

LIVRES

La science du secret

JACQUES STERN

Editions Odile Jacob, 1998

Ce livre n'est pas à proprement parler un livre de mathématiques, même si vous pouvez y apprendre les mathématiques de la cryptographie moderne, laquelle a commencé en 1976. C'est un livre qui s'achète un peu comme un roman policier et que vous pourrez lire dans le train, ou dans votre fauteuil après une journée de ski. Les protocoles utilisés avant 1976, même s'ils ne sont pas employés actuellement, sont passionnants, tant du point de vue historique que du point de vue scientifique et l'on s'en rend bien compte lorsqu'on enseigne la cryptographie. La première partie du livre parle de ces protocoles, avec leurs succès et leurs lacunes. En particulier, la fameuse machine *Enigma* était utilisée pendant la dernière guerre mondiale par les allemands qui la croyaient indécryptable, mais ses messages furent cependant compris par les forces alliées. Une des thèses défendue dans ce livre par J. Stern est que le grand mathématicien-informaticien A. Turing, qui a largement contribué à percer les secrets de cette machine, a, ce faisant, développé l'inspiration de ses recherches futures en informatique, et notamment les idées de la fameuse machine théorique qui porte maintenant son nom.

Le livre est partagé en deux parties de poids à peu près égal. La deuxième partie décrit les protocoles récents ainsi que les problèmes arithmétiques ou logiques sous-jacents : tests de primalité, construction de grands nombres premiers, méthodes de factorisation, problèmes de complexité et de « non divulgation » (zero knowledge).

Achetez le livre de J. Stern ; il est bien écrit et plaisant à lire. Si vous avez quelques connaissances en cryptographie, vous les complèterez ; sinon, vous en acquerez, et ceci de façon agréable.

J.-L. Nicolas, Université de Lyon 1

Decrypted secrets methods and maxims of cryptology

FRIEDRICH L. BAUER

Springer-Verlag, 1997

Le livre de F.L. Bauer est très différent de celui de J. Stern. D'abord, il est en anglais (le texte original a paru en allemand) et est beaucoup plus volumineux. Ensuite, la partie consacrée aux méthodes découvertes dans les 20 dernières années est très restreinte, le livre développant surtout les méthodes d'autrefois et les différentes attaques. Enfin il est plus technique, chaque méthode étant décrite en détail, et il est bon d'avoir un crayon et un papier pour suivre le texte.

Mais il a cependant son intérêt. L'auteur insiste, par exemple, sur le fait que les méthodes de chiffrement devaient être simples à exécuter, pour que le message ne soit pas déformé. Le code de Cesar est bien connu : il consiste, pour chiffrer un message, à remplacer la lettre *A* par *D*, *B* par *E*, *C* par *F*, et ainsi de suite, avec un décalage de trois lettres. A la fin de l'alphabet, on chiffre *X* par *A*, *Y* par *B* et *Z* par *C*. Dans son ouvrage, F.L. Bauer dit qu'Augustus, le successeur de Cesar, et inférieur en

SMF – Gazette – 80, juillet 1999

beaucoup de points à Cesar, utilisait un décalage d'une lettre seulement, parce que, probablement, il ne savait pas compter jusqu'à 3 de façon suffisamment sûre...

Les méthodes alphabétiques et polyalphabétiques sont expliquées à l'aide de nombreuses tables, graphiques, et illustrations. La fameuse machine *Enigma* y est longuement étudiée, ainsi que les procédés utilisés par les forces alliées pour la décrypter. C'est un livre sérieux, et si vous aimez jouer avec les mots et les lettres, ou si vous vous intéressez à l'histoire de la cryptographie, vous l'apprécierez grandement.

J.-L. Nicolas, Université de Lyon 1

Théorie des nombres (cours et exercices corrigés)

D. DUVERNEY

Dunod, 1998

Le contenu de l'ouvrage est accessible aux étudiants de licence et maîtrise de mathématiques et s'adresse également aux agrégatifs. Différents aspects de la théorie des nombres sont abordés dans le livre comme en témoignent les titres de chapitre à savoir : Irrationalité et approximation diophantienne, Développement des nombres réels en séries et produits infinis, Fractions continues, Fractions continues régulières, corps de nombres quadratiques et équations diophantiennes, Carrés et somme de carrés, Fonctions arithmétiques, Approximants de Padé, Nombres algébriques et mesure d'irrationalité, Corps, de nombres algébriques, Idéaux.

Un organigramme des chapitres placé au début du livre en facilite la lecture.

Le fil conducteur de l'ouvrage reste tout de même les problèmes diophantiens, sous leurs deux principaux aspects : les questions d'irrationalité et de transcendance.

En résumé, l'ouvrage de D. Duverney est très intéressant dans la mesure où il illustre bien la beauté entre la simplicité des énoncés et la force et la complexité des solutions.

M. Krir, Université de Versailles

Maths et Maple

JEAN-MICHEL FERRARD

2e cycle, écoles d'ingénieurs, Dunod

Le but de ce livre (465 pages) n'est pas, comme pourrait le laisser penser son titre, de présenter Maple comme aide à l'enseignement des concepts mathématiques. En fait, il traite de Maple et d'analyse numérique. L'auteur exploite Maple pour illustrer, expérimenter et comparer différentes méthodes classiques d'analyse numérique. Les thèmes abordés sont très variés : suites, polynômes, interpolation, intégration, décompositions matricielles, valeurs et vecteurs propres, équations différentielles ordinaires, séries. L'auteur fait donc sans cesse référence à la théorie des méthodes étudiées et vérifie expérimentalement la conformité des résultats obtenus avec la théorie. De ce fait cet ouvrage s'adresse plus particulièrement à un public familier à la fois avec Maple et l'analyse numérique. Un tel public, grâce aux nombreux exemples bien choisis, trouvera la lecture de cet ouvrage passionnante. Cet ouvrage devrait naturellement trouver sa place comme support à un cours d'analyse numérique de deuxième cycle.

J. Pian, Université de Versailles Saint-Quentin

Introduction à l'analyse numérique

JACQUES RAPPAZ, MARCO PICASSO

 Presses polytechniques et universitaires romandes

Ce cours d'introduction à l'analyse numérique (250 pages) a pour but de présenter les méthodes classiques utilisées en analyse numérique. Une bonne maîtrise du premier cycle universitaire est suffisante pour lire ce livre. Tous les thèmes essentiels (interpolation intégration, équation différentielles ordinaires, systèmes linéaires, vecteurs valeurs propres...) sont abordés. Les quatre derniers chapitres présentent les méthodes de différences finies et d'éléments finis pour la résolution des EDP. Pour chaque thème, les auteurs posent les bases théoriques, abordent les problèmes d'erreurs, de stabilité... A la fin de chaque chapitre des notes bibliographiques et remarques sont utiles au lecteur désireux d'approfondir le sujet. En résumé, ce livre, loin d'être un catalogue d'algorithmes, est une très bonne introduction à l'analyse numérique et s'adresse à un large public de non spécialistes du sujet.

