Université Grenoble Alpes **2019-2020**
M1 Mathématiques générales

Sujets de TER

Mode d'emploi : Envoyer au responsable du M1 un message indiquant votre nom et les numéros des quatre sujets sur lesquels vous souhaiteriez travailler, classés par ordre de préférence décroissante. Le titre du message doit obligatoirement inclure la chaîne de caractères `M1 MG TER`. Date limite d'envoi : mardi 3 décembre 23h59.

1. Autour du théorème de de Branges
2. Autour du théorème de la représentation conforme de Riemann
3. Bases de Gröbner et algèbres de Fomin-Kirillov
4. Bases de Gröbner et algèbres de Fomin-Kirillov duales
5. Biais de publication
6. Cadran solaire digital
7. Codes pour la métrique du rang
8. Comment croissent les groupes
9. Équation des ondes
10. Factorisation de polynômes à coefficients rationnels
11. Fonctions maximales de Hardy-Littlewood
12. Fonctions zêta d'Ihara sur des graphes et des groupes
13. Géométrie hyperbolique, groupes fuchsiens
14. Géométrie sphérique, caractéristique d'Euler et homologie simplicielle
15. Inégalités isodiamétriques et isopérimétriques
16. Jeux stochastiques : application au jeu du « Qui est-ce ? »
17. Lois de réciprocité
18. Lois Zêta pour l'arithmétique
19. Mélanges de cartes
20. Méthode de Coppersmith et applications cryptographiques
21. Métrique de Schwarzschild
22. Orbites de familles de champs de vecteurs
23. Parallélisabilité des sphères
24. Pavages par dominos et modèle des dimères
25. Période trois implique chaos et théorème de Sharkovsky
26. Problème de Schoenflies
27. Théorie de Floquet
28. Théorie du complot
29. Voyage sur les groupes de Lie

1 Autour du théorème de de Branges

En 1916, Ludwig Bieberbach démontre que, si une fonction analytique $z \mapsto z + a_2 z^2 + a_3 z^3 + \cdots$ est injective sur le disque unité D, alors $|a_2| \leqslant 2$. De plus, Bieberbach conjecture que $|a_n| \leqslant n$ pour tout $n \geqslant 2$ et que toutes ces inégalités sont strictes à part pour les rotations de la fonction de Koebe k, définie par $k(z) = \frac{z}{(1-z)^2}$. Cette conjecture, démontrée par Louis de Branges en 1984, permet de relier la structure analytique et le comportement géométrique d'une classe de fonctions, à savoir les fonctions univalentes sur D (c'est-à-dire, définies et injectives sur D).

La preuve du théorème de de Branges est hors de portée d'un travail de TER. Par conséquent, après s'être familiarisé avec le sujet par quelques calculs explicites, on s'intéressera dans un premier temps à la preuve originelle par Bieberbach que $|a_2| \leqslant 2$, basée sur le théorème de l'aire, et à quelques conséquences de ce résultat comme le théorème du quart de Koebe et le théorème de la distorsion.

Dans un second temps, on se tournera vers la preuve que $|a_n| < en$ pour tout n, due à John Edensor Littlewood en 1925, et vers la preuve de la conjecture de Bieberbach quand tous les coefficients a_n sont réels, due à Jean Dieudonné en 1931. Puis, si le temps le permet, on abordera la preuve que $|a_3| \leqslant 3$, due à Charles (Karl) Loewner en 1923. La démonstration de ce dernier résultat est basée sur une équation d'évolution, introduite par Loewner à cet effet et portant son nom depuis, utilisée plus tard par de Branges dans sa preuve de la conjecture complète, et réutilisée depuis le début des années 2000 par Oded Schramm, Greg Lawler, Wendelin Werner et d'autres, pour décrire la limite d'échelle de divers modèles probabilistes sur des réseaux planaires, issus de la mécanique statistique.

Prérequis

Le cours d'Analyse complexe du premier semestre.

Bibliographie

Conjecture de Bieberbach, page Wikipédia :
`fr.wikipedia.org/wiki/Conjecture_de_Bieberbach`

Jacob Korevaar (1986), Ludwig Bieberbach's Conjecture and Its Proof by Louis de Branges, The American Mathematical Monthly 93, n°7, 505-514. Disponible à l'adresse :
`www.maa.org/programs/maa-awards/writing-awards/ludwig-bieberbachs-conjecture-and-its-proof-by-louis-de-branges`

Terence Tao (2018), 246C Notes 3 : Univalent functions, the Loewner equation, and the Bieberbach conjecture. Disponible à l'adresse :
`terrytao.wordpress.com/2018/05/02/246c-notes-3-univalent-functions-the-loewner-equation-and-the-bieberbach-conjecture`

2 Autour du théorème de la représentation conforme de Riemann

Le théorème de la représentation conforme de Riemann montre que tout domaine simplement connexe du plan complexe différent du plan est biholomorphe au disque unité. Un domaine est simplement connexe si et seulement si les composantes connexes de son complémentaire sont toutes non bornées ce qui équivaut à dire que son complémentaire dans la sphère de Riemann est connexe. On va s'intéresser aux domaines comportant des trous et dans un premier temps aux couronnes $A_{r,R} = \{z \in \mathbb{C}\,;\, r < |z| < R\}$ où $0 < r < R$. Deux couronnes $A_{r,R}$ et $A_{r',R'}$ sont biholomorphes si et seulement si $R/r = R'/r'$.

On montrera ensuite que tout domaine doublement connexe du plan tel que les composantes connexes du complémentaire ne sont pas réduites à un point est biholomorphe à une couronne. Pour ceci, il faudra parler de problème de Dirichlet et de fonctions harmoniques, ce qui permettra d'étudier la preuve de Riemann du théorème de la représentation conforme.

Prérequis

Le cours d'Analyse complexe du premier semestre.

Bibliographie

Joseph L. Walsh (1973), History of the Riemann Mapping Theorem, The American Mathematical Monthly ; Vol. 80, n°3, 270-276.

