INSTITUT FOURIER

Sujets de TER 2023-2024
M1 Mathématiques générales

Novembre 2023

UGA UFR IM²AG Université Grenoble Alpes

Mode d'emploi

Vous enverrez, au plus tard le **lundi 11 décembre à 23h59**, un email à **Erwan Lanneau** indiquant les numéros des **quatre sujets** sur lesquels vous souhaitez travailler, écrits dans l'ordre décroissant de préférence (ou bien un message indiquant une absence de préférence). Pour les cas où une poursuite d'études est envisagée (par exemple en M2R 2024-2025 à l'IF, en M2 Cybersecurity ou en M2 ORCO) et qu'un sujet en lien avec cette poursuite d'études est choisi, veuillez alors le rappeler dans le message.

Nous essaierons de contenter tout le monde, et de faire au mieux en tenant compte des contraintes de l'équipe pédagogique.

Titres des sujets de TER

1 Ajout d'activités Moodle et VPL (caseine) dans des séquences de formation Fidle

L'objectif de ce stage est de transformer une ou plusieurs séquences de la formation Fidle (fidle.cnrs.fr) pour permettre une auto-évaluation des apprentissages. L'objectif de la formation Fidle est de proposer une introduction au Deep Learning, allant des concepts fondamentaux aux architectures avancées.

Un ensemble de séquences pour public ou objectif spécifique de Fidle sera sélectionné et le stagiaire devra construire des Quiz Moodle, de l'évaluation de notebook Jupyter ou des ateliers de programmation VPL pour permettre aux apprenants de manipuler les concepts enseignés et vérifier leur compréhension.

La formation Fidle et la plateforme caseine sont gratuites et ouvertes à toutes et à tous ! Par conséquent, les outils construits par le stagiaire seront proposés sur la plateforme caseine dans un cours ouvert à tous et gratuit également.

Ce stage se situe dans le cadre du projet EFELIA. Il sera encadré par des membres des équipes caseine et Fidle. L'équipe sélectionnera avec le stagiaire un ensemble de séquences (par exemple, Introduction à l'IA pour tous, comprendre l'IA et les outils pour les lycéens, initiation à l'IA pour des étudiants de licence scientifique...). Le stagiaire devra adapter les exercices existants pour intégrer de l'auto-évaluation. Il pourra ensuite éventuellement proposer un mécanisme pour créer des exercices similaires auto-évalués. Il pourra également proposer des exercices originaux d'entrainement (avec le soutien des concepteurs de Fidle et de l'équipe caseine).

Prérequis

1. Une curiosité pour l'IA (dans ce qu'elle a d'intéressant ou de critiquable) est nécessaire.
2. Python.
3. Ce projet s'adresse à des étudiants qui ont choisi l'option Operations Research qui vous donnera aussi des éléments de réflexion et un usage de caseine coté étudiant intéressants pour ce stage.

2 Arbres de marche

On considère une marche au hasard sur un arbre que la marche elle-même construit progressivement comme suit : à chaque étape, on ajoute un nombre aléatoire de nouvelles arêtes au sommet occupé par la marche, puis on effectue un pas de la marche sur l'arbre augmenté, puis on recommence à partir du nouveau sommet occupé, etc.

Les caractéristiques de ces marches et l'allure globale des arbres obtenus sont très différentes selon les détails du modèle, par exemple selon qu'on ajoute une arête au temps n avec une probabilité constante ou avec une probabilité qui décroît comme une puissance de n.

On s'intéressera à la récurrence/transience de la marche, à son caractère balistique ou non en cas de transience, et à la distribution empirique des degrés des sommets des arbres obtenus. Des simulations informatiques pourront venir enrichir le travail proposé.

Prérequis
Cours de M1 de Probabilités du premier semestre.

Bibliographie

1. János Engländer, Giulio Iacobelli, Rodrigo Ribeiro (2021). Tree builder random walk beyond uniform ellipticity, preprint.
2. Daniel R. Figueiredo, Giulio Iacobelli, Roberto Imbuzeiro Oliveira, Bruce A. Reed, Rodrigo Ribeiro (2021). On a random walk that grows its own tree, Electronic Journal of Probability 26, pp. 1-40.
3. Giulio Iacobelli, Daniel Figueiredo, Giovanni Neglia (2019). Transient and slim versus recurrent and fat : random walks and the trees they grow, Journal of Applied Probability 56 (3), pp. 769-786.
4. Giulio Iacobelli, Rodrigo Ribeiro, Glauco Valle, Leonel Zuaznábar (2022). Tree builder random walk : recurrence, transience and ballisticity, Bernoulli 28 (1), pp. 150-180.

