans la base des  $T_w$  :  $c_x c_y = \sum_{w \in W} h_{x,y,w} c_w$  et  $T_x T_y = \sum_{w \in W} f_{x,y,w} T_w$ . Modulo l'hypothèse que  $(W, L)$  est borné par un entier  $N$  (i.e., l'existence d'un entier  $N$  tel que  $v^{-N} f_{x,y,w} \in \mathcal{A}_{\leq 0}$  pour tout  $(x, y, w) \in W^3$ ), l'auteur montre que, pour tout  $w \in W$ , il existe un unique entier  $a(z) \in [0, n]$  tel que  $h_{x,y,w} \in v^{a(w)} \mathbb{Z}[v^{-1}]$  pour tout  $(x, y) \in W^2$ , et tel qu'il existe  $(x, y) \in W^2$  vérifiant  $h_{x,y,w} \notin v^{a(w)-1} \mathbb{Z}[v^{-1}]$ . Il s'ensuit qu'il existe un entier relatif  $\gamma_{x,y,w-1}$  bien déterminé tel que

$$h_{x,y,w} = \gamma_{x,y,w-1} v^{a(w)} \pmod{v^{a(w)-1} \mathbb{Z}[v^{-1}]}.$$

L'auteur énonce au chapitre 14 une liste de conjectures décrivant le comportement espéré des cellules et de la fonction  $a$ . Les chapitres 15, 16 et 17 sont consacrés aux démonstrations de ces conjectures dans de nombreux cas.

Soit  $J$  le groupe abélien libre de base  $(t_w)_{w \in W}$ . La multiplication

$$t_x t_y := \sum_{w \in W} \gamma_{x,y,w-1} t_w \quad (\text{la somme est finie})$$

définit une structure d'anneau associatif sur  $J$ . Le chapitre 18 étudie les propriétés de l'anneau basé  $J$ .

Supposant la validité des conjectures évoquées, l'auteur développe ensuite une théorie, dans le cas de paramètres non nécessairement égaux, des cellules et des représentations associées. Le livre se referme sur une réalisation géométrique nouvelle des algèbres de Hecke-Iwahori comme espaces de fonctions, incluant une interprétation conjecturale des polynômes de Kazhdan-Lusztig généralisés.

La première moitié du livre présente une introduction très complète à la théorie des cellules et des polynômes de Kazhdan-Lusztig, elle ne demande pas de connaissance particulière du sujet. La seconde moitié constitue un article de recherche d'importance, elle suppose une certaine familiarité avec la théorie des représentations des groupes réductifs finis et  $p$ -adiques.

Anne-Marie Aubert,  
Institut de Mathématiques de Jussieu