Steven G. Krantz (2006), Geometric Function theory, Explorations in Complex Analysis, Birkhäuser.

Walter Rudin (2009), Analyse réelle et complexe, 3ème édition, Dunod.

Lars V. Ahlfors (1978), Complex analysis. An introduction to the theory of analytic functions of one complex variable. Third edition. International Series in Pure and Applied Mathematics. McGraw-Hill.

3 Bases de Gröbner et algèbres de Fomin-Kirillov

Les bases de Gröbner sont un outil très utilisé en algèbre commutative et noncommutative pour pouvoir manipuler des algèbres données par des générateurs et relations. Par ailleurs les algèbres de Fomin-Kirillov ont été introduites par Sergey Fomin et Anatol Kirillov dans leur étude de la cohomologie des variétés de drapeaux. Ces algèbres apparaissent aussi dans la classification des algèbres de Hopf de dimension finie, car il s'agit d'algèbres de Nichols.

Le but de ce TER est d'utiliser des techniques de bases de Gröbner pour calculer une base de Hamel des algèbres de Fomin-Kirillov à six générateurs ainsi que les constantes de structure pour le produit, à l'aide du logiciel GAP.

Prérequis

Algèbre de L3A et de M1.

Bibliographie

Sergey Fomin, Anatol N. Kirillov (1999), Quadratic algebras, Dunkl elements, and Schubert calculus, Advances in geometry, Progr. Math., vol. 172, Birkhäuser Boston, Boston, MA, 147-182.

Alexander Milinski, Hans-Jürgen Schneider (2000), Pointed indecomposable Hopf algebras over Coxeter groups, New trends in Hopf algebra theory (La Falda, 1999), Contemp. Math., vol. 267, Amer. Math. Soc., Providence, RI, 215–236. Disponible à l'adresse : `www.mathematik.uni-muenchen.de/~hanssch/Publications.html`.

Victor A. Ufnarovskij (1995), Combinatorial and asymptotic methods in algebra. Algebra, VI, 1–196, Encyclopaedia Math. Sci., 57, Springer, Berlin.

Victor A. Ufnarovskij (1998), Introduction to noncommutative Gröbner bases theory. (English summary) Gröbner bases and applications (Linz, 1998), 259–280, London Math. Soc. Lecture Note Ser., 251, Cambridge Univ. Press, Cambridge.

4 Bases de Gröbner et algèbres de Fomin-Kirillov duales

Les bases de Gröbner sont un outil très utilisé en algèbre commutative et noncommutative pour pouvoir manipuler des algèbres données par des générateurs et relations. Par ailleurs les algèbres de Fomin-Kirillov ont été introduites par Sergey Fomin et Anatol Kirillov dans leur étude de la cohomologie des variétés de drapeaux. Ces algèbres apparaissent aussi dans la classification des algèbres de Hopf de dimension finie, car il s'agit d'algèbres de Nichols. Comme ces algèbres sont quadratiques, elles possèdent des algèbres duales quadratiques.

Le but de ce TER est d'utiliser des techniques de bases de Gröbner pour calculer une base de Hamel des algèbres de Fomin-Kirillov duales à six générateurs ainsi que les constantes de structure pour le produit, à l'aide du logiciel GAP.

Prérequis

Algèbre de L3A et de M1.

Bibliographie

Sergey Fomin, Anatol N. Kirillov (1999), Quadratic algebras, Dunkl elements, and Schubert calculus, Advances in geometry, Progr. Math., vol. 172, Birkhäuser Boston, Boston, MA,147–182.

Alexander Milinski, Hans-Jürgen Schneider (2000), Pointed indecomposable Hopf algebras over Coxeter groups, New trends in Hopf algebra theory (La Falda, 1999), Contemp. Math., vol. 267, Amer. Math. Soc., Providence, RI, 215–236. Disponible à l'adresse : `www.mathematik.uni-muenchen.de/~hanssch/Publications.html`.

Victor A. Ufnarovskij (1995), Combinatorial and asymptotic methods in algebra. Algebra, VI, 1–196, Encyclopaedia Math. Sci., 57, Springer, Berlin.

Victor A. Ufnarovskij (1998), Introduction to noncommutative Gröbner bases theory. (English summary) Gröbner bases and applications (Linz, 1998), 259–280, London Math. Soc. Lecture Note Ser., 251, Cambridge Univ. Press, Cambridge.

Chelsea Walton, James J. Zhang (2019), On the quadratic dual of the Fomin-Kirillov algebras. Trans. Amer. Math. Soc. 372, no. 6, 3921–3945.
Preprint `arXiv:1806.09263[math.RA]`.

5 Biais de publication

D'après Confucius, « L'homme sage apprend de ses erreurs et l'homme encore plus sage apprend des erreurs des autres ». On pourrait donc s'attendre à ce que les revues scientifiques publient avec même valeur les résultats *probants* et les *non* résultats, ce qui, on l'aura compris, n'est évidemment pas le cas. Les chercheur·se·s et les revues scientifiques ont plutôt tendance à ne publier que les résultats jugés *statistiquement significatifs* et à laisser de côté les résultats non concluants, ce qu'on appelle un *biais de publication*.

Le but de ce TER est d'étudier la modélisation du biais de publication et la possibilité (ou non) de le compenser, notamment en étudiant l'article donné en référence.

Bibliographie

Jeffrey D. Scargle (1999), Publication bias (the "file-drawer problem") in scientific inference. Preprint `arXiv:physics/9909033[physics.data-an]`.

6 Cadran solaire digital

En 1987, Kenneth Falconer montre qu'il existe une façon de construire un objet physique dont l'ombre à chaque heure est cette heure écrite en chiffres.

Plus mathématiquement, étant donnée une famille $(\theta_i)_{i\in I}$ de directions dans l'espace de dimension 3 et une famille $(A_i)_{i\in I}$ d'ensembles mesurables dans le plan, Falconer montre l'existence d'un ensemble mesurable A dans l'espace tel que, pour tout $i \in I$, la projection orthogonale de A sur un plan dans la direction θ_i est exactement A_i (à des

« presque partout » près).