3 Arbres télégraphistes

Un bit +1 ou –1 est choisi uniformément et déposé à la racine d'un arbre. Puis on propage ce bit de proche en proche le long de l'arbre comme suit : chaque sommet reçoit le bit placé en son ancêtre direct avec probabilité p et le bit opposé avec probabilité 1 – p. Pour un arbre infini donné, la question est de savoir s'il est possible de reconstruire le bit déposé à la racine à partir de la collection de bits des sommets de la génération n, avec probabilité de succès strictement supérieure à 50

Pour l'arbre régulier de degré b+1, Bleher, Ruiz et Zagrebnov ont démontré que la reconstruction était possible si $(1 - 2p)^2 > 1/b$ et impossible si $(1 - 2p)^2 < 1/b$, puis Evans, Kenyon, Peres et Schulman ont généralisé ce résultat à d'autres arbres, éventuellement aléatoires.

Il s'agit d'étudier les preuves de ces résultats, basées sur des techniques de conductances électriques, de flots maximaux, de percolation sur des arbres et sur certains arguments de couplage. On pourra également relier ces approches au problème de la pureté de l'état de Gibbs pour le modèle d'Ising à bord libre sur l'arbre considéré.

Prérequis
Cours de M1 de Probabilités du premier semestre.

Bibliographie

1. William Evans, Claire Kenyon, Yuval Peres, Leonard J. Schulman (2000). Broadcasting on trees and the Ising model, Annals of Applied Probabability 10, pp. 410-433.
2. Russell Lyons, Yuval Peres (2016). Probability on Trees and Networks, Cambridge.

4 Ateliers de Bernoulli

Un atelier de Bernoulli est une procédure de simulation d'une variable de Bernoulli de probabilité de succès f(p) à partir de variables de Bernoulli indépendantes de probabilité de succès p, avec p dans [0, 1/2]. Keane et O'Brien ont fourni une condition nécessaire et suffisante portant sur la fonction f pour l'existence d'un atelier de Bernoulli (par exemple, il n'en existe pas pour f(p) = 2p).

Il s'agit d'étudier la preuve de Keane et O'Brien et leur algorithme de construction d'un atelier de Bernoulli. On pourra ensuite s'intéresser à une modification de leur approche, proposée ultérieurement et permettant d'obtenir l'algorithme de coût optimal à un multiple près, quand il existe, ou à l'extension du problème au cas de sources biaisées markoviennes.

Prérequis
Cours de L3 de Probabilités.

Bibliographie

1. Mike S. Keane, George L. O'Brien (1994). A Bernoulli Factory, ACM Transactions in Modeling and Computer Simulation 4, pp. 213-219.
2. John von Neumann (1951). Various techniques used in connection with random digits, A.S. Householder, G.E. Forsythe, H.H. Germond éditeurs, Monte Carlo Method, National Bureau of Standards Applied Mathematics Series 12, pp. 36-38.

5 Autour du problème de Kakeya

La formulation moderne de ce problème est la suivante : Si Ω est un sous-ensemble de $\mathbb{R}^n$ possédant une droite dans chaque direction, est-il de dimension (de Hausdorff) ègale à n (c'est à dire de dimension optimale) ? Il est possible de construire de tels ensembles (appelés ensembles de Besicovitch) qui sont de n-mesure de Lebesgue nulle (mais de dimension optimale n !). On les appelle parfois ensembles invisibles. La question est toujours (largement) ouverte pour $n > 2$.

Le but du TER consistera à :
- Construire des ensembles de Besicovitch dans le plan (Ce qui permet de répondre à la question intiale de Kakeya (1917) : on peut retourner une aiguille en balayant une surface d'aire aussi petite que l'on veut).
- Considérer le cas des corps finis (ce qui peut être vu comme un cas discret de la question précédente).
- Donner une solution à la question précédente quand $n = 2$.
Si le temps le permet, on verra des applications en analyse réelle et complexe, et en théorie des équations aux dérivées partielles (Travaux de Fefferman, Bourgain, Tao, ...).

Prérequis
Algèbre et théorie de la mesure de L3.

Bibliographie

1. Lecture on harmonic analysis, Tom Wolff, University Lecture series, American Mathematical Society (2000).
2. From Rotating Needles to stability of Waves : Emerging Connections between Combinatorics, Analysis, and PDE, Terence Tao, Notices of the American Mathematical Society, Volume 48, p 294-303 (2001).

6 Bornes pour les sous-groupes finis du groupe linéaire

Comme on le voit pour $n = 1$, les sous-groupes finis de $\mathrm{GL}_n(\mathbb{C})$ sont de taille arbitraire ; par contre la taille des sous-groupes finis de $\mathrm{GL}_n(\mathbb{Q})$ est bornée en fonction de n (par exemple si une matrice est d'ordre p premier, en considérant son polynôme minimal on trouve que $p - 1$ est au plus n) : on établira la borne multiplicative de Minkowski (1877) et son optimalité. À l'aide de la théorie des caractères, on montrera aussi le théorème de Schur (1905) qui en étend la validité aux sous-groupes finis de $\mathrm{GL}_n(\mathbb{C})$ de traces rationnelles.

