Université Grenoble Alpes **2018-2019**
M1 Mathématiques générales

Sujets de TER

1. Algorithme AKS de primalité
2. Classification des surfaces
3. Sur la conjecture jacobienne
4. Continuité de l'opérateur de Cauchy et courbure de Menger
5. Cryptographie homomorphe
6. Empilements de cercles
7. Fondements mathématiques de la méthode des éléments finis
8. Formules de l'aire et de la co-aire
9. Groupe de Witt d'un corps
10. Groupe des rotations de l'espace euclidien et quelques sous-groupes
11. Groupe fondamental et SO(3)
12. Groupes aléatoires et petites simplifications
13. Inégalités de concentration et applications
14. Inégalités géométriques et courbure positive
15. Des inégalités isopérimétriques à la géométrie sous-riemannienne de contact
16. Irrationalité des valeurs de la fonction zeta de Riemann sur les entiers
17. Jeux stochastiques, application au jeu du *Qui est-ce ?*
18. Marches auto-évitantes, constante de connectivité
19. Mélanges
20. Modules projectifs
21. Nombres chanceux d'Euler et factorialité
22. Orbites de familles de champs de vecteurs
23. Pavages impossibles et groupes de Conway
24. Petit et grand théorèmes de Picard, le point de vue géométrique
25. Plan hyperbolique et surface modulaire
26. Ruptures
27. Le spin comme une conséquence de la théorie des représentations
28. Le terminateur de la Lune
29. Théorème des nombres premiers et hypothèse de Riemann
30. Théorie de Morse

1 Algorithme AKS de primalité

En 2002, une caractérisation de la primalité d'un nombre qui peut se verifier en un temps polynomial a été découverte. Il s'agit du test de primalité AKS (pour Manindra Agrawal, Neeraj Kayal, et Nitin Saxena), qui, contrairement à d'autres tests largement utilisés (et efficaces), n'est pas probabiliste, mais deterministe.

Le but du sujet proposé est d'explorer les mathématiques de cet algorithme.

Bibliographie

Terence Tao, *The AKS primality test*, post du 11 août 2009 sur le blog *What's new*.
`https://terrytao.wordpress.com/2009/08/11/the-aks-primality-test`

Andrew Granville, *It is easy to determine whether a given integer is prime*, Bull. Amer. Math. Soc. 42 (2005), 3-38.
`http://www.ams.org/journals/bull/2005-42-01/S0273-0979-04-01037-7/`

2 Classification des surfaces

Toute surface compacte, connexe, sans bord, est homéomorphe à la sphère, à une somme connexe de tores ou à une somme connexe de plans projectifs. Le but du sujet proposé est de démontrer ce résultat (on pourra admettre l'existence de triangulations des surfaces).

Bibliographie

William S. Massey, *A Basic Course in Algebraic Topology*.

André Gramain, *Topologie des surfaces*.

3 Sur la conjecture jacobienne

La conjecture jacobienne concerne les polynômes à plusieurs variables et a été proposée par Ott-Heinrich Keller en 1939, Shreeram Abhyankar lui donnant par la suite son nom actuel. *Grosso modo*, cette conjecture affirme que si $F : \mathbb{C}^n \to \mathbb{C}^n$ est une application polynomiale dont le jacobien est une constante non nulle, alors F admet une application réciproque F^{-1} dont les composantes sont des polynômes.

Cette conjecture est également célèbre pour les nombreuses tentatives de preuves qu'elle a suscitées, contenant souvent des erreurs subtiles, et elle figure dans la liste *Mathematical Problems for the Next Century* proposée par Stephen Smale en 1998 (problème 16).

Le travail proposé consiste à étudier l'équivalence entre la conjecture jacobienne et d'autres problèmes en géométrie et en algèbre (par exemple la conjecture de Dixmier et la conjecture de Poisson), ainsi que des réductions de la conjecture originale et des

contre-exemples à des conjectures proches (par exemple la conjecture jacobienne réelle forte).

Pré-requis Algèbre de L3.

Bibliographie

Severino C. Coutinho, *A primer of algebraic D-modules*, London Mathematical Society Student Texts, 33, Cambridge University Press, Cambridge, 1995.

Sergey Pinchuk, *A counterexample to the strong real Jacobian conjecture*, Math. Z. 217 (1994), no. 1, 1–4.

Arno van den Essen, *Polynomial automorphisms and the Jacobian conjecture*, Progress in Mathematics, 190, Birkhäuser, 2000.

Arno van den Essen, *Perhaps the Jacobian conjecture is simple*, In Polynomial automorphisms and related topics, Publishing House for Science and Technology, Hanoi, 2007, 21–41.

4 Continuité de l'opérateur de Cauchy, courbure de Menger

Le programme de Calderón-Zygmund, lancé dans les années 1960, consistait en l'étude des intégrales singulières qui interviennent par exemple dans les équations aux dérivées partielles. Ce fut un renouveau de l'analyse de Fourier. Une conjecture importante était que l'opérateur de Cauchy (celui qui vient de l'analyse complexe) était continu pour la norme L^2 sur les graphes lipschitziens. La conjecture fut résolue en 1981 dans un célèbre article de Ronald Coifman, Alan McIntosh et Yves Meyer. Leur preuve est très difficile à comprendre et une dizaine de démonstrations plus simples ont été proposées dans les années suivantes. Le but du stage sera de comprendre la dernière, due à Mark Melnikov et Joan Verdera, qui est liée à la géométrie du plan via la courbure de Menger.