Il existe plusieurs constructions d'un tel objet en plus de celle de Falconer, et le but du TER est d'en explorer quelques unes. Par exemple, on peut passer par la géométrie fractale, ou sous des hypothèses additionnelles sur les projections, réaliser A de manière explicite « par couches ». (C'est comme cela que sont fabriqués les cadrans solaires digitaux que l'on trouve dans le commerce.)

Si tout se passe bien, il sera possible de fabriquer pour de vrai un tel objet, et d'en faire la démonstration le jour de la soutenance.

Prérequis

Selon la méthode utilisée, un peu de théorie de la mesure, de la géométrie euclidienne en dimension 3, et (si tout se passe bien, donc) un peu de programmation et de travaux manuels.

Bibliographie

Kenneth Falconer (2003), *Fractal Geometry : Mathematical Foundations and Applications*. John Wiley and Sons.

Ian Stewart (1991), What in heaven is a digital sundial ?, Scientific American.

Un exemple : `www.fransmaes.nl/genk/en/gk-zw08-e.htm`.

7 Codes pour la métrique du rang

Les codes correcteurs d'erreurs sont des parties judicieusement choisies d'espaces vectoriels sur un corps fini (par exemple des sous-espaces), de sorte que la redondance que contiennent leurs éléments permette de retrouver le message initial en cas de perturbation modérée dans la transmission. Les codes pour la *métrique du rang* sont des sous-ensembles de l'espace des matrices de taille $m \times n$ à coefficients dans un corps $\mathbb{F}_q$, munis de la distance $d(M, M') = \mathrm{rg}(M - M')$. Introduits par Delsarte en 1978, ces codes suscitent toujours l'intérêt des chercheurs de par leur efficacité pour la transmission des informations en réseau.

L'objet de ce TER est l'étude de la théorie de base de ces codes. On y prouve des résultats analogues aux résultats classiques concernant les codes munis de la distance de Hamming : borne de Singleton sur la taille d'un code de distance minimale donnée, code dual d'un code linéaire et ses paramètres, identités de MacWilliams reliant les distributions de poids d'un code et de son dual, etc. Il s'agit aussi d'étudier les propriétés et des constructions des codes optimaux pour le rang, dits *MRD*, c'est-à-dire ceux pour lesquels la borne de Singleton est atteinte.

Prérequis

Algèbre linéaire élémentaire, dualité ; le cours d'Algèbre 1 sur les corps finis servira à l'occasion.

Bibliographie

Elisa Gorla, Alberto Ravagnani (2018), Codes Endowed With the Rank Metric, in Network Coding and Subspace Designs, M. Greferath et al. Eds., Springer, 3-23. Preprint `arXiv:1710.02067[cs.IT]`.

8 Comment croissent les groupes

Si G est un groupe de type fini, engendré par un ensemble fini S stable par passage à l'inverse, on définit $\gamma_{G,S} : \mathbb{N} \to \mathbb{N}$ la fonction de croissance du groupe G pour la partie S, comme associant à chaque entier naturel n le nombre $\gamma_{G,S}(n)$ d'éléments de G qui peuvent être écrits comme le produit d'au plus n éléments de S.

Le but de ce TER est d'observer quelques unes (au choix) des situations suivantes.

Le groupe G est fini si et seulement si $\gamma_{G,S}(n) = o(n)$ (pour S arbitraire). Un théorème plus subtil (dû à Jacques Justin, Alex Wilkie et Lou van den Dries), mais accessible ici, est que G possède un sous-groupe isomorphe à $\mathbb{Z}$, d'indice fini dans G si et seulement si $\gamma_{G,S}$ n'est pas bornée et $\gamma_{G,S}(n) = O(n)$.

Des exemples de croissance de groupes sont abordables : la croissance de tout groupe abélien de type fini (pour n'importe quelle partie génératrice finie) est bornée par une fonction polynomiale. Plus technique, la croissance de tout groupe nilpotent (en particulier le groupe de Heisenberg des matrices 3×3 sur $\mathbb{Z}$ triangulaires supérieures de diagonale 1) est bornée par une fonction polynômiale. La croissance de tout groupe libre de rang plus grand que 2 est minorée par une exponentielle (à nouveau, pour n'importe quelle partie génératrice finie).

Un théorème dû à John Milnor et Joseph A. Wolf dit que tout groupe résoluble dont la croissance est majorée par un polynôme, possède un sous-groupe nilpotent d'indice fini. (Hors de portée d'un TER plane ici un théorème dû à Mikhaïl Gromov, qui supprime l'hypothèse de résolubilité.)

Et en 1983, Rostislav Grigorchuk a fourni un exemple de groupe de croissance intermédiaire, c'est-à-dire tel que $\gamma_{G,S}(n) = o(a^n)$ pour tout $a > 1$ et $\gamma_{G,S}(n)$ est asymptotiquement supérieure à n'importe quel polynôme en n.

Bibliographie

Avinoam Mann (2011), How Groups Grow, London Mathematical Society, Lecture Notes Series 395 (chapitres 1 à 6, et 10).

9 Équation des ondes

Les équations des ondes figurent parmi les équations les plus importantes de la physique mathématique. Historiquement elles apparaissent d'abord dans une description de la vibration d'une corde. Elles peuvent être linéaires ou non linéaires. Les équations de Maxwell (linéaires) et les équations d'Einstein (non linéaires) possèdent des structures similaires. Dans ce stage on essaiera de comprendre quelques propriétés fondamentales des solutions de ces équations. On étudiera en détail les équations de Maxwell.

Prérequis

Les cours de M1 d'équations différentielles ordinaires et d'analyse fonctionnelle.

Bibliographie

Michael E. Taylor (1996), Partial Differential Equations 1 (Basic theory), Applied mathematical Sciences 115, Springer.