Par ailleurs la structure des sous-groupes finis de $\mathrm{GL}_n(\mathbb{C})$ est contrainte par le théorème de Jordan (1878), qui énonce l'existence d'un réel $f(n)$ tel que tout sous-groupe fini contienne un sous-groupe distingué *abélien* d'indice au plus $f(n)$. En suivant la méthode de Frobenius on établira une telle borne explicite. On pourra s'intéresser au cas $n = 2$ ($f(2) = 60$).

Prérequis
Cours d'Algèbre de L3 et M1. Il sera utile de suivre l'UE Théorie de Galois.

Bibliographie

1. J-P. Serre, *Finite groups : an introduction* International Press, 2016 : chapitre 9
2. R.M. Guralnick, M. Lorenz, *Orders of finite groups of matrices*, Contemporary Mathematics n° 420, 141–162 (2006). https ://arxiv.org/abs/math/0511191
3. R. Antetomaso (2014), *Autour du théorème de Jordan sur les sous–groupes finis de* $\mathrm{GL}_n(\mathbb{C})$, RMS vol. 124, n°3
4. Sujet d'agrégation *Mathématiques Générales* 2003, partie II.

7 Couches limites en homogénéisation périodique

La théorie de l'homogénéisation permet d'approcher par la solution u_* d'une équation 'effective', les solutions u_ε d'équations aux dérivées partielles dont les coefficient sont fortement oscillants (par exemple avec une période de l'ordre d'un petit paramètre $\varepsilon > 0$). Alors que le calcul numérique de u_ε serait trop coûteux, celui de u_* est bien plus abordable, car les coefficients de l'équation effective sont plus réguliers : on a 'moyenné' les oscillations.

L'homogénéisation est une théorie très pertinente pour (entre autres) l'étude des matériaux composites : les coefficients des EDP qui les régissent traduisent en effet les propriétés physiques (mécaniques, optiques,...) du milieu. Cette théorie a été beaucoup développée à partir des années 80 dans le cadre de milieux parfaitement périodiques. De nombreuses questions restent largement ouvertes, notamment dès qu'on cherche à prendre en compte la présence d'imperfections dans les milieux.

On s'intéressera en particulier à l'interaction entre les microstructures d'un milieu composite et le bord du domaine qu'il occupe. On peut montrer que le contrôle de l'erreur entre u_ε et la solution effective u_* dépend fortement de la géométrie du bord et fait intervenir des problèmes de petits diviseurs. On considérera en particulier des milieux fibrés, pour lesquels des couches limites peuvent apparaître, qu'on cherchera à corriger pour améliorer l'approximation des u_ε.

Prérequis
Une bonne maîtrise du contenu du cours de théorie de la mesure et intégration de L3. On pourra éventuellement orienter le sujet vers des questions de calcul numérique des solutions des EDP étudiées.

Bibliographie

1. P. AMENOAGBADJI, S. FLISS, AND P. JOLY. *Wave propagation in one-dimensional quasiperiodic media*. arXiv 2301.01159 (2023).
2. A. BENSOUSSAN, J.-L. LIONS AND G. PAPANICOLAU, *Asymptotic analysis of periodic structures*, North Holland, (1978).
3. S. MOSKOW AND M. VOGELIUS. *First-order corrections to the homogenised eigenvalues of a periodic composite medium. A convergence proof.* Proceedings of the Royal Society of Edinburgh Section A : Mathematics 127.6. pp. 1263–1299 (1997).

8 De l'analyse discrète

L'inégalité de Poincaré–Wirtinger dit essentiellement que, si f est une fonction d'un domaine borné $D \subset \mathbb{R}^d$ vers $\mathbb{R}$ suffisamment régulière, alors

$$\int_D \left(f - \int_D f \right)^2 \leq \int_D |\nabla f|^2.$$

Cette inégalité est centrale dans divers domaines des maths, comme l'étude des équations aux dérivées partielles. Dans ce sujet, on propose d'étudier cette inégalité, et d'autres inégalités analogues, dans un cadre discret. Plus précisément, on va remplacer D par l'ensemble fini $\{0,1\}^d$ (qui est l'ensemble des sommets

de l'hypercube $[0,1]^d$).

Manipuler ce genre d'inégalité dans ce cadre plus élémentaire peut aider à forger une intuition dans le cadre continu. Selon les désirs de l'étudiant-e, plusieurs orientations du TER pourraient être envisagées : une direction probabiliste en étudiant des variables aléatoires dans $\{0,1\}^d$, une direction plus analytique en faisant de la théorie de Fourier dans $\{0,1\}^d$, une direction plus géométrique en liant ce genre d'inégalités à des problèmes dits isopérimétriques, ou enfin des directions plus appliquées, ce genre de théorie étant aussi liée à la théorie de complexité d'algorithmes en informatique théorique.