J.P.

Mathématiques pour la licence, Algèbre cours et exercices avec solutions

LIONEL SCHWARTZ

 Dunod, 1998

Issu d'un cours de licence, ce livre très agréable à lire a le mérite d'être accessible avec un minimum de prérequis (programme de deug) et de pouvoir être lu par des étudiants de licence. Dans son cours l'auteur présente clairement les bases des thèmes suivants :

- Groupes, groupes abéliens de type fini, actions de groupes en privilégiant l'étude de S_n .
- Anneaux, polynômes, séries formelles autour de la question de divisibilité.
- Extensions des corps (sans théorie de Galois), corps finis.

Pour illustrer l'importance de ces notions, l'auteur propose des applications à la cryptographie et aux codes correcteurs d'erreurs.

Les deux derniers chapitres consacrés à la réduction des endomorphismes, à la structure de $GL(n)$, $O(n)$ sont l'occasion de réinvestir les notions abordées dans les premiers chapitres. Sont aussi étudiées les propriétés topologiques de ces groupes.

Enfin des exercices, avec indications, viennent compléter chaque chapitre.

Ce livre peut aussi s'avérer certainement très utile aux candidats au Capes.

J.P.

An Introduction to Gröbner bases

RALF FRÖBERG

 ed. John Wiley & Sons, Pure and Applied Mathematics, 1997

Ce livre est bien fait, agréable à lire, suivant une progression régulière depuis les définitions de base de l'algèbre commutative, jusqu'à l'étude de l'anneau des polynômes à plusieurs indéterminées sur un corps. Ce qui mène naturellement à la notion de division et de reste dans cet anneau, puis aux bases de Gröbner : d'abord leur définition, disons théoriques, puis l'algorithme de Buchberger.

Les questions soulevées par la détermination d'ensembles algébriques et leur lien avec les idéaux sont alors développées, y compris le théorème des zéros, la décomposition primaire ... Un chapitre est alors consacré à l'utilisation des bases de Gröbner dans ce cadre.

L'auteur aborde ensuite les problèmes « projectifs », et les questions qui arrivent à ce propos pour les bases de Gröbner (pour les idéaux homogènes).

Le livre se termine par des coups d'œil sur les développements et généralisations possibles des bases de Gröbner et sur les variantes et améliorations connues de l'algorithme de Buchberger (chapitre qui risque de devenir rapidement dépassé).

Ce livre est adapté à des étudiants de licence, il part des notions de base et est facile à lire.

Cependant, on peut regretter l'absence d'un réel chapitre introductif qui mette en lumière les problèmes qui se posent lorsqu'il s'agit de résoudre des questions qui sont faciles en une variable, et qui deviennent difficiles à plusieurs indéterminées (résolution de système polynomiaux, problème d'appartenance ...).

De plus l'intérêt géométrique de ces questions n'est pas réellement mis en valeur, le lien avec la géométrie n'est pas abordé franchement, et seulement sous entendu, ce qui est dommage.

Malgré cela, ce livre contient de nombreuses références, une bibliographie qui ne se veut pas exhaustive mais qui permet de couvrir bien le sujet. C'est donc un petit livre qu'on peut conseiller de lire et qu'il est intéressant à avoir sous la main lorsqu'on débute sur ces sujets.

A. Szpirglas, Université de Poitiers

Book of involutions

MAX-ALBERT KNUS, ALEXANDER MERKURJEV, MARKUS ROST, JEAN-PIERRE TIGNOL

Colloquium Publications, volume 44, AMS, 1998

Partant des théorèmes fondamentaux d'Albert sur les involutions des algèbres simples centrales, ce livre de 560 pages passe en revue plusieurs théories liées à ces involutions : groupes algébriques linéaires, formes quadratiques et algèbres de Clifford, algèbres de Jordan, cohomologie galoisienne, formes traces. Le livre est d'un accès agréable à plusieurs points de vue. Pour le néophyte, il contient une exposition claire des concepts fondamentaux des thèmes abordés (e.g. classification des groupes semi-simples, cohomologie galoisienne), accompagnée d'une grande variété d'exercices. La commodité du livre est appréciable au mathématicien pressé souhaitant se focaliser sur tel ou tel aspect, comme au mathématicien moins pressé intéressé par l'évolution historique du sujet ; en particulier, on dispose d'une abondante bibliographie (321 articles) doublement référencée ainsi que de notes de fin de paragraphe. Le *Livre des Involutions* convient donc à un public particulièrement vaste, c'est manifestement une réussite.

Après ce préambule, nous allons tenter de décrire sans exhaustivité la matière abordée. En particulier, nous n'allons pas nous aventurer dans la caractéristique 2, alors même que le livre ne fait pas de restriction sur le corps de base, traitant le plus souvent de façon uniforme la caractéristique 2 et distincte de 2 avec des concepts appropriés — les *paires quadratiques* sont définies à cet effet. Nous fixons donc par commodité un corps de base F de caractéristique distincte de 2. D'après un théorème de Wedderburn, une F -algèbre simple centrale A de dimension finie n'est pas autre chose qu'une algèbre de matrices sur un corps gauche T/F de dimension finie sur son centre F , une involution σ de A un antihomomorphisme de A (non nécessairement F -linéaire), i.e. $\sigma^2 = id_A$, $\sigma(x+y) = \sigma(x) + \sigma(y)$ et $\sigma(xy) = \sigma(y)\sigma(x)$. Donnons deux exemples classiques d'algèbres à involutions :

- L'algèbre $M_n(F)$ des matrices de dimension n et la transposition $X \rightarrow {}^t X$,
- L'algèbre de quaternions $(a, b)_F$ ($a, b \in F^\times$) définie par les relations $I^2 = a$, $J^2 = b$, $IJ + JI = 0$, munie de l'involution $x + yI + zJ + tIJ \rightarrow x - yI - zJ - tIJ$.

D'après Weil, on dispose d'un dictionnaire entre algèbres simples centrales à involutions et groupes semi-simples adjoints classiques. En effet, si (A, σ) est une F -algèbre à involution, on définit le F -groupe algébrique des isométries $\underline{\text{Iso}}(A, \sigma)$, dont le groupe des points rationnels est

$$\underline{\text{Iso}}(A, \sigma)(F) = \{a \in A^\times \mid \sigma(a)a = 1\};$$