10 Factorisation de polynômes à coefficients rationnels

S'il est bien connu que tout polynôme de $\mathbb{Q}[X]$ se décompose de façon unique en produit de polynômes irréductibles, calculer une telle décomposition en pratique n'est pas un problème évident. Le but de ce TER est de comprendre le fonctionnement de l'algorithme récent de factorisation de van Hoeij et idéalement d'arriver à en implémenter quelques étapes sous SageMath.

L'idée principale est de commencer par calculer une factorisation modulo un nombre premier p (algorithme de Berlekamp ou de Cantor-Zassenhaus), puis de relever cette factorisation au corps $\mathbb{Q}_p$ des nombres p-adiques. La dernière phase, plus délicate, consiste à regrouper les facteurs obtenus dans $\mathbb{Q}_p[X]$ de façon à obtenir des éléments de $\mathbb{Q}[X]$.

Bibliographie

Alin Bostan et al. (2017), *Algorithmes Efficaces en Calcul Formel.* Preprint HAL `hal-AECF`.

11 Fonctions maximales de Hardy-Littlewood

Soit (X, d) un espace métrique muni d'une mesure (extérieure) μ. Si $f : X \to \mathbb{R}$ est mesurable, on pose, pour $x \in X$,

$$M(f)(x) = \sup_{R>0} \frac{1}{\mu(B(x,R))} \int_{B(x,R)} |f(y)| d\mu(y)$$

La fonction $M(f)$ s'appelle la fonction maximale de Hardy-Littlewood de f. La transformation $M : f \to M(f)$, introduite en 1930 par Godfrey Harold Hardy et John Edensor Littlewood, constitue un outil puissant en analyse harmonique.

Le but de ce TER est de démontrer que M est continue de L^p dans L^p pour $1 < p \leqslant +\infty$ et est faiblement continue dans L^1 dans les cas suivants :

1. $X = \mathbb{R}^n$ muni de sa structure euclidienne et μ est la mesure de Lebesgue. On utilise alors des techniques classiques d'analyse réelle comme des théorèmes d'interpolation et des approximations de l'identité.
2. (X, d) est un espace métrique quelconque et μ vérifie la condition dite de doublement du volume, à savoir que $\mu(B(x, 2r)) \leqslant c \cdot \mu(B(x, r))$ uniformément en x dans X et en $r > 0$. Dans ce cas, on utilise des lemmes de recouvrement de type Vitali.

Si le temps le permet, on donnera des applications en analyse de Fourier.

Prérequis

Théorie de la mesure de L3 et Analyse fonctionnelle de M1.

Bibliographie

Javier Duoandikoetxea (2000), Fourier Analysis, Graduate Studies in Mathematics 29, American Mathematical Society.

Juha Heinonen (2001), Lectures on analysis on metric spaces, Springer.

12 Fonctions zêta d'Ihara sur des graphes et des groupes

La fonction zêta de Riemann est un objet important associé à la répartition des nombres premiers, définie comme

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ premier}} \left(1 - \frac{1}{p}\right)^{-1}.$$

D'autres types de fonctions zêta peuvent être étudiés, qu'elles soient définies par un produit eulérien comme ci-dessus, ou comme solution d'une équation fonctionnelle (de Dedekind, associée à un corps de nombres, de Dirichlet, associée à une représentation, d'Epstein, associée à une forme quadratique...).

Dans ce TER, on s'intéresse à des fonctions zêta associées à des graphes (au sens des graphes constitués de sommets et d'arêtes), dites fonctions zêta d'Ihara. On part d'un graphe, on définit ce qu'est un “premier” pour le graphe en termes de cycles réduits, et on définit la fonction zêta par le produit eulérien analogue à la formule ci-dessus.

Cette fonction est liée au décompte de classes de conjugaison dans les groupes libres, munis d'une métrique.

Un résultat dans ce contexte, dû à Yasutaka Ihara, Hyman Bass et Ki-ichiro Hashimoto, exprime la fonction zêta comme un déterminant faisant intervenir la matrice d'adjacence et la matrice diagonale des degrés des sommets.

On pourra explorer la preuve de ce théorème, l'analogue du théorème des nombres premiers pour les cycles premiers d'un graphe, l'analogue de l'hypothèse de Riemann dans ce contexte, et pourquoi cette version de l'hypothèse de Riemann est vraie si et seulement si le graphe est un graphe dit de Ramanujan, c'est à dire, un graphe optimal pour une certaine inégalité spectrale pour sa matrice d'adjacence.

Il est possible d'opter pour une approche expérimentale du sujet, selon les goûts.

Bibliographie

Audrey Terras (2011), Zeta Functions of Graphs: A Stroll through the Garden. Cambridge Studies in Advanced Mathematics 128 (chapitres 1, 2, 6, 7, 10, 11).

13 Géométrie hyperbolique, groupes fuchsiens

Les cinq axiomes des Éléments d'Euclide, proposés aux alentours de 300 avant J.-C., troublèrent les mathématiciens presque dès leur invention. Le dernier axiome, stipulant que par chaque point il passe une unique droite parallèle à une droite donnée, paraissait peu naturel en comparaison des autres, et on espérait redonner une harmonie complète à la théorie en réduisant cet axiome au rang de théorème, démontré à partir des quatre axiomes « naturels ». De nombreuses démonstrations erronées de l'axiome des parallèles ont été données.

Plus de deux mille ans après les travaux d'Euclide, les premiers exemples de géométries non euclidiennes, c'est-à-dire des espaces vérifiant tous les axiomes d'Euclide sauf le postulat des parallèles, furent donnés. On les connaît aujourd'hui sous le nom d'espaces hyperboliques. Dans ce TER, nous étudierons ces espaces, leurs droites, leurs formules trigonométriques, leurs groupes d'isométries. Le cas échéant, on élargira la thématique du travail en s'intéressant à leurs sous-groupes discrets et à leurs liens avec la classification des surfaces de Riemann via le théorème d'uniformisation.

Bibliographie

Svetlana Katok (1992), Fuchsian Groups, Chicago Lectures in Mathematics, University of Chicago Press.