Prérequis
Cours de théorie de la mesure de L3.

Bibliographie

1. O'Donnel, Analysis of Boolean functions, Cambridge University Press,
2. Et d'autres références selon la direction choisie !

9 Géométrie aléatoire

En juin 2023, Agnès Désolneux a donné une conférence pour Math en ville 2023 organisée par l'Institut Fourier, intitulée "Quand le hasard se mêle à la géométrie ".

Le résumé est : *On peut faire remonter la rencontre du hasard et de la géométrie à un texte de Buffon daté de 1733, dans lequel il entend "mettre la géométrie en possession de ses droits sur la science du hasard". Pour ce faire, il considère, entre autres, un problème connu maintenant sous le nom de "l'aiguille de Buffon" : étant donnée une aiguille que l'on lance au hasard sur un parquet dont les lattes sont de largeur constante, quelle est la probabilité que l'aiguille tombe à cheval sur deux lattes du parquet ? Cette question, qui peut paraître anecdotique, est en fait très représentative des questions qui se posent dans le domaine des mathématiques appelé la géométrie aléatoire où il s'agit de faire des calculs de probabilités sur des objets de nature géométrique : des points, des droites, des segments (comme l'aiguille), des triangles, etc. La géométrie aléatoire est un champ très actif des mathématiques, avec de nombreuses questions ouvertes, et qui donne lieu à de nombreuses applications dans des domaines tels que les télécommunications, la science des matériaux poreux ou encore l'imagerie médicale et la synthèse d'images.*

Lien de la vidéo : https ://www.youtube.com/watch ?v=t4rsKfyoGDA

L'objet du TER est en première partie de démontrer les résultats de la première demi-heure de cette conférence. En particulier, on montrera la formule de Cauchy-Crofton qui permet de calculer la longueur d'une courbe à l'aide du nombre de points d'intersection de cette courbe avec des droites "jetées au hasard ".

Prérequis
Aucun.

Bibliographie

1. Pierre Calka. Some Classical Problems in Random Geometry. Stochastic geometry, 2237, , pp.1-43, 2019, Lecture Notes in Mathematics, 978-3-030-13546-1.
https ://hal.science/hal-02377523

10 Géométrie différentielle affine

Le but de la géométrie différentielle affine est un sujet qui vise à étudier des notions de géométrie, notamment la courbure, pour des courbes et des surfaces dans l'espace euclidien, mais de manière que, à différence de la géométrie différentielle classique, soit invariante par le groupe des transformations equiaffines (i.e. les transformations affines qui préservent le volume), et non seulement par le groupe d'isométries. Le but du stage est d'étudier cette théorie, d'abord pour les courbes dans le plan, et ensuite pour les (hyper)surfaces, et de comprendre quelques résultats de classification.

Prérequis
Calcul différentiel. Il sera utile de suivre Géométrie Différentielle en M1.

Bibliographie

1. Nomizu, K.; Sasaki, T. (1994), Affine Differential Geometry : Geometry of Affine Immersions, Cambridge University Press
2. Su, Buchin (1983), Affine Differential Geometry, Harwood Academic
3. An-Min Li , Udo Simon , Guosong Zhao and Zejun Hu (2015), Global Affine Differential Geometry of Hypersurfaces, De Gruyter Expositions in Mathematics

11 Géométrie spectrale

Considérons un domaine plan Ω borné et suffisamment régulier. Alors le Laplacien sur Ω peut être "diagonalisé" : il existe une suite de valeurs propres croissantes $\{\lambda_n\}_{n\in\mathbb{N}}$ du Laplacien (= le spectre du Laplacien), et si on note φ_n les fonctions propres associées ($\Delta\varphi_n = -\lambda_n\varphi_n$) alors $\{\varphi_n\}_{n\in\mathbb{N}}$ est une base Hilbertienne de $L^2(\Omega)$. Le but du TER sera d'abord de comprendre la preuve de ce résultat. Puis on étudiera certaines propriétés des valeurs propres et des fonctions propres. Par exemple, l'asymptotique de Weyl : le nombre de valeurs propres $\leq \lambda$ (comptées avec multiplicité) est $\sim \frac{\text{Aire}(\Omega)}{4\pi}$ quand $\lambda \to \infty$. Le sujet est très vaste et pourra être orienté éventuellement suivant les goûts de l'étudiant, une fois la base effectuée et sous réserve du temps nécessaire; on pourra par exemple considérer le cas de variétés, ou construire des domaines plans différents ayant même spectre, ou bien encore faire des simulations numériques pour calculer le spectre et les fonctions propres de domaines donnés.
C'est un sujet d'analyse, avec éventuellement un peu de géométrie et (si on veut) de programmation.