on considère ensuite le groupe adjoint $\underline{\text{Iso}}^+(A, \sigma)_{ad}$, quotient de la composante neutre $\underline{\text{Iso}}^+(A, \sigma)$ de $\underline{\text{Iso}}(A, \sigma)$ par son centre. Le groupe $\underline{\text{Iso}}^+(A, \sigma)_{ad}$, est le groupe semi-simple adjoint correspondant à (A, σ) . Dans le premier exemple, le groupe $\underline{\text{Iso}}^+(A, \sigma)_{ad}$ est le groupe projectif spécial orthogonal de la forme quadratique $X_1^2 + X_2^2 + \dots + X_n^2$, dans le second exemple, pour l'algèbre de quaternions usuelle $(-1, -1)_{\mathbb{R}}$, on obtient le groupe algébrique réel $PSU(2)$. Réciproquement, l'algèbre (A, σ) apparaît comme une algèbre de Tits du groupe $\underline{\text{Iso}}(A, \sigma)_{ad}^+/F$, intrinsèquement attachée au groupe par la théorie des représentations linéaires. Cette correspondance est utilisée constamment dans le livre, qui précise ce dictionnaire. La théorie des formes quadratiques attache à une forme quadratique non dégénérée q/k , à travers sa classe de similitude, de nombreux invariants : indice de Witt, discriminant, invariant de Hasse, algèbre de Clifford paire $C_0(q)$. La généralisation de ces invariants à d'autres objets (e.g. formes hermitiennes sur les algèbres de quaternions), constitue les chapitres II et III où sont définis pour toute algèbre à involution (A, σ) l'indice de Witt, l'algèbre discriminant et l'algèbre de Clifford $C(A, \sigma)$. Précisons ce que l'on entend par isotropie. Un idéal à droite $I \subset A$ est *isotrope* si $I \subset I^\perp := \{x \in A \mid \sigma(x)y = 0 \ \forall y \in I\}$; l'indice de Witt de (A, σ) est la moitié de la dimension d'un idéal à droite isotrope de dimension maximale. Ainsi, on dit que (A, σ) est hyperbolique s'il existe un idéal à droite isotrope de dimension $\dim_F(I) = \dim_F(A)/2$.

On poursuit dans les sections III et IV par une classification des involutions des algèbres de petites dimensions (16 et 81), pour lesquelles les isomorphismes exceptionnels des groupes semi-simples de rang 1 et 2 jouent un rôle important. Un exemple fondamental est le cas d'une algèbre de biquaternions $D = (a_1, b_1)_F \otimes_F (a_2, b_2)$ à laquelle est associée via l'isomorphisme exceptionnel $SL_4 \approx \text{Spin}_6$ la forme quadratique d'Albert $q_D = a_1X_1^2 + b_1Y_1^2 - a_1b_1Z_1^2 - a_2X_2^2 - b_2Y_2^2 + a_2b_2Z_2^2$. Le groupe $SK_1(D) = SL_1(D)/[D^\times, D^\times]$, quotient du noyau du déterminant de Dieudonné $\text{Nrd} : D^\times \rightarrow F^\times$ par le groupe des commutateurs de D^\times , est un invariant important; la non trivialité de $SK_1(D)$ entraîne que la variété de groupes $SL_n(D)$ n'est pas rationnelle. Ce chapitre comporte en particulier la construction d'une injection

$$SK_1(D) \hookrightarrow H^4(F, \mathbb{Z}/2\mathbb{Z})$$

dans la cohomologie galoisienne modulo 2 à coefficients $\mathbb{Z}/2\mathbb{Z}$ du corps F . Ce résultat recouvre la construction de Platonov d'un exemple d'algèbre simple centrale D/F telle que le groupe $SK_1(D)$ est non trivial; plus généralement, utilisant cette injection, Merkurjev a démontré que si D est un corps gauche (ce qui équivaut à dire que la forme quadratique q_D est anisotrope), le groupe $SL_1(D)/F$ n'est pas une variété rationnelle sur le corps de base F (K-theory 7 (1993)).

Les trois derniers chapitres concernent respectivement les groupes exceptionnels de type G_2, F_4 , trialitaires de type D_4 et leurs algèbres sous-jacentes, octonions pour G_2 , algèbres de Jordan exceptionnelles de dimension 27 pour F_4 (appelées aussi algèbres d'Albert), et algèbres d'Allen pour D_4 . Un dénominateur commun à ces trois types de groupe est la *trialité* présente dès la couverture du livre (une aquarelle de type D_4 !) avec le diagramme de Dynkin



traduisant que le groupe des automorphismes extérieurs du groupe déployé Spin_8 est le groupe symétrique S_3 . Notant G_2 (resp. F_4) le groupe déployé de type G_2 (resp. F_4), il existe un automorphisme φ de Spin_8 d'ordre 3 tel que $G_2 = (\text{Spin}_8)^\varphi$ (les points fixes de φ) et on dispose d'un plongement $\text{Spin}_8 \rtimes S_3 \rightarrow F_4$. Disons quelques mots sur le type F_4 . La trialité et l'imbrication entre les groupes jouent un rôle essentiel dans les constructions des F -algèbres de Jordan exceptionnelles de dimension 27 (constructions de Freudenthal, Springer, Tits, travaux de Petersson–Racine) dont les classes d'isomorphie correspondent bijectivement aux classes d'isomorphie de F -groupes de type F_4 , le tout étant classifié par l'ensemble pointé de cohomologie galoisienne $H^1(F, F_4)$. Les *invariants cohomologiques* de $H^1(F, F_4)$ sont décrits en termes d'algèbres de Jordan (cf. exposé de Serre, séminaire Bourbaki **783** (1994)). L'invariant $g_3 : H^1(F, F_4) \rightarrow H^3(F, \mu_3^{\otimes 2})$, qui associe à toute algèbre d'Albert J un symbole dans $H^3(F, \mu_3^{\otimes 2})$, détecte si J a des diviseurs de 0 ou non, i.e. J a des diviseurs de 0 si et seulement si $g_3(J) = 0$, et dans ce cas, on dit qu'une telle algèbre J est réduite. On peut associer à toute algèbre d'Albert J sa forme trace $T_J : J \rightarrow k$, qui est une forme quadratique non dégénérée de dimension 27 ; il est établi que cet invariant est classifiant pour les algèbres d'Albert réduites, i.e. une algèbre d'Albert réduite J est déterminée par la classe d'isométrie de la forme T_J .

Il est à noter que le livre contient des travaux originaux, notamment la notion de *paires quadratiques* permettant de construire certaines algèbres de Clifford sans hypothèse de caractéristique, ainsi que les algèbres trialitaires du dernier chapitre. De même, le discriminant des algèbres à involutions de seconde espèce est un nouvel invariant. En conclusion, le point de vue développé dans le livre réside principalement dans l'étude des objets en eux-mêmes par opposition aux classes d'objets pour une relation de stabilité, e.g. on étudie les algèbres simples centrales (resp. les formes quadratiques), et assez peu le groupe de Brauer (resp. le groupe de Witt) et pas du tout la K -théorie. Ce livre est donc un livre d'Algèbre, et les applications arithmétiques possibles, qui fourmillent sous beaucoup d'énoncés, sont laissées à d'autres ouvrages, par exemple le livre de Scharlau. Nous ne résistons pas au plaisir de citer ici une application étonnante de l'existence d'involutions sur les algèbres simples centrales sur les corps de nombres ; il s'agit de l'article de Deligne–Sullivan *Division algebras and the Hausdorff–Banach–Tarski paradox* (Enseign. Math **29** (1983), 145–150).