14 Géométrie sphérique, caractéristique d'Euler et homologie simplicielle

Le caractéristique d'Euler est un objet mathématique dont la forme le plus simple peut s'expliquer à des collégiens et la forme la plus compliquée est encore un sujet actuel de recherche.

Dans sa forme la plus simple, la formule d'Euler affirme que la somme du nombre de faces et du nombre de sommets d'un polyèdre est égale au nombre de ses arêtes plus deux. Nous verrons trois démonstrations de cette formule, l'une basée sur une récurrence sur la complexité du polyèdre, une deuxième basée sur les formules trigonométriques en géométrie sphérique (notamment un lien étonnant entre la somme des angles d'un triangle et son aire) et une troisième basée sur un invariant topologique sophistiqué : les groupes d'homologie simplicielle. À l'aide de cet invariant, nous verrons que la forme simple de la formule d'Euler énoncée ci-dessus, peut se généraliser à une classe très générale d'espaces topologiques.

Bibliographie

Mark A. Armstrong (1997), Basic Topology, Springer, Undergraduate Texts in Mathematics.

William S. Massey (1990), Algebraic topology : An introduction, Springer, Graduate Texts in Mathematics 56.

15 Inégalités isodiamétriques et isopérimétriques

Le but du stage est de démontrer les deux résultats suivants :

1. Si A est un sous-ensemble de $\mathbb{R}^n$ de diamètre d, alors sa mesure de Lebesgue est inférieure à celle d'une boule de même diamètre et il y a égalité si et seulement si A est une boule de diamètre d.
2. Si A est un sous-ensemble (régulier) de $\mathbb{R}^n$ de périmètre $P(A)$ (en un sens à donner), alors $V(A)^{(n-1)/n} \leqslant C_n \cdot P(A)$, où $V(A)$ désigne la mesure de Lebesgue de A et C_n est une constante explicite puisque C_n réalise l'égalité dans l'inégalité prćeédente si A est une boule.

Les démonstrations reposent sur des procédés de symétrisation. On étudiera quelques applications en analyse et en théorie géométrique de la mesure.

Prérequis

Théorie de la mesure et Calcul différentiel de L3.

Bibliographie

Lawrence Craig Evans, Ronald F. Gariepy (2015), Measure theory and fine properties of functions, Revised edition, CRC Press.

16 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 principales questions en théorie des jeux sont l’existence d’une stratégie optimale (argument de compacité), et la valeur du gain pour un joueur très patient (grand nombre de répétitions) sous la stratégie optimale.

Le but de ce TER est d’étudier le cadre des jeux stochastiques tel que présenté dans les notes de cours de Laraki et/ou le livre de Sorin, et l’application de cette théorie à la stratégie optimale pour le jeu du “Qui est-ce ?”.

Prérequis

Probabilités discrètes.

Bibliographie

Rida Laraki (2006), *Jeux Stochastiques*. Disponible à l’adresse :
`www.math.polytechnique.fr/xups/xups06-04.pdf`

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

Mihai Nica (2016), *Optimal Strategy in “Guess Who ?”: Beyond Binary Search*. Preprint `arXiv:1509.03327[math.PR]`.

17 Lois de réciprocité

Il est connu que pour p nombre premier impair qui ne divise pas l’entier a, la congruence $x^2 \equiv a \bmod p$ admet une solution si et seulement si $a^{\frac{(p-1)}{2}} \equiv 1 \bmod p$. Ceci s’exprime en termes d’un caractère (c’est-à-dire un morphisme dans $\mathbb{C}^\times$) d’ordre 2 du groupe $\mathbb{F}_p^\times$: le symbole de Legendre. Inversant la question, la *loi de réciprocité quadratique* permet de savoir, a étant fixé, pour quels premiers p la congruence $x^2 \equiv a \bmod p$ admet une solution. Cette loi fut d’abord formulée par Euler et Legendre, puis Gauss en donna la première preuve en 1801, la baptisant le *théorème d’or*.

Cette loi a par la suite été très largement généralisée, par étapes successives. Suivant Gauss et Eisenstein, qui introduirsient à cet effet les anneaux d’entiers euclidiens $\mathbb{Z}[i]$ et $\mathbb{Z}[j]$, on étudiera ici les *lois de réciprocité cubique* et *biquadratique* : la considération des carrés modulo un nombre premier y fait place à celle des cubes, puis des puissances quatrièmes, modulo un irréductible de ces anneaux, et on définit les généralisations adéquates du symbole de Legendre.

Plusieurs preuves de ces trois lois de réciprocité seront proposées ; on étudiera à cet effet les *sommes de Gauss* puis les *sommes de Jacobi* associées à des caractères sur $\mathbb{F}_p$. On verra des applications arithmétiques de ces sommes, notamment pour compter les solutions d'équations polynomiales sur $\mathbb{F}_p$.

Prérequis

Anneaux et corps du cours de M1 du premier semestre (structures quotients).

Bibliographie

Kenneth F. Ireland, Michael Rosen (1990), A classical introduction to modern number theory, Springer, second edition (chapitres 6, 8 et 9).

18 Lois Zêta pour l'arithmétique

Il s'agit de détailler les preuves, et de procéder à quelques généralisations faciles, de résultats de l'article en référence.

En utilisant la loi Zêta, l'auteur fournit plusieurs jolies démonstrations de résultats classiques. À titre d'exemple :

1. Pour $s > 1$, $\dfrac{1}{\zeta(s)} = \prod_{p\,\text{premier}} (1 - p^{-s})$ (un résultat dû à Euler).

2. On tire $k \geqslant 2$ entiers dans l'ensemble $\{1, 2, \ldots, n\}$ et on note $p_n(k)$ la probabilité que ces entiers soient premiers entre eux. Alors $p_n(2) \to 6/\pi^2$ lorsque $n \to +\infty$ (un résultat dû à Dirichlet). Plus généralement, $p_n(k) \to 1/\zeta(k)$ quand $n \to +\infty$.