Prérequis
Cours d'Analyse du S1.

Bibliographie

1. "Topics in spectral geometry" par M. Levitin, D. Mangoubi, I. Polterovich, AMS. Disponible en téléchargement ici : https ://michaellevitin.net/Book/TSG230529.pdf

12 Graphes aléatoires et fonctions de seuil

Nous considérons un modèle de graphes aléatoires dans lequel un graphe G possède un nombre N de sommets et des arêtes apparaissent entre ces sommets avec une certaine probabilité p.

Le but de ce TER sera d'étudier le comportement de la probabilité

$$P(N, p, M(G))$$

ou M est une propriété du graphe G (par exemple - G est connexe, G possède un vertex isolé, G admet un cycle qui visite chaque sommet une fois). Plus précisement, nous fixerons une fonction probabilité $p(N)$ variant avec N et considérerons le comportement de $P(N, p(N), M(G))$ quand $N \to \infty$.

Depuis le travail fondateur de Erdös, nous savons que pour un grand nombre de propriétés $M(G)$, la limite

$$\lim_{N\to\infty} P(N, p(N), M(G))$$

passe assez rapidement de 0 à 1 quand la fonction $p(N)$ est proche d'une fonction $f_M(N)$ appelée *fonction seuil* de $M(G)$. Dans ce travail sera nous étudierons la notion de la fonction seuil et établirons sa valeur dans certains cas importants, notamment

— $M(G) = G$ est connexe,
— $M(G) = G$ contient un sous-graphe donné,
— $M(G) = G$ admet une compostante géante.

Plus généralement, nous étudierons pour différentes fonctions $p(N)$ le comportement probable de la taille des composantes connexes de G.

Le cas écheant, ce travail pourra s'ouvrir sur d'autres propriétés des graphes aléatoires, comme l'existence de certains cycles, la k-connectivité, ou les coloriages des graphes.

Prérequis
Cours de probabilité de L3 et L2.

Bibliographie

1. Bollabas, B. *Random Graphs*.
2. Erdős, P. Rényi, A (1959) *On Random Graphs I* in Publ. Math. Debrecen 6, p. 290–297

13 Graphes, laplacien et expanseurs

Considérons un graphe fini dont l'ensemble des sommets est noté S. On considère l'espace des fonctions de S dans $\mathbb{R}$, noté $\mathbb{R}^S$. On peut définir un opérateur appelé laplacien de l'espace $\mathbb{R}^S$ dans lui-même. Le but du projet est d'étudier cet opérateur, de voir qu'il est auto-adjoint (pour le produit scalaire naturel sur $\mathbb{R}^S$) et positif, puis d'étudier la relation entre les valeurs propres de cet opérateur et la géométrie du graphe. Pour un graphe connexe, on verra que la première valeur propre strictement positive du laplacien est reliée à un

invariant du graphe appelé *constante isopérimétrique*. On pourra aussi calculer tout le spectre du laplacien sur des exemples simples de graphes finis.

Dans un deuxième temps on pourra étudier la notion de *famille de graphes expanseurs*. Une suite de graphes finis $(\Gamma_n)_{n\geq 0}$ est une famille de graphes expanseurs si le nombre de sommets de Γ_n tend vers l'infini avec n, s'il existe un entier k tel que Γ_n est k-régulier pour tout n (c'est-à-dire que tout sommet de Γ_n a exactement k voisins) et s'il existe $\varepsilon > 0$ tel que la première valeur propre strictement positive du laplacien sur Γ_n est $\geq \varepsilon$ pour tout n. On pourra essayer d'étudier cette notion et de construire des familles de graphes expanseurs en utilisant des outils de la théorie des groupes infinis (graphes de Cayley, propriété T de Kazhdan, étude du groupe $\mathrm{SL}_3(\mathbb{Z})$).

Prérequis
Diagonalisation des endomorphismes auto-adjoints des espaces euclidiens, théorie des groupes (sous-groupe engendré par une partie, sous-groupes distingués, quotients), espaces de Hilbert.

Bibliographie

1. E. Kowalski, *An introduction to expander graphs*, Cours spécialisés **26**, Société Mathématique de France (2019), téléchargeable gratuitement sur le site de la SMF.
2. M. Burger, *Kazhdan constants for* $\mathrm{SL}_3(\mathbb{Z})$, J. Reine Angew. Math. **413** (1991).
3. G. Davidoff, P. Sarnak et A. Valette, *Elementary number theory, group theory, and Ramanujan graphs*, London Math. Soc. Stud. Texts **55**, Cambridge University Press, Cambridge, (2003).
4. B. Bekka, P. De La Harpe et A. Valette, *Kazhdan's property T*, New Math. Monogr. **11**, Cambridge University Press, Cambridge (2008). **Paragraphes 6.1 et 6.2 seulement ! Ne pas tout lire !**

14 Groupe fondamentale et SO(3)

ou pourquoi une rotation d'un angle de 2π n'est pas l'identité [1]

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 gentille" nous pouvons construire à l'aide du groupe fondamental un recouvrement universel $V \to T$ qui a le propriété de "deplier" totalement l'espace T.