P. Gille, CNRS, Orsay

Symmetric functions and orthogonal polynomials

I.G. MACDONALD

University Lecture Series, 12, AMS, 1998

Les polynômes symétriques interviennent de façon profonde en théorie des groupes. On sait bien par exemple que les polynômes de Schur associés aux partitions d'un entier n calculant les caractères irréductibles du groupe des permutations d'un ensemble à n éléments. Ils calculent aussi les traces des représentations algébriques irréductibles du groupe $GL(n, \mathbb{C})$. Au fil du temps, des polynômes symétriques de plus en plus compliqués sont intervenus dans la théorie des représentations du groupe $GL(n)$ sur divers corps de base : corps fini, \mathbb{F}_q , corps des réels \mathbb{R} , corps p -adique \mathbb{Q}_p .

Par exemple, les valeurs des fonctions sphériques sur $GL(n, \mathbb{Q}_p)$ sont calculées par les polynômes de Hall-Littlewood associés à des partitions de longueur $\leq n$. Ceux-ci dépendent d'un paramètre auxiliaire, ici égal à p^{-1} . Il est remarquable qu'il existe une famille de polynômes $P_\lambda(q, t)$, où λ est une partition et a, t deux paramètres auxiliaires, qui « coiffe » un bon nombre des polynômes évoqués ci-dessus en ce sens que l'on retrouve ces derniers en spécialisant q et t en des valeurs particulières. Par exemple, pour $q = 0$, $P_\lambda(0, t)$ est le polynôme de Hall-Littlewood associé à λ .

En fait, cette famille de polynômes $P_\lambda(q, t)$ peut elle-même être généralisée. A tout système de racines, on peut associer une telle famille. La famille précédente était implicitement associée au système de racines A_{n-1} , c'est pourquoi elle intervenait dans la théorie des représentations du groupe $GL(n)$. Ces nouvelles familles "coiffent" à leur tour les familles de polynômes utilisées par Heckman et Opdam, qui interviennent dans la théorie des fonctions hypergéométriques.

Une conjecture de Macdonald concernant les « produits scalaires » des polynômes de ces familles est restée pendant une quinzaine d'années un point central de cette théorie. Elle a été résolue en 1995 par Cherednik, qui a introduit à cette occasion les « algèbres de Hecke doubles ». Celles-ci sont assez mystérieuses du point de vue de la théorie des groupes (elles paraissent mêler des données relatives au groupe et à son L -groupe comme disent les spécialistes).

Le livre de Macdonald expose crescendo la théorie évoquée ci-dessus : le chapitre I introduit les polynômes symétriques les plus classiques et la famille des polynômes $P_\lambda(q, t)$ associée au système A_{n-1} ; le chapitre II introduit les familles associées à des systèmes de racines quelconques ; le chapitre III, qui a été ajouté à une rédaction initiale, explique les nouveautés introduites par Cherednik et sa démonstration de la conjecture de Macdonald.

Certes, ce livre reprend assez largement la littérature déjà existante. En particulier, le chapitre III recopie presque à l'identique un exposé de Macdonald au séminaire Bourbaki. Ce livre apportera donc peu aux spécialistes. Par contre, les mathématiciens non spécialistes mais utilisateurs potentiels de cette théorie en trouveront ici un exposé assez complet et remarquablement clair.

J.-L. Waldspurger, CNRS/Paris 7

Mixed Hodge structures and singularities

V. KULIKOV

Tracts in Math. vol 132, Cambridge Univ. Press, 1998

Depuis les théorèmes de Hodge réalisant la cohomologie des variétés algébriques projectives lisses complexes à l'aide de formes harmoniques (voir par exemple [D] pour une bonne introduction), la *théorie de Hodge* a investi petit à petit tous les domaines homologues ou homotopiques de la géométrie algébrique. Les objets singuliers n'ont pas été oubliés, mais ont nécessité un élargissement du cadre initial, la *théorie de Hodge mixte*.

Le livre de V. Kulikov reprend le cheminement historique qui a mené à la compréhension de la structure de Hodge mixte sur la cohomologie de la fibre de Milnor d'une fonction holomorphe f à singularité isolée. Les premiers résultats, dus à J. Steenbrink, montrent l'existence d'une telle structure. Puis A.N. Varchenko a rendu plus explicite cette structure, la reliant aux développements asymptotiques d'intégrales oscillantes. Une approche claire et détaillée (mais pas complète du point de vue des démonstrations) est développée dans le volume 2 du livre [AGV].

Un exposé assez complet de la théorie a été donné par J. Scherk et J. Steenbrink en 1985. C'est cet exposé que reprend V. Kulikov au chapitre 2 de son livre, en rappelant

d'abord les prérequis sur la connexion de Gauss-Manin (premier chapitre, un tiers du livre).

On peut regretter que l'auteur ne prenne pas assez de recul vis-à-vis de ses sources :

- l'auteur aurait pu faire l'économie de la construction de la connexion de Gauss-Manin donnée au chapitre 1, qui fait double emploi avec la construction du système de Gauss-Manin au chapitre 2, construction qui est la seule utilisée finalement ;

- il est connu maintenant que le premier article de Steenbrink contenait un argument incomplet, qui a été complété depuis par d'autres auteurs ; pourquoi l'auteur ne l'indique-t-il pas ?

- l'aspect microlocal (la dualité notamment) a beaucoup fait avancer la théorie (et a permis d'en corriger les premières erreurs) ; ici encore, l'auteur néglige complètement cet aspect ;

- d'une manière générale, l'auteur donne peu d'idées sur la nature et la difficulté des démonstrations délicates.

Le principal reproche que je pourrais faire à ces deux premiers chapitres est que, au lieu d'intégrer la théorie dans le cadre général de la géométrie algébrique et d'ouvrir ainsi des perspectives, l'auteur l'enferme dans celui des idées et des techniques qui lui ont donné naissance. Il a choisi délibérément d'ignorer les travaux ultérieurs à 1985, essentiellement ceux de M. Saito, mais aussi V. Navarro Aznar, qui donnent un cadre général à la théorie de Hodge mixte des objets singuliers. Le prétexte que cette théorie de Saito est « monstrueuse » ne tient pas : il est possible d'en exposer les énoncés et certaines méthodes de manière compréhensible, même si les démonstrations sont techniques. D'ailleurs, l'auteur a choisi de ne donner dans son livre que très peu de démonstrations. Ainsi, la lecture des deux premiers chapitres apporte peu par rapport aux articles existants.