3. Une généralisation du résultat de 2. : si X_n et Y_n sont deux variables aléatoires indépendantes de loi uniforme sur $\{1, 2, \ldots, n\}$, alors $\mathrm{pgcd}(X_n, Y_n)$ converge en loi vers la loi Zêta de paramètre 2.

4. Soient X_n et Y_n deux variables aléatoires indépendantes de loi uniforme sur l'ensemble des entiers de Gauss de partie imaginaire non nulle et de norme au plus n^2, et Z_n le plus grand diviseur commun de X_n et Y_n dans l'anneau des entiers de Gauss. En 1989, George E. Collins et Jeremy R. Johnson ont démontré que

$$\lim_{n\to+\infty} \mathbb{P}\,(Z_n = 1) = \frac{1}{\zeta(2)\,\beta(2)},$$

où, pour tout $s > 0$,

$$\beta(s) = \sum_{n=0}^{+\infty} \frac{(-1)^n}{(2n+1)^s}.$$

Bibliographie

Olivier Garet (2015). Les lois Zêta pour l'arithmétique. *Quadrature*, 96, 1-20. Preprint HAL `hal-01277715`.

19 Mélanges de cartes

Pour garantir l'équité, un joueur doit savoir bien mélanger un paquet de cartes en le battant, alors qu'un magicien doit savoir battre un paquet de cartes sans le mélanger. Après avoir modélisé mathématiquement l'opération "battage d'un paquet de cartes", le sujet du TER pourra évoluer au gré des envies de l'étudiant. Voici des exemples possibles.

- Les mélanges parfaits (combinatoire) : recherche d'invariants utiles pour faire un tour de magie par exemple.
- Les "bons" mélanges (probabilités) : qu'est-ce qu'un jeu bien mélangé ? combien de battages faut-il exécuter pour en obtenir un ?

Prérequis

Probabilités de L3.

Bibliographie

Aimé Lachal (2010), *Mélanges parfaits de cartes (I). In-shuffles et out-shuffles*, Quadrature 76, 13-25. Preprint HAL `hal-00864428`.

Aimé Lachal (2010), *Mélanges parfaits de cartes (II). Mélanges de Monge*, Quadrature 77, 23-29. Preprint HAL `hal-00864433`.

Djalil Chafaï, Florent Malrieu (2018), *Recueil de Modèles Aléatoires*. Preprint HAL `hal-01897577v3`.

20 Méthode de Coppersmith et applications cryptographiques

Étant donné un polynôme $P \in \mathbb{Z}[X]$, il est facile de trouver ses racines modulo un nombre premier p, c'est-à-dire les entiers x pour lesquels $P(x) \equiv 0\ [p]$. Mais si N est un nombre composé, trouver les racines de P modulo N revient en général à factoriser N, ce qui est un problème difficile lorsque N est grand.

En 1996, Don Coppersmith a donné un algorithme permettant de déterminer les « petites » racines de P modulo N, c'est-à-dire les entiers $x \in \mathbb{Z}$ vérifiant $P(x) \equiv 0\ [N]$ et $|x| < N^{1/\deg(P)}$. Cet algorithme permet d'attaquer certains usages du protocole de chiffrement RSA ; il a aussi rendu possible une attaque sur des centaines de clés RSA.

Un outil fondamental de la méthode de Coppersmith est la réduction de réseaux euclidiens. Cette réduction consiste essentiellement à trouver, dans un sous-groupe additif Γ de $\mathbb{Z}^n$ donné par une famille de générateurs, des petits vecteurs non nuls (pour une norme usuelle). Trouver le plus court vecteur non nul de Γ est un problème difficile quand n est grand, mais pour la méthode de Coppersmith on a seulement besoin de trouver un vecteur « suffisamment court », ce qui peut se faire avec l'algorithme LLL de réduction de réseaux.

Bibliographie

Don Coppersmith (1996), *Finding a small root of a univariate modular equation*, in *Advances in Cryptography – EUROCRYPT'96*, vol. 1070 of Lecture Notes in Comput. Sci., Springer, 155–165.

Daniel J. Bernstein et al. (2013), *Factoring RSA keys from certified smart cards : Coppersmith in the wild*, in *Advances in Cryptography – ASIACRYPT 2013*, vol. 8270 of Lecture Notes in Comput. Sci., Springer, 341–360. Cryptology ePrint disponible à l'adresse `ia.cr/2013/599`.

Arjen K. Lenstra, Hendrik W. Lenstra, László Lovász (1982), *Factoring polynomials with rational coefficients*, Mathematische Annalen, vol. 261 (4), 515–534. Disponible sur le site de Hendrik W. Lenstra : `www.math.leidenuniv.nl/~hwl`.

21 Métrique de Schwarzschild

La métrique de Schwarzschild décrit des trous noirs à symétrie sphérique. C'est une solution exacte des équations d'Einstein dans le vide. Un bon nombre de prédictions de la relativité générale est basé sur une étude détaillée de cette métrique. Pendant ce TER, l'étudiant(e) devra d'abord apprendre les bases de la géométrie lorentzienne. On examinera ensuite plus en détail la métrique de Schwarzschild. On comprendra en particulier la notion de trou noir et l'existence d'une sphère de photons qui est une sphère sur laquelle des photons peuvent tourner sans aller à l'infini.

Prérequis

Le cours de M1 de géométrie différentielle.

Bibliographie

Robert M. Wald (1984), General Relativity, University of Chicago Press.

Barrett O'Neill (1983), Semi-Riemannian Geometry, With applications to relativity. Pure and Applied Mathematics, volume 103, Academic Press.