Pré-requis Théorie de la mesure et calcul différentiel de L3.

Bibliographie

Mark S. Melnikov, Joan Verdera, *A geometric proof of the L^2 boundedness of the Cauchy integral on Lipschitz graphs*, International Mathematical Research Notices volume 7 (1995), 325-331.
`http://mat.uab.cat/~jvm` (Aller à *Research papers*, puis presque tout en bas de la page.)

5 Cryptographie homomorphe

Supposons que l'on souhaite chiffrer un jeu de données numériques de manière à ce qu'un observateur indélicat ne puisse pas les trouver facilement (des données médicales sur une cohorte de patients, des résultats secrets d'une experience sensible, etc.). On sait qu'on peut faire appel à un protocole basé sur la théorie des nombres, sa sécurité théorique reposant sur la difficulté à inverser les logarithmes discrets, ou à factoriser des grands nombres.

Supposons à présent que l'on souhaite effectuer des calculs sur ce jeu de nombres. Il peut être fastidieux, ou même dangereux, de devoir déchiffrer les nombres avant de procéder aux calculs.

On s'intéresse alors à des méthodes de chiffrement homomorphes. Il s'agit de demander que les applications de chiffrement soient des morphismes pour l'addition et la multiplication. Les opérations que l'on souhaite effectuer sur les données véritables peuvent alors être réalisées directement sur les données chiffrées, et on ne devra déchiffrer que le résultat.

Au moins dans une certaine mesure, on peut décrire de tels protocoles ingénieux de chiffrement. Ils font intervenir l'algèbre et la gèométrie des réseaux euclidiens, et des empilements de sphères.

Bibliographie

Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer UTM, 2008, chapitre 7.

Chris Peikert, *A decade of lattice cryptography*, Cryptology ePrint Archive : Report 2015/939.
`https://eprint.iacr.org/2015/939`

6 Empilements de cercles

Étant donné un graphe G dessiné dans le plan, un empilement de cercles (ou *circle packing*) de géométrie G est une famille (C_v) de cercles du plan, indexés par les sommets de G, dont les intérieurs sont disjoints, et tels que deux cercles C_v et C_w sont tangents si et seulement si les sommets v et w sont adjacents. Un tel empilement de cercles existe toujours, mais ce fait n'est pas du tout évident et il en existe plusieurs preuves. Dans le cas d'un graphe fini G, on peut imposer aux cercles les plus extérieurs d'être tangents intérieurement au cercle unité.

Si on part d'un domaine simplement connexe Ω borné du plan, on peut fabriquer un graphe planaire fini G_δ en considérant l'intersection de Ω avec le réseau triangulaire de pas δ. Ce graphe G_δ correspond donc à un empilement de cercles $(C_v)_{v\in G_\delta}$ contenus dans le disque unité U ; on peut regarder l'application qui à v associe le centre de C_v

et l'étendre de manière affine par morceaux à une application $\phi_\delta : \Omega \to U$. C'est un joli résultat dû à Thurston, Rodin et Sullivan que, quand δ tend vers 0, l'application ϕ_δ (normalisée correctement) converge uniformément vers une application conforme entre Ω et U, ce qui constitue une preuve « graphique » du théorème de Riemann. D'une certaine façon, la structure d'empilements de cercles apparaît donc comme une version discrète de l'analyse complexe.

Le but du travail proposé est de comprendre la construction des empilements de cercles ainsi que la preuve de la convergence mentionnée ci-dessus.

Pré-requis

Pas beaucoup pour la première partie, le cours de fonctions holomorphes pour la seconde.

Bibliographie

Zheng-Xu He, Oded Schramm, *Fixed Points, Koebe Uniformization and Circle Packings*, Annals of Mathematics 137 (1993), 369–406.

Burt Rodin, Dennis Sullivan, *The convergence of circle packings to the Riemann mapping*, J. Differential Geom. 26 (1987), 349–360.
`https://projecteuclid.org/euclid.jdg/1214441375`

Kenneth Stephenson, *Introduction to Circle Packing : The Theory of Discrete Analytic Functions*, Cambridge University Press, 2005.

7 Fondements mathématiques de la méthode des éléments finis

La méthode des éléments finis est une méthode numérique qui fournit des approximations des solutions d'équations aux dérivées partielles sur un ouvert borné Ω de $\mathbb{R}^n$, notamment via une reformulation variationnelle de l'équation à résoudre. Elle est utilisée couramment, entre autres, pour résoudre numériquement les équations physiques décrivant les modes de vibration d'une structure mécanique. Sa justification mathématique, basée sur des techniques d'analyse fonctionnelle, nécessite l'étude fine de plusieurs sous-espaces normés de $L^2(\Omega)$.

Le travail principal du sujet consiste à examiner de près cette justification.