Le dernier chapitre est consacré aux problèmes de type « problème de Torelli » pour les singularités : est-ce que les invariants donnés par la théorie de Hodge sont suffisants pour distinguer les singularités ? On trouve dans ce chapitre des exemples intéressants de calculs d'applications de périodes.

références

V.I. ARNOLD, S. GUSEIN-SADE, A.N. VARCHENKO, *Singularités des applications différentiables*, éditions MIR, Moscou, 1982 (en russe) et 1986 (en français)

J.-P. DEMAILLY, *Théorie de Hodge L^2 et théorèmes d'annulation*, *Introduction à la théorie de Hodge*, Panoramas et Synthèses, vol. 3, SMF, 1996, pages = 3-111

C. Sabbah, CNRS, École polytechnique

Singularities (The Brieskorn Anniversary Volume)

V.I. ARNOLD, G.-M. GREUEL, J.H.M. STEENBRINK

PM in math, 162, Birkhäuser, 1998

Le nom de Brieskorn est attaché à plusieurs résultats marquants de la théorie des singularités : un des plus connus est sans doute celui donnant des équations algébriques pour les 28 structures différentiables non isomorphes sur la sphère S^7 , trouvées par Kervaire et Milnor, à savoir

$$(*) \quad z_1^{2k-1} + z_2^3 + z_3^2 + z_4^2 + z_5^2 = 0, \quad (k = 1, \dots, 28)$$

où $(z_1, \dots, z_5) \in \mathbb{C}^5$ reste sur la sphère $S^9 = \{z \mid \sum_{i=1}^5 |z_i|^2 = 1\}$, reliant ainsi ces structures aux points critiques des polynômes (*). Un de ses thèmes de prédilection a été la recherche d'une description combinatoire de la structure locale des points critiques isolés d'un polynôme $f(z_1, \dots, z_n)$ et de ses déformations.

À la suite d'Arnold, les travaux sur la classification des singularités ont permis de mettre en évidence des listes de modèles, généralisant les catastrophes élémentaires de Thom. Si les premiers de la liste (singularités simples) ont été mis dès la fin des années 60 en relation avec les algèbres de Lie simples de dimension finie et les groupes de Coxeter, la compréhension de cette relation fait encore intervenir de nouveaux points de vue (article de Cassens et Slodowy, Kleinian singularities and quivers).

À chaque point critique isolé est attaché un espace vectoriel réel \mathbb{R}^{μ} (espace des cycles évanescents) contenant un réseau \mathbb{Z}^{μ} , muni d'une action du groupe (discret) de monodromie et d'une forme quadratique d'intersection. Ce groupe s'identifie à un groupe de Weyl pour les singularités simples. Brieskorn s'est attaché à étendre cette identification pour les classes suivantes de la liste. L'article d'Ebeling et Guzeïn-Zade (Suspensions of fat points and their intersection forms) participe de la même idée.

La théorie de Hodge et ses applications aux singularités est absente des travaux de Brieskorn, bien qu'il en ait introduit des outils essentiels (la connexion de Gauss-Manin et le « réseau de Brieskorn »). On en trouvera une jolie application à des théorèmes de type Torelli pour les singularités dans l'article de Hertling (Brieskorn lattices and Torelli type theorems) et des calculs de nombres de Hodge dans l'article de Hamm (Hodge numbers for isolated singularities of complete intersections).

Les mathématiciens allemands cités plus haut ont été influencés directement par Brieskorn. D'autres thèmes, plus éloignés des préoccupations du maître, sont présents dans le volume : résolution des singularités, topologie globale des polynômes complexes, espaces de modules pour les singularités, ainsi que des thèmes directement influencés par Arnold. Notamment, un article de Vassiliev développe le théorème de Newton-Arnold : le potentiel créé par une hypersurface algébrique lisse de degré d dans \mathbb{R}^n (une sphère par exemple), portant une densité de charge décrite par un polynôme de degré $\leq d-2$ (constante par exemple), est constant sur le domaine d'hyperbolicité de l'hypersurface (l'intérieur de la sphère, plus généralement l'ensemble des points tels que toute droite passant par ce point coupe l'hypersurface projectivée en d points), de sorte que la force d'attraction est nulle sur ce domaine. Vassiliev (avec l'aide d'Ebeling), montre que sur les autres domaines du complémentaire de l'hypersurface supposée assez générale, le potentiel est une fonction analytique réelle qui *n'est pas* algébrique.

Le texte de la conférence de Hirzebruch, concernant les premiers travaux de Brieskorn en relation avec les siens sur les surfaces qui portent son nom et ceux de ses autres élèves n'a malheureusement pas été reproduit.

C. Sabbah, CNRS, École polytechnique

Bifurcations of planar vector fields and Hilbert's 16e problem

R. ROUSSARIE

PM, 164, Birkhäuser, 1998

La partie B du 16e problème de Hilbert concerne (au sens large) l'étude des trajectoires périodiques isolées dans l'ensemble des trajectoires périodiques (appelées cycles limites) des champs de vecteurs du plan. Dans un article récent publié au Math. Intelligencer [S], S. Smale dresse une liste des problèmes qui lui semblent importants à étudier dans le futur. S. Smale aborde en particulier le problème des cycles limites parmi 18 autres considérés comme particulièrement significatifs. Malgré l'attention internationale que ce problème recueille, les recherches qu'il suscite en France ne sont pas très bien (re)connues (en France!) peut-être en raison de l'absence d'ouvrages systématiques sur le sujet. Le livre de Roussarie est la première contribution dans ce sens. L'auteur fait le point sur une démarche qu'il a suivie depuis une quinzaine

d'années et pour laquelle lui-même, ses collaborateurs et ses étudiants ont publié de nombreux articles.

L'origine de la démarche repose sur un théorème de Poincaré-Bendixson concernant les champs du plan. Une fois compactifié l'espace de phase, les ensembles sur lesquels peuvent s'accumuler des orbites périodiques sont de trois types :

- (i) les orbites périodiques
- (ii) les points singuliers
- (iii) les graphiques (ensembles formés de points singuliers et de séparatrices qui les joignent).

Poincaré, lui-même avait montré que les cycles limites ne peuvent s'accumuler sur une orbite périodique dans le cas d'un champ analytique. Seuls restent les cas (ii) et (iii) et on se ramène essentiellement au troisième cas par désingularisation. On est amené ainsi à faire une liste des ensembles qui peuvent être limites d'orbites périodiques (cette notion convenablement précisée prend le nom d'ensemble limite-périodique) dans une famille de champs du plan. On définit alors la cyclicité d'un ensemble limite-périodique comme le maximum (s'il existe) de cycles limites en lesquels l'ensemble peut se casser dans une déformation à l'intérieur de la famille. Le 16e problème est résolu une fois qu'on a montré que tous les ensembles limite-périodique ont une cyclicité finie.

Roussarie et ses collaborateurs ont ainsi étudié au cas par cas des ensembles limite-périodique et démontré avec des techniques variées d'analyse fine à chaque fois la finitude de la cyclicité (et souvent en ont obtenu une estimation exacte). Parmi les techniques utilisées, figurent des éclatements quasi-homogènes, l'utilisation de développements asymptotiques (du type considéré par J. Ecalle, [E]) et des propriétés algébriques des idéaux engendrés par les coefficients de ces développements. Les résultats obtenus ont non seulement fait considérablement progresser sur le 16e problème ; ils ont aussi apporté des éclairages nouveaux sur la théorie des bifurcations des systèmes différentiels, en particulier sur la bifurcation de Bogdanov-Takens.