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). Disponible à l'adresse :
`www.ams.org/journals/tran/1973-180-00/S0002-9947-1973-0321133-2/`

23 Parallélisabilité des sphères

L'espace vectoriel $\mathbb{R}^n$ admet une structure d'algèbre à division seulement pour $n = 1, 2, 4, 8$ (réels, complexes, quaternions, octonions). Ce fait algébrique est lié à des propriétés du fibré tangent de la sphère, qui est trivial seulement pour les sphères de dimension 0, 1, 3, ou 7. On est ainsi ramené à un problème purement topologique, résolu à la fin des années 50 par John Willard Milnor et Raoul Bott, et par John Frank Adams. La démonstration repose sur plusieurs aspects de la théorie des fibrés vectoriels : K-théorie topologique et classes caractéristiques.

Ce TER sera l'occasion de se familiariser avec les notions de variétés, fibrés vectoriels, cohomologie, etc., et ne nécessite pas de prérequis particulier outre ceux mentionnés ci-dessous.

Prérequis

Algèbre et Topologie de L3A.

Bibliographie

Allen Hatcher, Vector bundles and K-theory, notes de cours non publiées, disponibles à l'adresse : `pi.math.cornell.edu/~hatcher/VBKT/VBpage.html`.

Raoul Bott, John Milnor (1958), On the parallelizability of the spheres, Bull. Amer. Math. Soc. 64, 87-89.

John Frank Adams (1958), On the nonexistence of elements of Hopf invariant one, Bull. Amer. Math. Soc.64, 279-282.

24 Pavages par dominos et modèle des dimères

Le modèle des dimères est un modèle de mécanique statistique de nature combinatoire, relié à la fois à de « vrais » modèles physiques (par exemple le modèle d'Ising, qui explique la stabilité du champ magnétique créé par un aimant si la température n'est pas trop élevée) et à des questions purement mathématiques.

Le modèle est défini de la manière suivante : étant donné un graphe $G = (V, E)$ (où V est l'ensemble des sommets de G et E l'ensemble de ses arêtes), une *configuration de dimères* sur G est une collection $\mathcal{E}$ d'arêtes telle que chaque $v \in V$ est l'extrémité d'exactement une arête dans $\mathcal{E}$. Dans le cas où G est une partie du réseau carré en dimension 2, on peut voir une telle configuration comme une collection de « dominos » (des rectangles de taille 1×2 ou 2×1) disjoints qui recouvrent G. On cherche alors à étudier les propriétés d'une telle configuration choisie aléatoirement uniformément parmi toutes les configurations de dimères sur G.

Le TER consistera à étudier quelques unes des questions naturelles liées au modèle :

- Combien y a-t-il de configurations de dimères ? Dans le cas général, il n'y a pas de formule exacte, mais par exemple si G est planaire, ce nombre peut être écrit comme un déterminant grâce au « *matrix-tree theorem* ».
- De manière reliée, si G est un rectangle de taille $k \times n$ avec k petit, on peut obtenir une relation de récurrence par la méthode des *matrices de transfert* qui a de nombreuses applications en physique statistique.
- À quoi ressemble un pavage par dominos « typique » dans une grande région du plan ? La réponse est spectaculaire et fait apparaître deux régions, l'une où la configuration est « vraiment aléatoire » et l'autre où elle est déterministe, ces régions étant séparées par un « cercle arctique ». *Cette direction est plus ambitieuse, mais des résultats partiels sont tout à fait accessibles dans le cadre d'un TER, et le modèle est amusant à simuler.*

Prérequis

Notions de base de probabilités, éventuellement un peu de combinatoire énumérative mais cela peut constituer une partie du travail de TER.

Bibliographie

Richard Kenyon (2003), *An introduction to the dimer model.* Preprint `arXiv:math/0310326[math.CO]`.

25 Période trois implique chaos et théorème de Sharkovsky

Dans ce TER, nous considérons des systèmes dynamiques d'apparence très simple : des récurrences de la forme

$$x_{n+1} = f(x_n)$$

où f est une application continue d'un intervalle fermé de la droite réelle dans lui-même, et nous nous poserons la question toute aussi simple : quelles sont les périodes possibles des cycles de ce système dynamique ?

Un résultat très étonnant de Tien-Yien Li et James A. Yorke affirme que si un tel système possède un point périodique d'ordre trois, alors il possède des points périodiques de tout ordre. Nous débuterons le TER avec la démonstration de ce résultat. Nous nous attaquerons ensuite à la démonstration (partielle) d'une généralisation de ce résultat : il existe un ordre total, dit ordre de Sharkovsky, sur l'ensemble des entiers positifs, tel que si un système de cette forme possède un point périodique d'ordre m, alors il possède un point périodique d'ordre n pour tout n plus grand que m.

Bibliographie

Tien-Yien Li, James A. Yorke (1975), Period three implies chaos, The American Mathematical Monthly, volume 82, 85-92.

Veniamin L. Smirnov, Juan J. Tolosa (2017), The Sharkovsky Theorem. Preprint `arXiv:1702.07964[math.DS]`.

26 Problème de Schoenflies

Un cercle dans la sphère de dimension 2, aussi tordu et peu régulier soit-il, sépare toujours la sphère en deux composantes connexes homéomorphes à des disques. La généralisation en dimension 3 est fausse : James Waddell Alexander découvre en 1924 une sphère de dimension 2 qui sépare la sphère de dimension 3 en une boule et une région C non homéomorphe à la boule. Autre fait surprenant découvert par R. H. Bing en 1952 : si on considère deux copies de C recollées sur leur bord commun, on obtient à nouveau la sphère de dimension 3. L'adhérence de la région C est un objet assez singulier. Si on suppose en revanche que c'est une variété, Barry Mazur et Morton Brown ont tous deux démontré en 1959 que C doit être une boule.

Le TER tournera autour de ces objets topologiques amusants. Ce sera l'occasion d'apprendre un peu de topologie des variétés avec des constructions concrètes. Pas de prérequis particulier outre ceux mentionnés ci-dessous, mais un goût pour la topologie.

Prérequis

Topologie de L3A et Géométrie différentielle et dynamique de M1.

Bibliographie

Andy Putman, The generalized Schoenflies theorem, notes de cours non publiées, disponibles à l'adresse : `www3.nd.edu/~andyp/notes/Schoenflies.pdf`.