Pour fournir des bases sûres à la méthode, on doit « triturer » les normes sur des espaces de Banach appropriés, afin que certaines applications linéaires deviennent continues, et se poser des questions sur la compacité de la boule unité d'un espace de dimension infinie.

S'il vous est arrivé de vous demander, pendant vos cours de topologie de L3, à quoi pouvait bien servir tout l'appareillage que l'on vous présentait, alors ce sujet est taillé sur mesure pour vous.

Pré-requis Topologie et théorie de la mesure de L3.

Bibliographie

Haïm Brézis, *Analyse fonctionnelle, théorie et applications.*

8 Formules de l'aire et de la co-aire

Les formules de l'aire et de la co-aire donnent des formules de changement de variables par une fonction $f : \mathbb{R}^n \to \mathbb{R}^m$ si f est non lisse, en fait lipschitzienne, et $n \neq m$.

Le but du travail proposé est de démontrer ces formules « magiques », ce qui implique de comprendre des bases de la théorie géométrique de la mesure, comme la mesure de Hausdorff. Suivant le temps, des applications aux calculs d'aire ou des extensions à des cadres non euclidiens pourront être discutées.

Pré-requis Théorie de la mesure et calcul différentiel de L3.

Bibliographie

Lawrence C. Evans, Ronald F. Gariepy, *Measure theory and fine properties of functions*, CRC Press (2015).

Harold R. Parks, Steven G. Krantz, *Geometric integration theory*, Birkhauser (2008).

9 Groupe de Witt d'un corps

Étant donné un corps k, le but est de classer à isométrie près les formes bilinéaires symétriques sur k non dégénérées, i.e. classer à conjugaison près les matrices symétriques inversibles à coefficients dans k. Dans ce but, Ernst Witt a introduit ce qu'on appelle aujourd'hui le groupe de Witt de k. Le but du projet est de calculer ce groupe pour certains corps k et d'en tirer des résultats de classification via le théorème de simplification de Witt, qui est un résultat fondamental de la théorie. On redécouvrira par exemple le théorème d'inertie de Sylvester, qui se traduit par le fait que le groupe de Witt du corps des nombres réels est simplement $\mathbb{Z}$.

Pré-requis Algèbre de L3.

Bibliographie

Tsit Yuen Lam, *The algebraic theory of quadratic forms.*

10 Groupe des rotations de l'espace euclidien et quelques sous-groupes

Il s'agira d'abord d'étudier les propriétés de base du groupe SO(3) des rotations de l'espace euclidien : engendrement, connexité, non commutativité et *simplicité* via son action sur la sphère unité S^2.

On s'intéressera alors notamment à deux types bien différents de sous-groupes.

D'une part l'action sur S^2 permettra de classer tous les *sous-groupes finis* de SO(3), et de les identifier comme les sous-groupes d'isométries positives laissant invariants un polygone ou un polyèdre régulier de $\mathbb{R}^3$ (les groupes obtenus sont les groupes cycliques, les groupes diédraux, et les groupes de permutation A_4, S_4 et A_5). On complétera l'étude en examinant leurs *représentations* (voir le cours d'Algèbre 2) : pour les trois derniers on verra qu'un des « caractères » de leur « table » est la trace de leur présence comme sous-groupe dans $\mathrm{SO}(\mathbb{R}^3)$, et on pourra éventuellement même en déduire cette présence.

D'autre part, on exhibera certains sous-groupes infinis engendrés par deux rotations a et b, sans relation non triviale entre elles. En particulier on étudiera l'exemple donné par Felix Hausdorff de telles rotations vérifiant $a^2 = b^3 = id$, qui est la base de son *paradoxe* (1914) : la sphère S^2 est la réunion disjointe d'un ensemble dénombrable et de trois parties isométriques X, Y et Z, telles que $Y = b(X)$, $Z = b(Y)$, et $X = a(Y \cup Z)$. Autrement dit X est isométrique à Y et à son double $Y \cup Z$! Ce paradoxe est le point de départ du célèbre paradoxe de Banach-Tarski (1924).

Bibliographie

Philippe Caldero, Jérôme Germoni, *Histoires hédonistes de groupes et de géométries, Tome second*, Calvage & Mounet, 2015, chapitres IX et X.

Bertram Huppert, *Character theory of finite groups*, de Gruyter, 1998, §29.

Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996, chapitre VI.

Stan Wagon, *The Banach-Tarski paradox*, Encyclopedia of mathematics, Volume 24, Cambridge, 1985, chapitres 2 et 3.

11 Groupe fondamental et SO(3)

Ou :

Pourquoi une rotation d'un angle 2π n'est pas l'identité (mais une rotation d'un angle 4π l'est...)

Le groupe fondamental $\pi_1(T, t)$ d'un espace topologique T contenant un point t est un invariant qui donne une réponse rigoureuse à la question floue : combien l'espace

T contient-il de trous ? Par ailleurs, lorsque l'espace T est « assez gentil », on peut construire à l'aide du groupe fondamental un recouvrement universel $V \to T$ qui a la propriété de « déplier » totalement l'espace T.