Dans ce travail, nous étudierons la construction du groupe fondamental et du recouvrement universel. Nous les calculerons tous deux dans des cas importants (surfaces compactes, certains groupes géométriques) en s'attardant particulièrement sur le cas du groupe fondamentale de $SO(3)$. Nous verrons 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 écheant, on verra comment cet exemple, anecdotique de prime abord, est rélié à la physique des particules, ou c'est un élément central de notre compréhension de la notion de spin des particules sous-atomiques.

Prérequis

1. mais une rotation d'un angle de 4π l'est

Cours d'algèbre et topologie du L3.

Bibliographie

1. Massey, *Algebraic Topology*
2. Rotman, *An introduction to Algebraic Topology*
3. Berger, *Géométrie*.

15 Implémentation en C/C++ de la recherche de valeurs approchées des racines complexes d'un polynôme à coefficients réels ou complexes

Comme indiqué dans le titre, l'objectif principal du TER est de réaliser un programme écrit en C/C++ qui renvoie des racines complexes approchées d'un polynôme. On pourra commencer par trouver une racine complexe approchée par une méthode itérative de type Newton ou méthode de la puissance, avec une estimation sur la précision de la racine, puis l'éliminer et recommencer, et observer la précision du résultat. Dans un deuxième temps, on essaiera de trouver toutes les racines simultanément pour améliorer la précision, par exemple par la méthode d'Aberth ou Durand-Kerner-Weierstrass ou par une méthode de recherche numérique de valeurs propres (de type QR). On pourra aussi chercher à éliminer les racines multiples si les coefficients du polynôme sont exacts.

Prérequis
polynômes de $\mathbb{C}[X]$, être à l'aise avec un langage de programmation impératif (Python, Javascript, Pascal, Java, ...), mais pas forcément C/C++.

Bibliographie

1. https ://fr.wikipedia.org/wiki/M
2. https ://fr.wikipedia.org/wiki/M
3. https ://en.wikipedia.org/wiki/Aberth_method
4. https ://en.wikipedia.org/wiki/Durand
5. https ://en.wikipedia.org/wiki/QR_algorithm
6. Langage : https ://www-fourier.univ-grenoble-alpes.fr/˜ parisse/#info

16 Implémentation en C/C++ de la résolution exacte de systèmes linéaires à coefficients entiers

Comme indiqué dans le titre, l'objectif principal du TER est de réaliser un programme écrit en C/C++ qui résout dans $\mathbb{Q}$ un système linéaire à coefficients entiers. On pourra commencer par programmer l'algorithme de Gauss ou de Gauss-Bareiss et observer l'efficacité en fonction de la taille du système et des coefficients. On pourra ensuite s'intéresser à des méthodes modulaires ou p-adiques pour améliorer l'efficacité.

Prérequis

algèbre linéaire (pivot de Gauss), arithmétique entière (Euclide, Bézout, restes chinois), être à l'aise avec un langage de programmation impératif (Python, Javascript, Pascal, Java, ...), mais pas forcément C/C++.

Bibliographie

1. https ://fr.wikipedia.org/wiki/
2. https ://en.wikipedia.org/wiki/Bareiss_algorithm
3. https ://www-fourier.univ-grenoble-alpes.fr/~parisse/giac/doc/fr/algo.html#sec248
4. https ://gmplib.org/
5. Langage : https ://www-fourier.univ-grenoble-alpes.fr/~parisse/#info

17 Interpolation et hypothèse du continu

Le but initial de ce sujet est d'explorer des extensions du principe de prolongement analytique, autour de la question suivante. Soit $(f_i)_{i\in I}$ une famille de fonctions holomorphes (distinctes) telle que, pour tout $z \in \mathbb{C}$, l'ensemble $F(z) := \{f_i(z), i \in I\}$ soit au plus dénombrable. Peut-on en déduire que I est lui-même au plus dénombrable ?

Si on remplace "holomorphe" par "de classe $\mathcal{C}^\infty$", c'est faux, on peut construire explicitement des contre-exemples où pour tout z, $F(z)$ a au plus deux éléments.

Si on remplace "dénombrable" par "fini", c'est vrai presque sans hypothèse sur les fonctions.

Le résultat surprenant, prouvé par Paul Erdös en 1963, est que la réponse à la question dans le cas dénombrable dépend de l'hypothèse du continu, et est donc indépendante des axiomes de la théorie des ensembles ! Si le temps le permet, on pourra parler de logique et d'indécidabilité.