James Waddell Alexander (1924), An Example of a Simply Connected Surface Bounding a Region which is not Simply Connected, PNAS, vol. 10, n°1, 8-10.

R. H. Bing (1952), A homeomorphism between the 3-sphere and the sum of two solid horned spheres, Ann. of Math. (2) 56, 354-362.

Morton Brown (1960), A proof of the generalized Schoenflies theorem, Bull. Amer. Math. Soc. 66, 74-76.

Barry Mazur (1959), On embeddings of spheres, Bull. Amer. Math. Soc. 65, 59-65.

27 Théorie de Floquet

Soit $q : \mathbb{R} \to \mathbb{R}$ une fonction continue et périodique de période $T > 0$. L'équation de Hill associée à q est l'équation différentielle

$$y'' + q(t)\,y = 0$$

Par exemple, l'orbite de la Lune autour de la Terre est décrite par une équation de Hill.

Soient y_1 et y_2 les solutions élémentaires de l'équation de Hill, définies par les conditions initiales $y_1(0) = 1$, $y_1'(0) = 0$, et $y_2(0) = 0$, $y_2'(0) = 1$. Soient u_1 et u_2 les deux racines (possiblement égales) du polynôme du second degré $u^2 - (y_1(T) + y_2'(T))\,u + 1$.

Le théorème de Floquet pour l'équation de Hill donne les résultats suivants :

1 Si $u_1 \neq u_2$, il existe deux solutions indépendantes z_1 et z_2 de l'équation de Hill telles que, pour tout $t \in \mathbb{R}$,

$$z_1(t+T) = u_1 y_1(t), \quad \text{et} \quad z_2(t+T) = u_2 y_2(t).$$

2 Si $u_1 = u_2$ alors $u_1 = u_2 = \pm 1$ et il existe deux solutions indépendantes z_1 et z_2 de l'équation de Hill telles que z_1 est T-périodique si $u_1 = u_2 = 1$, et $2T$-périodique si $u_1 = u_2 = -1$.

Théorème de Floquet (1883). *Soient* $A \in C(\mathbb{R}, M_n(\mathbb{C}))$ *périodique de période* $T > 0$, *et* $\Phi(t)$ *une matrice fondamentale du système* $y' = A(t)\, y$. *Il existe* $P \in \mathbb{C}(\mathbb{R}, GL_n(\mathbb{C}))$ T*-périodique et* $B \in M_n(\mathbb{C})$ *constante, telles que*

$$\Phi(t) = P(t)\, e^{t\,B} \quad \textit{(forme normale de Floquet)}.$$

De plus, si on note λ_k *les valeurs propres de* B *et* m_k *leur multiplicité, pour* $1 \leqslant k \leqslant p$, *où* p *est le nombre de valeurs propres distinctes de* B, *alors les solutions du système* $y' = A(t)\, y$ *sont de la forme*

$$y(t) = \sum_{k=1}^{p} \sum_{\ell=0}^{m_k-1} c_{k,\ell}\, e^{\lambda_k\, t}\, t^l\, \nu_{k,\ell}(t),$$

où les $\nu_{k,\ell}$ *sont des fonctions* T*-périodiques et les* $c_{k,\ell}$ *sont des constantes complexes.*

Le théorème de Floquet caractérise le cas d'existence de solutions périodiques et il permet d'en étudier la stabilité.

On s'intéressera aussi au théorème de Massera et au théorème de Reissig sur les solutions périodiques.

Bibliographie

Florent Berthelin (2017). *Équations différentielles*, Cassini.

Stéphane Gonnord, Nicolas Tosel (1998). *Thèmes d'analyse pour l'Agrégation : Calcul différentiel*, Ellipses.

Hervé Reinhard (1992). *Équations différentielles : Fondements et applications*, Dunod.

28 Théorie du complot

L'homme a-t-il réellement marché sur la lune ? Le changement climatique est-il une invention destinée à faire peur ? Existe-t-il une conspiration pour nous imposer des vaccins inutiles ? Existe-t-il un remède caché contre le cancer ? Voici quatre exemples classiques cités pour présenter la théorie du complot. Mais, comme disait Jerry Fletcher, « Un bon complot est un complot qu'on ne peut pas prouver », et il y a plusieurs possibilités pour qu'un complot soit découvert, comme le nombre de conspirateurs impliqués, la quantité de temps qui a passé et la probabilité d'un défaut intrinsèque du complot.

Le but de ce TER est d'étudier l'article donné en référence, qui prend en compte ces trois facteurs afin de modéliser la probabilité qu'un complot soit découvert dans le temps. L'étudiant·e devra reprendre les calculs de l'article et étudier les critiques apportées par certain·e·s de ses lecteur·trice·s.

Bibliographie

David Robert Grimes (2016). On the viability of conspiratorial beliefs. *PLOS One*, e0147905. Disponible à l'adresse :
`journals.plos.org/plosone/article?id=10.1371/journal.pone.0147905`

29 Voyage sur les groupes de Lie

L'objet de ce TER est la lecture de l'article en référence. L'idée générale est de comprendre, étant donnée une famille de champs de vecteurs que l'on peut emprunter (comme on emprunte une route), où on peut aller dans l'espace que l'on considère. Ici les espaces ambiants ont beaucoup de structure puisqu'il s'agit de groupes de Lie et les champs de vecteurs sont des champs de vecteurs invariants à droite ou à gauche.

Il s'agira de découvrir les objets introduits (groupes de Lie, notions de contrôlabilité), de comprendre les résultats et les preuves, et d'en faire une restitution simplifiée (donc moins détaillée) que ce soit à l'écrit comme à l'oral.

Bibliographie

Velimir Jurdjevic, Ivan Kupka (1981), Control systems on semi-simple Lie groups and their homogeneous spaces, Annales de l'Institut Fourier, 31 no. 4, 151-179. Disponible à l'adresse : `www.numdam.org/article/AIF_1981__31_4_151_0`