Le travail proposé consiste à étudier la construction du groupe fondamental et du recouvrement universel. On les calculera tous les deux dans des cas importants (surfaces compactes, certains groupes géométriques) en s'attardant particulièrement sur le cas du groupe fondamental de SO(3). On verra que dans ce cas le groupe fondamental est $\mathbb{Z}/2\mathbb{Z}$ et que le recouvrement universel peut être muni d'une structure de groupe isomorphe à SU(2). Le cas échéant, on verra comment cet exemple, anecdotique de prime abord, est en fait relié à la physique des particules, où c'est un élément central de notre compréhension de la notion de spin des particules sous-atomiques.

Pré-requis Algèbre et topologie de L3.

Bibliographie

William S. Massey, *Algebraic Topology.*

Joseph J. Rotman, *An introduction to Algebraic Topology.*

Marcel Berger, *Géométrie.*

12 Groupes aléatoires et petites simplifications

En 2003, Mikhail Gromov a proposé des modèles de présentations de groupes aléatoires. Dans ces modèles, on prend un ensemble à quatre elements $\{a, b, a^{-1}, b^{-1}\}$, qui sera l'ensemble générateur du groupe. On choisit $L > 0$, et d dans $]0, 1[$, et on sélectionne aléatoirement (indépendamment et uniformément) $4 \cdot 3^{dL}$ éléments parmi les $4 \cdot 3^L$ mots réduits de longueur $L + 1$. On déclare que ce sont les relations de la présentation du groupe.

Si $d > 1/2$, alors, avec grande probabilité, le groupe obtenu est trivial ou $\mathbb{Z}/2\mathbb{Z}$.

Si $d < 1/2$, alors, avec grande probabilité, le groupe obtenu est infini, non-abélien (et même hyperbolique).

On se propose d'explorer le modèle, un sens, et une preuve du premier énonce reposant sur le paradoxe des anniversaires. Pour le deuxième énoncé, on se propose de se restreindre à $d < 1/12$, et de relier ces présentations à celles traitées par la théorie de la petite simplification dans les présentations de groupes.

Selon qu'on a le temps d'approfondir le remplacement de la combinatoire par la géométrie, on pourra tenter de comprendre ce que veut dire la mention sybilline « et même hyperbolique » ci-dessusus, et pourquoi le résultat reste vrai pour tout $d < 1/2$.

Bibliographie

Yann Ollivier, *A January 2005 invitation to random groups*, Sociedade Brasileira de Matemática, 2005.
`http://www.yann-ollivier.org/rech/publs/randomgroups.pdf`

Roger C. Lyndon, Paul E. Schupp, *Combinatorial group theory*, Classics in Mathematics, 2013, Reprint of the original edition, Springer, 1977.

13 Inégalités de concentration et applications

Les inégalités de concentration donnent des majorants de la probabilité qu'une variable aléatoire X s'éloigne d'une certaine valeur prescrite (généralement sa moyenne ou sa médiane). Un exemple simple est l'inégalité de Bienaymé-Tchebychev : soit X une variable aléatoire de carré intégrable, de variance σ^2, alors, pour tout $a > 0$,

$$\mathbb{P}\left(|X - \mathbb{E}\left[X\right]| \geq a\right) \leq \frac{\sigma^2}{a^2}.$$

Le but du projet est d'étudier plusieurs inégalités de concentration (inégalités de Hoeffding, de Bernstein, etc.) et quelques unes des principales méthodes utilisées pour les obtenir. On pourra également s'intéresser à leur utilisation dans un ou plusieurs cadres d'application (par exemple, matrices aléatoires, sommes permutées, statistique).

Pré-requis Probabilités de L3.

Bibliographie

Stéphane Boucheron, Gabor Lugosi, Pascal Massart, *Concentration inequalities : A nonasymptotic theory of independence*. Chapitres 1 et 2.
`https://hal.archives-ouvertes.fr/hal-00942704/`

14 Inégalités géométriques et courbure positive

Dans le cadre bien connu de la géométrie riemannienne, la courbure positive implique des inégalités géométriques comme celles de Poincaré ou de Brunn-Minkowski. Ces inégalités ont de nombreuses applications. Le but du travail proposé est de comprendre comment, dans un espace métrique mesuré, on peut étendre ces résultats sous une condition de courbure positive au sens du transport optimal.

Pré-requis

Théorie de la mesure et calcul différentiel de L3, Analyse fonctionnelle de M1, aucun prérequis en géométrie différentielle.

Bibliographie

Cédric Villani, *Optimal transport, old and new*, Springer (2008).
`http://cedricvillani.org/wp-content/uploads/2012/08/preprint-1.pdf`

15 Des inégalités isopérimétriques à la géométrie sous-riemannienne de contact

Le problème de départ remonte à l'Antiquité : la légende de la fondation de Carthage raconte que la princesse Elisha de Tyr (également connue sous le nom de Dido) aurait été chassée de Tyr et qu'elle se serait réfugiée dans l'actuelle Tunisie, où on lui aurait concédé tout le territoire que pourrait enfermer une peau de bœuf. Elisha aurait alors découpé cette peau en une longue bande de plusieurs kilomètres de longueur, ce qui lui aurait permis de délimiter un territoire conséquent et ainsi de fonder Carthage.