Prérequis

L'analyse de L3, et un peu du cours de fonctions holomorphes de M1 mais quasiment pas.

Bibliographie

1. Paul Erdös, An interpolation problem associated with the continuum hypothesis, Michigan Math. J. 11(1964), 9-10 (ce n'est pas une typo, l'article fait une page et demie)

18 Introduction à la théorie algébrique des nombres et applications au théorème de Fermat

Le point de départ est la démonstration de Kummer du grand théorème de Fermat dans le cas où n est un nombre premier $p > 2$ (vérifiant certaines conditions).

Si $x, y, z \in \mathbb{Z}$ et $\zeta_p = e^{2i\pi/p}$, l'égalité $x^p + y^p = z^p$ se récrit

$$(x + \zeta_p y) \cdots (x + \zeta^{p-1} y) = z^p$$

dans l'anneau $\mathbb{Z}[\zeta_p]$. En raisonnant sur les décompositions en irréductibles des deux membres, et après quelques efforts, on démontre qu'il n'existe pas de solutions vérifiant $xyz \neq 0$.

Malheureusement, l'anneau $\mathbb{Z}[\zeta_p]$ n'est pas factoriel en général (c'est vrai pour $p < 23$, et faux pour $p = 23$), et le raisonnement ne tient plus.

En revanche, il est vrai tout idéal non nul dans cet anneau s'écrit de manière unique comme produit de puissance d'idéaux premiers. On peut alors modifier le raisonnement pour aboutir à une démonstration du théorème de Fermat, lorsque p vérifie la condition suivante : pour tout idéal $\mathfrak{a}$ de $\mathbb{Z}[\zeta_p]$,

$$\mathfrak{a}^p \text{ est principal } \iff \mathfrak{a} \text{ est principal .}$$

Un tel nombre premier est dit régulier.

Ce qui se cache derrière tout ceci est la chose suivante : l'anneau $\mathbb{Z}[\zeta_p]$ est l'anneau des entiers algébriques du corps $\mathbb{Q}(\zeta_p)$, i.e. l'ensemble des éléments de $\mathbb{Q}(\zeta_p)$ qui sont racines d'un polynôme unitaire de $\mathbb{Z}[X]$..

Plus généralement, si $K/\mathbb{Q}$ est une extension de corps de degré fini, l'ensemble des éléments de K qui sont racines d'un polynôme unitaire de $\mathbb{Z}[X]$ est un anneau, noté $\mathcal{O}_K$, appelé anneau des entiers de K. Cet anneau est noethérien, intègre, intégralement et tout idéal premier non nul est maximal : c'est ce qu'on appelle un anneau de Dedekind.

Il se trouve que dans tout anneau de Dedekind, tout idéal non nul s'écrit de manière unique comme produit de puissance d'idéaux premiers.

On montre également que l'ensemble des idéaux non nuls d'un anneau de Dedekind A, muni de la relation d'équivalence

$$\mathfrak{a} \sim \mathfrak{b} \iff \text{ il existe } a, b \in A \setminus \{0\} \text{ tels que } a\mathfrak{a} = b\mathfrak{b},$$

et muni de la loi induite par le produit d'idéaux, est un groupe abélien $Cl(A)$, appelé groupe des classes de A, qui est trivial si, et seulement si, A est un anneau principal.

Lorsque $A = \mathcal{O}_K$, on montre que ce groupe abélien est fini. Demander qu'un nombre premier soit régulier revient exactement à dire que p ne divise pas l'ordre du groupe $Cl(\mathbb{Z}[\zeta_p])$.

Notons au passage que l'étude du groupe $Cl(\mathcal{O}_K)$ est un domaine de recherche très actif et vital en mathématiques, même dans le cas des extensions de de la forme $\mathbb{Q}(\sqrt{d})$, avec $d > 0$, où des conjectures importantes ne sont toujours pas démontrées.

Dans ce travail, de multiples objectifs sont proposés (à aborder en partie ou en totalité selon la rapidité de l'avancement du travail) :

- Étudier les anneaux de Dedekind : montrer tout idéal non nul s'écrit de manière unique comme produit de puissance d'idéaux premiers, montrer que $Cl(A)$ est un groupe, démontrer que tout anneau d'entiers est un anneau de Dedekind.

- Démontrer la finitude du groupe des classes de $\mathcal{O}_K$, et présenter quelques exemples simples de calcul de ce groupe.

- Comprendre la démonstration du théorème de Fermat dans le cas des nombres premiers réguliers.

- Aborder un peu de théorie de la ramification des nombres premiers dans une extension $K/\mathbb{Q}$: si p est premier, comment se factorise l'idéal $p\mathcal{O}_K$? en particulier, quels sont les nombres premiers p pour lesquels il apparaît un idéal premier de $\mathcal{O}_K$ à une puissance > 1.