Le livre se termine par un passionnant chapitre qui ouvre des perspectives sur la désingularisation de familles de champs analytiques et qui intéressera autant les spécialistes de la géométrie analytique et de la théorie des singularités que ceux des systèmes dynamiques.

Suivant le schéma des dissertations scolaires, l'auteur du rapport fait une courte antithèse. De son point de vue, la partie « faible » du livre concerne l'approche de Bautin. Les références de ce passage sont dépassées. Elles ne rendent pas compte des récents développements de cette partie du sujet. La référence à Yakovenko pour l'approche des dérivées successives est un peu fantaisiste car cet auteur ne fait que mentionner l'existence de cette méthode.

De toute façon, il faut bien reconnaître, vu la variété des méthodes utilisées et l'abondance des résultats obtenus ces dernières années, la difficulté voir l'impossibilité de faire un ouvrage exhaustif.

Le livre de Roussarie a le mérite de permettre aux non-spécialistes de s'initier aux développements de l'approche « théorie des bifurcations » avec une grande clarté et un réel effort pédagogique. De ce fait, il devrait être très utile aux étudiants de DEA et de thèse en systèmes dynamiques. Les spécialistes y trouveront rassemblés des résultats jusque là dispersés dans la littérature et l'annonce de développements nouveaux sur les désingularisations de familles dans l'étude des ensembles limite-périodique singuliers.

références

[E] J. Ecalle : Introduction aux fonctions analysables et preuve constructive de la conjecture de Dulac, Hermann, Paris, 1992

[S] S. Smale : Mathematical Problems for the next Century, Math. Intelligencer, 20, 1998.

J.-P. Francoise, Université Paris 6

Perfect incompressible fluids

JEAN-YVES CHEMIN

Oxford lecture series in Mathematics and its Applications, vol. 14, 1998

La théorie mathématique de l'équation d'Euler des fluides parfaits incompressibles a connu un renouveau en 1991 lorsque Jean-Yves Chemin et Jean-Marc Delort résolurent chacun une question majeure : la persistance des poches de tourbillon (J.-Y. Chemin, Séminaire EDPs 1990-91, exposé No XIII, École Polytechnique, Palaiseau 1991 & Ann. Sci. ENS, **26**, 1993, pp 517-542) et l'existence pour les nappes de tourbillon (J.-M. Delort, C.R.A.S., **312**, 1991, pp 85-88 & J. of the AMS, **4**, 1991, pp 553-586). Aucun résultat de cette importance n'avait pu être obtenu durant les vingt-huit années précédentes. Encore faut-il noter qu'il s'agit de problèmes dans le plan et que la situation réaliste d'un écoulement dans l'espace physique \mathbb{R}^3 (mieux, un ouvert de \mathbb{R}^3) nous résiste pour l'instant.

De tels succès justifiaient amplement qu'un ouvrage voie le jour, qui fasse le point sur la théorie de cette équation. Comme de plus les nouveaux points de vue fournissent des preuves élégantes ou plus claires d'énoncés classiques, ce livre devenait indispensable. Personne n'était mieux qualifié que J.-Y. Chemin pour l'écrire, par le rôle central qu'il a joué dans le sujet et par sa connaissance du paraproduit.

Ce livre est d'abord paru en Français en 1995 (Astérisque, vol. 230). Voici maintenant la traduction anglaise, dont les modifications, mineures, tiennent compte des développements récents. Ceux-ci se traduisent par six entrées nouvelles dans la bibliographie. Ce faible nombre s'explique par la difficulté des problèmes ouverts. Une fois n'est pas coutume, la traduction est à la hauteur de la version originale, grâce à deux traducteurs de très haut niveau scientifique et parfaitement bilingues.

Cet ouvrage poursuit donc deux objectifs, à savoir présenter de manière moderne et synthétique la théorie classique de Wolibner et Yudovich entre autres, puis d'expliquer les résultats récents. La grande qualité de ce texte est de parvenir à une présentation unifiée, au moyen d'estimations de Hölder et de Sobolev du paraproduit, données par la décomposition de Littlewood-Paley (chapitres 2 et 3). Notons que la classification des espaces fonctionnels est somme toute standard, à l'exception de l'espace \mathbb{C}^1 qui laisse la place à \mathbb{C}_*^1 . Cet espace, légèrement plus gros, convient cependant pour démontrer un théorème à la Cauchy-Lipschitz pour les équations différentielles ordinaires, ce qui est fondamental pour définir le flot associé au champ de vitesse. Ainsi, un point de vue Lagrangien peut être adopté dans la plupart des situations.

L'équation d'Euler est introduite au chapitre 1, comme conséquence du principe de moindre action. Ce point de vue abstrait ne traduit pas forcément toute la physique du problème : tout d'abord, il n'est pas transposable au cas des fluides réels, qui sont toujours un peu visqueux et obéissent aux équations de Navier-Stokes (ou pire). Ensuite, ce principe ne distingue pas entre le passé et l'avenir, alors que pour certaines solutions très faibles (celles des nappes de tourbillon, ou les solutions $3-d$ après une singularité éventuelle), peuvent obéir à une « condition d'entropie » traduisant l'irréversibilité. Des exemples récents de solutions à support compact en temps (Shnirelman, Comm. in Pure & Applied Math. **50**, 1997, pp 1261-1286) montrent qu'en l'absence d'une telle restriction, certaines solutions au sens des distributions n'ont aucun sens physique.

Cette définition est cependant tout-à-fait acceptable pour les questions abordées dans ce livre. Elle est suivie au chapitre 2 par une présentation particulièrement élégante de la théorie de Littlewood-Paley. Cette partie peut avoir à elle seule un intérêt pour des étudiants avancés. Elle s'achève avec l'étude, via le calcul paradifférentiel, de l'opérateur

$$\pi : v \mapsto p := -\Delta^{-1} \partial_i \partial_j (v_i v_j),$$

qui à la vitesse du fluide associe sa pression.

Le troisième chapitre est consacré aux estimations du champ de vitesses au moyen de son rotationnel $\Omega(v)$, utilisant l'ellipticité de l'opérateur

$$v \mapsto (\Omega(v), \operatorname{div} v).$$

Une attention particulière est donnée à la notion de régularité tangentielle, relativement à une structure géométrique, anticipant ainsi sur le problème des poches de tourbillon.

Le premier résultat arrive au chapitre 4. Il s'agit des solutions classiques (Wolibner, *Math. Zeitschrift*, vol **37**, 1933, pp 698-726), qu'on obtient lorsque v_0 est de classe \mathbb{C}^α , $\alpha > 1$. L'équation d'Euler est vue ici comme une équation d'évolution abstraite dont le terme non-linéaire, quadratique, satisfait une estimation douce. En particulier, on n'utilise pas, dans cette approche, la conservation de l'énergie. L'existence qu'on obtient est locale en temps, avec un critère à la Beale-Kato-Majda pour l'explosion en temps fini. Ce critère, joint à la conservation du rotationnel en dimension deux, fournit immédiatement l'existence globale dans ce cas.