Elisha de Tyr a donc cherché la forme que doit prendre cette bande (pour nous, une courbe de longueur donnée) afin de délimiter la surface la plus grande possible.

Le travail proposé consiste à étudier le lien entre cette question et la géométrie sous-riemannienne de contact, ce qui fournit une occasion de découvrir une version simple du principe du maximum de Pontryagin, théorème fondamental de la théorie du contrôle optimal.

Bibliographie

Lev S. Pontriaguine, Vladimir G. Boltianski, Revaz V. Gamkrelidze, Evgeni F. Michtchenko, *Théorie mathématique des processus optimaux*. Moscou, Éditions Mir (1974).

Davide Barilari, *A comprehensive introduction to sub-riemannian geometry.*
`https://webusers.imj-prg.fr/~davide.barilari/Notes.php`

16 Irrationalité des valeurs de la fonction zeta de Riemann sur les entiers

La fonction zeta de Riemann, définie par $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ pour tout nombre complexe s tel que $\mathrm{Re}(s) > 1$, est une fonction méromorphe qui s'étend à $\mathbb{C} \setminus \{1\}$ par prolongement analytique. Cette fonction mystérieuse, fortement liée à la distribution des nombres premiers et objet d'un problème à un million de dollars, intrigue les mathématiciens depuis Euler. Dans ce sujet, on propose d'effleurer l'immense littérature consacrée à la fonction zeta à travers une question simple : les valeurs $\zeta(m)$ de cette fonction en les entiers positifs m sont-elles rationnelles ?

Pour les valeurs paires de m, Euler fut le premier à résoudre la question, en donnant une formule explicite pour $\zeta(2k)$ pour tout k entier positif. Presque trois cents ans plus

tard, et alors que la fonction zeta s'est rapidement imposée comme un objet d'étude majeur de la théorie des nombres, on ne sait presque rien des valeurs $\zeta(2k+1)$ pour les entiers positifs impairs $2k+1$. Ainsi, il a fallu attendre 1979 pour voir apparaître une démonstration, due à Roger Apéry, de l'irrationalité de $\zeta(3)$. En 2000, Keith Ball et Tanguy Rivoal ont établi l'existence d'une infinité de valeurs irrationnelles de zeta sur les entiers impairs.

Le travail proposé consiste à établir la formule d'Euler et à étudier la démontration du théorème d'Apéry.

Pré-requis

Cours d'analyse complexe, et une absence d'aversion pour les séries entières.

Bibliographie

Frits Beukers, *A note on the irrationality of* $\zeta(2)$ *and* $\zeta(3)$. Bulletin of the London Mathematical Society, Volume 11, Issue 3, 1979, 268-272.

Alfred van der Poorten, Roger Apéry, *A proof that Euler missed... An informal report.* The Mathematical Intelligencer, 1979, Volume 1, Issue 4, 195-203.

Martin Aigner, Günter M. Ziegler, *Proofs from the Book*, Springer, 1998.

17 Jeux stochastiques, application au jeu du *Qui est-ce ?*

Dans un jeu stochastique, les joueurs agissent sur l'environnement dans des buts différents et possiblement contradictoires. C'est le cas particulier des jeux à somme nulle pour lesquels un gain pour un joueur se traduit par une perte pour les autres. Les deux principales questions en théorie des jeux sont l'existence d'une stratégie optimale (souvent obtenue par un argument de compacité), et la valeur du gain pour un joueur très patient (grand nombre de répétitions) sous la stratégie optimale.

Le but du projet est d'étudier le cadre des jeux stochastiques dans les notes de cours de Rida Laraki et/ou le livre de Sylvain Sorin donnés en référence, et l'application de cette théorie pour la stratégie optimale au jeu du « Qui est-ce ? »

Pré-requis Probabilités de L3.

Bibliographie

Rida Laraki, *Jeux Stochastiques.*
`http://www.math.polytechnique.fr/xups/xups06-04.pdf`

Sylvain Sorin (2002). *A first course on zero-sum repeated games*, Springer, chapitres 1 et 5.

Mihai Nica (2016). *Optimal Strategy in "Guess Who ?" : Beyond Binary Search.*
`https://arxiv.org/abs/1509.03327`

18 Marches auto-évitantes, constante de connectivité

Une *marche aléatoire auto-évitante* sur un réseau est un chemin sur ce réseau qui ne passe jamais deux fois par le même sommet. Si c_n désigne le nombre de tels chemins, issus d'un sommet d'origine fixé et de longueur n, un argument de sous-multiplicativité implique qu'il existe une constante μ, dépendant du réseau, pour laquelle $c_n = \mu^{n+o(n)}$. Cette constante μ porte le nom de *constante de connectivité* du réseau et on ne sait pas en général calculer sa valeur.

Un résultat marquant obtenu récemment par Hugo Duminil-Copin et Stanislav Smirnov est que, pour le réseau hexagonal (en « nid d'abeille »), $\mu = \sqrt{2+\sqrt{2}}$.

Le but du travail proposé est de comprendre ce résultat, qui a la particularité d'être obtenu par des méthodes élémentaires (mais très astucieuses).

Pré-requis Un peu d'analyse complexe, de combinatoire et de séries entières.

Bibliographie

Hugo Duminil-Copin, Stanislav Smirnov, *The connective constant of the honeycomb lattice equals* $\sqrt{2+\sqrt{2}}$, Annals of Mathematics 175 (2010), 1653–1665.
`https://arxiv.org/abs/1007.0575`

Neil Madras, Gordon Slade, *The Self-avoiding Walk*, Birkhäuser, 1993.

19 Mélanges

Dans la théorie de la statistique enseignée en M1, on suppose que les observations sont indépendantes et issues d'une même loi. En pratique, il peut arriver que plusieurs lois soient en présence : considérer par exemple le cas d'impacts de balles provenant d'un seul tireur ou de plusieurs. La problématique en présence de plusieurs lois est qu'on ne sait pas quelle observation est obtenue à partir de quelle loi.

Le but du travail proposé est d'étudier l'estimation des lois et l'appartenance de chaque observation à chaque groupe. Un intérêt pour la programmation serait bienvenu pour pouvoir aborder certains aspects de la problématique.

Pré-requis Statistique, estimation, programmation.

20 Modules projectifs

Si k est un corps, les k-espaces vectoriels de dimension finie sont très faciles à comprendre puisqu'ils sont classés à isomorphisme près par leur dimension. Lorsque on remplace k par un anneau commutatif R, le premier réflexe est de considérer les R-modules libres de type fini, qui sont une généralisation évidente des k-espaces vectoriels. Malheureusement, un facteur direct d'un module libre n'est en général pas libre et cette notion s'avère donc trop restrictive dans de nombreuses situations. Ces considérations mènent naturellement à la notion de module projectif, qui est par définition un facteur direct d'un module libre.

Le but du travail proposé est de comprendre la notion de module projectif, puis de démontrer le théorème de classification des modules projectifs sur un anneau de Dedekind.

Pré-requis Algèbre de L3.

Bibliographie

Grégory Berhuy, *Modules : théorie, pratique... et un peu d'arithmétique*, Calvage & Mounet, 2012.

21 Nombres chanceux d'Euler et factorialité

En 1772, Leonhard Euler remarque que la suite des nombres $f(n) = n^2 + n + 41$ pour n entier fournit un nombre premier pour *chaque* valeur de n entre 0 et 39. On dit aujourd'hui que 41 est un nombre chanceux d'Euler.

Par ailleurs, l'expérimentation montre que $f(n)$ est premier pour de nombreuses valeurs de n (mais actuellement on ne sait pas prouver si ce fait se produit pour une infinité de valeurs de n).

La stratégie consistant à utiliser un anneau plus grand que $\mathbb{Z}$ pour y obtenir des factorisations est classique : ainsi l'anneau euclidien des entiers de Gauss permet de décrire précisément les entiers sommes de deux carrés, et une première étape dans la preuve du grand théorème de Fermat consiste à passer dans l'anneau $\mathbb{Z}[\zeta]$ engendré par ζ une racine p-ième de l'unité, où l'expression $z^p - y^p$ est produit de p facteurs ; malheureusement pour $p \geqslant 23$ cet anneau n'est pas factoriel...

Concernant les nombres chanceux d'Euler, les entiers $f(n)$ sont chacun la norme d'un élément de l'anneau d'entiers quadratiques $A_d = \mathbb{Z}[\frac{1+i\sqrt{d}}{2}]$ avec $d = 163$. On étudiera la factorialité des anneaux A_d pour d sans facteur carré tel que $1 \leqslant d \leqslant 200$ (seuls sept d'entre eux sont factoriels), et on établira que le phénomène remarqué par Euler est équivalent à cette factorialité. Au passage, on étudiera deux théorèmes très utiles en arithmétique : la loi de réciprocité quadratique et le théorème de Minkowski sur

l'existence de points proches de l'origine dans un réseau.

Bibliographie

Daniel Perrin, *Pourquoi y a-t-il beaucoup de nombres premiers de la forme n^2+n+41 ?*
`https://www.math.u-psud.fr/~perrin/journeedu2311/redaction2311e.pdf`

Daniel Perrin, *Anneaux d'entiers des corps quadratiques imaginaires*, §5.
`https://www.math.u-psud.fr/~perrin/TER/anneauxd%27entiers.pdf`

Gaëtan Chenevier, *Théorie géométrique des nombres, cours à l'X*, 2018.
`http://gaetan.chenevier.perso.math.cnrs.fr/MAT552/cours2.pdf`

Ian Stewart, David Tall, *Algebraic number theory and Fermat's last theorem*, AK Peters, 2002, chapitre 7.

22 Orbites de familles de champs de vecteurs

On propose de lire et de comprendre la preuve du théorème de Sussmann.

On se donne k champs de vecteurs sur une variété connexe M. Le théorème de Sussmann, démontré en 1973, établit que l'orbite de tout point de M, c'est-à-dire l'ensemble des points que l'on peut obtenir à partir de ce point en intégrant alternativement ces champs de vecteurs en temps positifs ou négatifs, est une sous-variété immergée de M.

Ce résultat permet de retrouver le théorème de Chow-Rashevskii, obtenu en 1938-1939, qui, sous des hypothèses locales en chaque point de la variété, assure que l'orbite de chaque point est la variété toute entière.