Au chapitre suivant, l'auteur décrit le résultat de Yudovich (*Z. Vycisl. Mat. i Mat. Fiz.*, vol **3**, 1963, pp 1032-1066), pour les données initiales à rotationnel borné, en deux variables d'espace. C'est exactement le cas où le champ de vitesse doit rester dans \mathbb{C}_*^1 , le flot étant donc bien défini. La solution est encore unique, mais la régularité de Hölder du flot peut se détériorer avec le temps; un exemple explicite (section 5.3) montre qu'il en est bien ainsi. La section 5.5 est particulièrement importante puisqu'elle contient la preuve de la persistance des poches de tourbillon. L'annonce de ce résultat, dû à l'auteur (voir ci-dessus) et indépendamment à P. Serfati (*C. R. A. S.*, vol **318**, 1994, pp 515-518), créa la surprise en 1991. En fait, des expériences numériques (N.J. Zabusky, *J. Comput. Phys.*, vol **30**, 1979, pp 96-106) suggéraient que des singularités devaient se développer à la frontières des poches, sans doute en temps fini. A.J. Majda (*Comm. Pure & Applied Math*, vol **39**, 1986, no. S, suppl., pp S187-S220) avait même conjecturé l'existence de poches de tourbillon, régulières à l'instant initial, dont le bord cesserait d'être rectifiable au bout d'un temps fini. Enfin, S. Alinhac (*J. Func. Anal.*, vol **98**, 1991, pp 361-379) avait étudié une approximation quadratique de l'équation qui gouverne l'évolution de la frontière d'une poche, et trouvé quelque évidence de la formation d'une singularité. Il est donc juste de dire que le théorème de Chemin est l'une des plus importantes découvertes de la dernière décennie dans la théorie mathématique des fluides.

Le chapitre suivant est consacré aux nappes de tourbillon en dimension deux. Des résultats intermédiaires avaient été obtenus par R. DiPerna et A. Majda (*Comm. Pure & Applied Math.*, vol **40**, 1987, pp 301-345). C'est la plus faible de toutes les théories en dimension deux, au sens où seule l'existence d'une solution faible est connue, sans aucune information sur la régularité ni l'unicité. Puisque l'équation de Birkhoff-Rott, qui gouverne l'évolution des nappes lipschitziennes, est linéairement mal posée, on n'espère même pas que la structure géométrique soit préservée. En particulier, le flot ne devrait pas être une bijection. Le point crucial dans l'analyse de Delort est l'étude d'une intégrale singulière. Ici, on a besoin que la partie singulière de $\Omega(v_0)$ soit de signe constant. Cette restriction semble être justifiée au vu des simulations numériques de R. Krasny, mais qui sait ?

Les chapitres 7 (régularité Gevrey) et 9 (poches de tourbillon à frontières peu régulières) sont plus spécialisés et ont moins retenu mon attention. En revanche, le chapitre 8 présente des résultats récents de l'auteur, relatifs à la régularité du flot par rapport au temps, qui sont loin d'être intuitifs. En gros, le flot est analytique pour les solutions classiques et est encore Gevrey-3 pour les solutions de Yudovitch. C'est d'autant plus surprenant que, le champ de vitesse n'étant pas plus régulier que v_0 , on n'espère pas tant de régularité en espace. L'exemple de la section 5.3 est clair à ce sujet.

En définitive, cet ouvrage est un grand moment de mathématiques et offre un point de vue très étendu sur la théorie mathématique des fluides parfaits incompressibles. Il montre clairement à quel point la différence est grande, entre le cas 2D et le cas 3D (le lecteur devra être attentif à certains énoncés, qui n'ont de sens qu'en dimension deux, bien que ce ne soit pas précisé). Ce livre remplit un vide dans la littérature, qui comprend très peu d'ouvrages sur le sujet. J'ai trouvé peu de points de comparaison valables. Le livre de C. Marchioro et M. Pulvirenti (Applied Math. Sc, vol **96**, Springer-Verlag, 1994), fait des choix assez différents (la dynamique des tourbillons ponctuels), et son intérêt diminuera peut-être avec le temps, tandis que celui de Chemin ne se démodera pas de sitôt. Quant au premier volume de P.-L. Lions (Oxford lecture series in Math. & its Appl., vol **3**, Oxford Sc. Publ., 1996), il n'accorde qu'un seul chapitre, certes dense, aux fluides parfaits, et n'aborde pas les questions liées à la structure géométrique des solutions.

La parution d'un tel ouvrage sur un sujet classique est un événement rare, qui devrait inciter beaucoup de chercheurs à l'ajouter à leur collection personnelle.

D. Serre, ENS Lyon

Lectures on representation theory and Knizhnik-Zamolodchikov equations

P. ETINGOF, I. FRENKEL, A. KIRILLOV (JR)
Math. Surveys and mono, 58, AMS, 1998

Le livre de P. Etingof, I. Frenkel et A. Kirillov est une présentation de la théorie des équations de Knizhnik-Zamolodchikov (KZ), de leurs versions aux différences et de leurs liens avec la théorie des représentations de diverses algèbres. Le point de vue des auteurs est que la correspondance entre l'algèbre de Kac-Moody $\hat{\mathfrak{g}}$ et le groupe quantique $U_q\mathfrak{g}$ (Kohno-Drinfeld, et Kazhdan-Lusztig) motive l'étude de correspondances entre : l'algèbre toroïdale $\hat{\mathfrak{g}}$ (extension centrale de l'algèbre de doubles lacets $LL\mathfrak{g}$) et l'algèbre quantique affine $U_q\hat{\mathfrak{g}}$ d'une part et $U_q\hat{\mathfrak{g}}$ et les groupes quantiques elliptiques $E_{q,\tau}(\mathfrak{g})$ introduits par Felder, de l'autre. Ces développements s'insèrent dans un programme de déformation des théories conformes des champs. Le deuxième type de correspondance est maintenant compris dans le cas $\mathfrak{g} = \mathfrak{sl}_2$, grâce aux travaux de Felder, Tarasov et Varchenko.

Les équations KZ sont les systèmes différentiels

$$(1) \quad \kappa \frac{\partial}{\partial z_i} u = \sum_{j \neq i} \frac{t^{ij}}{z_i - z_j} u,$$

où $u(z_1, \dots, z_n)$ est une fonction de n variables complexes, à valeurs dans un produit $V_1 \otimes \dots \otimes V_n$ de représentations d'une algèbre de Lie semi-simple \mathfrak{g} , t^{ij} est l'action de l'élément de Casimir de $\mathfrak{g} \otimes \mathfrak{g}$ sur les modules i et j , et κ est une constante complexe.