Les théorèmes de Sussmann et de Chow-Rashevskii sont fondamentaux en théorie du contrôle, où il s'agit de répondre à la question dite de la contrôlabilité d'un système donné, c'est-à-dire de la possibilité effective d'amener le système d'un état à un autre.

Bibliographie

Hector J. Sussmann, *Orbits of Families of Vector Fields and Integrability of Distributions*, Transactions of the American Mathematical Society, Vol. 180, 171-188 (1973).
`https://www.ams.org/journals/tran/1973-180-00/S0002-9947-1973-0321133-2/`

23 Pavages impossibles et groupes de Conway

Exemple 1 : on peut paver le carré 8×8 avec des rectangles de taille 1×2.
Exemple 2 : on ne peut pas paver le carré 8×8 privé de l'un de ses coins, avec des rectangles de taille 1×2.
Question (exemple 3) : peut-on paver le carré 8×8 privé de deux de ses coins diagonalement opposés, avec des rectangles de taille 1×2 ?

S'il est facile de donner une raison convaincante pour l'exemple 1 et pour l'exemple 2, répondre à la question de l'exemple 3 demande une idée interessante (ingénieuse, mais simple).

Cette idée s'applique à d'autres situations, mais seule, elle est insuffisante pour aller bien loin.

Pour aller plus loin, ce qui est l'objet du sujet proposé, on peut associer un objet algébrique aux tuiles que l'on a le droit d'utiliser, introduire le groupe de Conway, et explorer diverses ramifications.

Bibliographie

Dmitry Fuchs, SergeTabashnikov, *Mathematical Omnibus*, Lecture 23.
`http://www.math.psu.edu/tabachni/Books/taba.pdf`

William P. Thurston, *Conway's tiling groups*, Amer. Math. Monthly, Volume 97 Issue 8, 1990, 757-773.

Voir aussi les références indiquées par Igor Pak dans `http://www.math.ucla.edu/~pak/lectures/ribbon.html`.

24 Petit et grand théorèmes de Picard, le point de vue géométrique

Le petit théorème de Picard affirme qu'une fonction entière non constante prend toutes les valeurs complexes sauf peut-être une. Le grand théorème de Picard affirme qu'une fonction holomorphe possédant une singularité essentielle prend dans tout voisinage de cette singularité toutes les valeurs complexes sauf peut-être une.

Il existe de nombreuses preuves de ces deux résultats. On propose d'étudier une approche de nature géométrique, utilisant la notion de métrique sur un domaine du plan complexe et la notion de courbure.

Poincaré a introduit une distance sur le disque unité, appelée distance de Poincaré et base de la géométrie hyperbolique. Pour celle-ci toute fonction holomorphe du disque dans le disque rapproche les points. La courbure de la métrique de Poincaré sur le disque est constante et vaut -4 et en fait, le lemme d'Ahlfors, qui est une extension du lemme de Schwarz, affirme que toute métrique sur un domaine du plan complexe dont la courbure est majorée par -4 est « plus petite » que la métrique de Poincaré . En construisant une métrique sur le plan complexe moins deux points, de courbure majorée par un nombre strictement négatif, on arrivera ainsi à prouver que toute fonction holomorphe sur $\mathbb{C}$ à valeurs dans $\mathbb{C}\setminus\{0,1\}$ est constante. La preuve du grand théorème de Picard nécessitera, quant à elle, d'obtenir une généralisation du théorème de Montel.

Ce travail sera aussi l'occasion de découvrir des géométries non euclidiennes, la géométrie hyperbolique et la géométrie sphérique.

Pré-requis Cours de fonctions holomorphes du premier semestre de M1.

Bibliographie

Steven G. Krantz, *Complex analysis : the geometric viewpoint.*

25 Plan hyperbolique et surface modulaire

On étudiera quelques propriétés de la surface modulaire, qui est le quotient du demi-plan supérieur par l'action du groupe $\mathrm{SL}(2,\mathbb{Z})$.

Le premier objectif sera de comprendre la géométrie invariante par l'action de $\mathrm{SL}(2,\mathbb{R})$, qui est un modèle du plan hyperbolique. On explicitera un domaine fondamental pour l'action de $\mathrm{SL}(2,\mathbb{Z})$, et on en déduira une présentation de $\mathrm{SL}(2,\mathbb{Z})$ en termes de générateurs et relations.

On pourra étudier les propriétés des sous-groupes de congruences, et/ou le lien avec les courbes elliptiques sur $\mathbb{C}$.

Bibliographie

Alan F. Beardon, *The Geometry of Discrete Groups*, chapitre 7.

Éric Reyssat, *Quelques Aspects des Surfaces de Riemann*, chapitre X.

Lars V. Ahlfors, *Complex Analysis*, chapitre 7.

26 Ruptures

Dans le cas de données temporelles, les observations peuvent être indépendantes mais la loi des observations peut être différente entre deux instants suffisamment éloignés. Ce modèle s'appelle un modèle de ruptures. On propose d'étudier ces modèles et en particulier les estimateurs du maximum de vraisemblance des instants de ruptures et des paramètres des lois, dans les cadres paramétrique et non-paramétrique. Un intérêt pour la programmation n'est pas obligatoire mais permettrait des ouvertures à ce projet.

Pré-requis Statistique, estimation.

27 Le spin comme une conséquence de la théorie des représentations

L'apparition du spin dans la mécanique quantique peut être expliquée à partir du lien entre la théorie des représentations projectives des groupes et la théorie des représenta-

tions linéaires des recouvrements universels associés. En effet, un théorème de Wigner affirme que les symétries de la mécanique quantique sont données par des applications unitaires ou anti-unitaires de l'espace de Hilbert de base, ce qui induit une représentation projective du groupe $\mathrm{SO}(3,\mathbb{R})$ pour le cas des rotations. À partir du lien mentionné ci-dessus, on trouve alors des représentations linéaires du recouvrement universel $\mathrm{SU}(2)$, dont les pièces irréductibles donnent les spins possibles.

Le travail proposé consiste à étudier une formulation élémentaire de la mécanique quantique et en particulier le théorème de Wigner, qui permettra ensuite d'introduire la notion de spin. Pour cela, on étudiera les notions basiques de la théorie des représentations projectives (sur des espaces de Hilbert) des groupes, ainsi que le lien avec la théorie des représentations linéaires des recouvrements universels respectifs. On étudiera spécialement le cas du groupe $\mathrm{SO}(3,\mathbb{R})$ et de son recouvrement universel $\mathrm{SU}(2)$.

Pré-requis Topologie et algèbre de L3.

Bibliographie

Alexander Holevo, *Probabilistic and statistical aspects of quantum theory*, Second edition, Springer, 2011.

Veeraualli Seshadri Varadarajan, *Geometry of quantum theory*, Second edition, Springer, 1985.

28 Le terminateur de la Lune

En 1609, Galilée vient de construire une lunette astronomique. Il remarque, entre autres choses merveilleuses, que le terminateur de la Lune, c'est-à-dire la ligne qui sépare l'ombre et la lumière sur notre satellite, n'est pas régulier, ce qui indique l'existence d'un relief.

Le travail proposé consiste à réfléchir à la géométrie de cette ligne. Ce sujet est ouvert, puisque l'encadrant.e ne connaît pas de réponse à la question et n'est pas sûr.e qu'une telle réponse soit même connue.

Pour une introduction passionnante au problème, on se réfèrera à deux articles parus sur le site web *Images des mathématiques*, écrits par Étienne Ghys et Jos Leys :

Il y a quatre cents ans... Sidereus Nuncius.
`http://images.math.cnrs.fr/il-y-a-quatre-cents-ans-sidereus.html`

Sidereus Nuncius... aujourd'hui.
`http://images.math.cnrs.fr/Sidereus-Nuncius-aujourd-hui.html`

On attend donc de l'étudiant.e qu'il ou elle modélise le problème et, en le simplifiant selon ses vœux, qu'elle ou il lui trouve des éléments de réponse.

29 Théorème des nombres premiers et hypothèse de Riemann

L'identité d'Euler $\zeta(s) = \sum_{n \geqslant 1} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1-p^{-s}}$ valable pour $\mathrm{Re}(s) > 1$ permet de relier les propriétés de la fonction ζ de Riemann à la répartition des nombres premiers.

Soit $\pi(x)$ le nombre de nombres premiers inférieurs ou égaux à x. Le théorème des nombres premiers affirme que $\pi(x)$ est équivalent à $\frac{x}{\ln x}$ quand x tend vers $+\infty$. Ce théorème est équivalent au fait que la fonction ζ n'a pas de zéros sur la droite $\mathrm{Re}(s) = 1$. La première partie de ce travail consistera à prouver cette équivalence.

L'hypothèse de Riemann dit que les zéros s non triviaux de ζ sont tous situés sur la droite $\mathrm{Re}(s) = \frac{1}{2}$. On peut montrer que cette conjecture est équivalente à l'estimation $\pi(x) - \mathrm{li}(x) = O(\sqrt{x} \ln x)$ où li est la fonction logarithme intégral. Ces considérations feront l'objet de la seconde partie du travail.

Pré-requis Cours de fonctions holomorphes du premier semestre de M1.

Bibliographie

Elias M. Stein, Rami Shakarchi, *Complex analysis*.

Don Zagier, *Newman's short proof of the Prime Number Theorem*, American Mathematical Monthly 104 (1997), no. 8, 705-708.
`https://people.mpim-bonn.mpg.de/zagier` (aller au paragraphe « Other articles (announcements, expository, recreational) », item 23)

30 Théorie de Morse

La théorie de Morse fournit une compréhension de la topologie d'une variété différentiable compacte à partir d'une fonction différentiable, plus précisément, à partir de son flot de gradient et de ses points critiques. L'un des corollaires les plus importants est que la somme des nombres de Betti de la variété, des invariants topologiques, est toujours plus petite que le nombre de points critiques d'une fonction sur cette variété. Un corollaire de ce corollaire est trivial mais instructif : une fonction définie sur une variété compacte possède toujours au moins au moins deux points critiques.

Dans ce contexte, le travail proposé consiste à lire et à comprendre le livre de John Milnor intitulé *Morse Theory*.