Ces équations proviennent d'une connexion naturelle sur l'espace des opérateurs d'entrelacement entre modules sur l'algèbre de Kac-Moody $\hat{\mathfrak{g}}$ associée à \mathfrak{g} . Elles ont

été introduites par Knizhnik et Zamolodchikov dans leur étude de modèles de théorie conforme, les modèles de Wess-Zumino-Witten.

On peut voir les équations KZ comme des généralisations des équations hypergéométriques, qui apparaissent dans le cas $\mathfrak{g} = \mathfrak{sl}_2$. Des formules intégrales pour les solutions ont été données par divers groupes d'auteurs ; les plus générales sont dues à Schechtman-Varchenko et Cherednik. Ces formules se présentent comme des intégrales de fonctions multivaluées sur des classes d'homologie à valeurs dans un système local ; ces classes d'homologie correspondent à des vecteurs singuliers pour des modules sur un groupe quantique.

Ces formules intégrales ont une explication algébrique et une interprétation géométrique. L'explication algébrique est la réalisation de $\hat{\mathfrak{g}}$ par des algèbres de Heisenberg (due à Wakimoto et Feigin-Frenkel), dont on déduit les réalisations de modules de Verma sur $\hat{\mathfrak{g}}$ par des modules de Fock. L'interprétation géométrique est que la connexion KZ est une connexion de Gauss-Manin. Ces résultats sont exposés dans les chapitres 4 à 7.

Les auteurs exposent ensuite, sans démonstrations, le calcul de la monodromie des équations KZ. Le résultat de base est celui de Kohno-Drinfeld, qui dit que la représentation du groupe de tresses associée à la connexion KZ est la même que celle provenant du groupe quantique $U_q\mathfrak{g}$. Un raffinement en est l'équivalence de catégories entre classes de modules sur $U_q\mathfrak{g}$ et sur $\hat{\mathfrak{g}}$ (Kazhdan-Lusztig). Ces résultats ne reposent pas sur les formules intégrales mais peuvent en être déduits.

Les auteurs étudient ensuite une version aux différences des équations KZ (équations de KZ quantique ou qKZ). Il s'agit du système

$$(2) \quad u(p^{\delta_i} \mathbf{z}) = K_i(\mathbf{z})u(\mathbf{z}),$$

où \mathbf{z} est le n -uplet de variables complexes (z_1, \dots, z_n) , δ_i est le i ème vecteur de base de \mathbf{C}^n , $u(\mathbf{z})$ est à valeurs dans un produit $V_1 \otimes \dots \otimes V_n$ de modules V_i de niveau zéro sur $U_q\hat{\mathfrak{g}}$ et de plus haut poids λ_i , et $K_i(\mathbf{z})$ est le produit

$$K_i(\mathbf{z}) = R^{(i, i-1)}(pz_i/z_{i-1}) \dots R^{(i, 1)}(pz_i/z_1) q^{(\lambda_0 + \lambda_N + 2\rho)^{(i)}} \times \\ \times R^{(ni)}(z_n/z_i)^{-1} \dots R^{(i+1, i)}(z_{i+1}/z_i)^{-1}$$

où ρ est la demi-somme des racines positives de \mathfrak{g} , et $R^{(ij)}(z)$ est l'action de la R -matrice universelle de $U_q\hat{\mathfrak{g}}$ sur les modules V_i et V_j ; à un facteur scalaire près, $R^{(ij)}(z)$ est une fonction rationnelle de z .

(2) définit un système compatible d'équations aux différences. I. Frenkel et N. Reshetikhin ont montré que de façon analogue aux équations KZ, ces équations sont la traduction d'une connexion naturelle sur l'espace des opérateurs d'entrelacement entre des modules sur $U_q\hat{\mathfrak{g}}$ de niveau k et les V_i , si on a $p = q^{-2(k+h^\vee)}$ (h^\vee est le nombre de Coxeter dual de \mathfrak{g}). Dans le cas $k = 0$, les équations 2 avaient été introduites auparavant par F. Smirnov, dans son étude des facteurs de forme pour des théories intégrables.

Les auteurs montrent comment les équations 2 sont obtenues à partir de la théorie des représentations de $U_q\hat{\mathfrak{g}}$ (chap. 9 à 11) ; puis, suivant le travail original de Frenkel et Reshetikhin, ils donnent les formules intégrales pour les solutions de 2, pour $\mathfrak{g} = \mathfrak{sl}_2$ (chap. 11).

Dans le chapitre 12, les auteurs énoncent un analogue du résultat de Kohno-Drinfeld pour les équations 2, dans le cas $\mathfrak{g} = \mathfrak{sl}_2$. Le point de vue adopté pour parler de monodromie d'une équation aux différences est le suivant : considérons une équation vectorielle

$$(3) \quad u(pz) = A(z)u(z),$$

où $u(z)$ est une fonction d'une variable complexe z , à valeurs dans \mathbf{C}^n , et $A(z)$ est une matrice de $GL_n(\mathbf{C})$, dépendant rationnellement de z .

Sous certaines hypothèses sur $A(z)$, on peut construire des solutions $u_i^{(0)}(z)$ et $u_i^{(\infty)}(z)$ de (3), de comportements asymptotiques fixés près de 0 et de ∞ . On peut alors exprimer les $u_i^{(\infty)}(z)$ en termes des $u_i^{(0)}(z)$ par

$$u_i^{(\infty)}(z) = \sum_j C_{ij}(z) u_j^{(0)}(z);$$

$(C_{ij}(z))_{1 \leq i, j \leq n}$ est une matrice p -périodique, qui joue le rôle de matrice de monodromie. On l'appelle matrice de connexion. En pratique, on ne sait la calculer que si l'on dispose de formules intégrales pour les solutions de (3).

Le résultat, dû à Tarasov et Varchenko, est que la matrice de connexion de l'équation 2 est donnée par une R -matrice elliptique. De telles R -matrices elliptiques apparaissent comme poids de Boltzmann pour les modèles RSOS en mécanique statistique; elles sont les objets de base de la construction des groupes quantiques elliptiques par Felder. Un analogue elliptique de ce résultat est dû à Felder et Varchenko (dualité entre deux groupes quantiques elliptiques).

Dans un chapitre de conclusion, les auteurs mentionnent quelques problèmes ouverts : simplifier les formules intégrales pour les solutions de 2; généralisation de la correspondance de Tarasov-Varchenko en rang supérieur; lien avec l'algèbre de Virasoro quantique; avec les algèbres toroïdales; étude aux valeurs spéciales de k et q ; interprétation des équations 2 elliptiques; étude au niveau critique, et q -déformation des systèmes de Beilinson-Drinfeld...

Le livre de P. Etingof, I. Frenkel et A. Kirillov est issu d'un cours de niveau DEA d'I. Frenkel à l'université de Yale. Il constitue une introduction claire et vivante aux équations (q)KZ. Le chapitre de conclusion formule les problèmes principaux se posant actuellement dans le sujet. Il pourra être lu avec profit tant par des spécialistes que par des étudiants désireux d'apprendre le sujet.

B. Enriquez, ETH