Comprendre en particulier l'exemple de $\mathbb{Q}(\zeta_p)$.

- Démontrer que $\mathbb{Z}[\zeta_{23}]$ n'est pas principal.

- Appliquer la théorie de la ramification à la résolution d'autres équations diophantiennes plus simples.

- Comprendre comment calculer de manière algorithmique le groupe des classes

- ou encore d'autres choses (faire un panorama des résultats connus ou des conjectures ouvertes, y compris sur l'aspect analytique de la théorie, via les fonctions L, la formule du nombre de classes,etc., sans nécessairement se plonger dans les démonstrations)

Remarque. Ce sujet est difficile, long et exigeant. Il est réservé à un étudiant motivé et travailleur, ayant des bases solides en théorie des anneaux commutatifs.

Prérequis
Le cours d'Algèbre de L3 et le cours d'Algèbre de M1.

19 Introduction à la théorie des modules et applications

Motivations.

Soit A un anneau unitaire (non nécessairement commutatif). Un *A-module* est la structure mathématique obtenue lorsque l'on remplace le corps de base K par A dans la définition d'un K-espace vectoriel.

Autrement dit, un *A-module* est un ensemble M muni d'une loi interne $(x, y) \in M \times M \mapsto x + y$ et d'une loi externe $(a, x) \in A \times M \mapsto a \cdot x \in M$ appelée parfois *multiplication par un scalaire*, satisfaisant aux propriétés suivantes :

1. l'ensemble M, muni de la loi $+$, est un groupe abélien ;
2. pour tous $x, y \in M$, et tout $a \in A$, on a $a \cdot (x + y) = a \cdot x + a \cdot y$;
3. pour tout $x \in M$, on a $1_A \cdot x = x$;
4. pour tout $x \in M$, et tous $a, b \in A$, on a $(a + b) \cdot x = a \cdot x + b \cdot x$;
5. pour tous $a, b \in A$, et tout $x \in M$, on a $(ab) \cdot x = a \cdot (b \cdot x)$.

La théorie des modules sur un anneau a été développée par Noether, et a eu pour point de départ l'étude des représentations linéaires d'un groupe fini.

Afin d'expliquer le lien avec les modules, introduisons brièvement une notation. Si G est un groupe fini, noté multiplicativement, et si k est un corps, on note $k[G]$ l'ensemble des combinaisons linéaires formelles des éléments de G, c'est-à-dire

$$k[G] = \Big\{ \sum_{g \in G} \lambda_g g \mid \lambda_g \in k \Big\}$$

que l'on munit de l'addition et de l'unique loi produit distributive sur $k[G]$ qui étend la loi de groupe. On vérifie alors que $k[G]$ est un anneau, muni d'une structure de k-espace vectoriel pour laquelle la loi produit de l'anneau $k[G]$ est k-bilinéaire. C'est donc une k-algèbre associative unitaire. On montre alors facilement que se donner une action k-linéaire de G sur V revient à se donner une structure de $k[G]$-module sur V qui étend la loi externe du k-espace vectoriel V.

On obtient alors un dictionnaire entre la théorie des $k[G]$-modules et la théorie des représentations. L'étude systématique des $k[G]$-modules simples est particulièrement importante, puisque ceux-ci correspondent aux représentations irréductibles.

La théorie des modules permet aussi à Wedderburn de démontrer que toute k-algèbre associative unitaire de dimension finie sur k, de centre k, et n'ayant pas d'idéaux bilatères non triviaux, est isomorphe à une algèbre de matrices sur un anneau à division (i.e. un corps gauche).

Enfin, la théorie des modules sur un anneau principal permet d'obtenir à peu de frais la structure des groupes abéliens de type fini, ainsi qu'une classification complète des endomorphismes d'un espace vectoriel de dimension finie en termes de certains polynômes se calculant de manière algorithmique. Comme application de cette théorie, on peut également (entre autres) résoudre des systèmes d'équations linéaires à coefficients entiers, démontrer des résultats sur le commutant et le bicommutant d'un endomorphisme, et aussi retrouver la décomposition de Jordan aisément avec en prime une méthode de calcul systématique.

But du TER.

Dans un premier temps :

1) Comprendre les définitions de bases (module libre, de torsion, applications linéaires...), et pointer les différences fondamentales avec les espaces vectoriels. En particulier, on étudiera de plus près l'existence de bases, et on étudiera aussi si deux bases ont même cardinal (**Spoiler** : ce n'est pas toujours le cas !)

2) Démontrer le théorème de structure des modules de type fini sur un anneau principal (ou au moins au cas d'un anneau euclidien) et appliquer ce résultat aux groupes abéliens de type fini, et au problème de similitudes d'endomorphismes. On pourra même programmer soi-même un algorithme de calcul explicite.

Éventuellement, appliquer aussi la théorie au calcul du commutant et du bicommutant d'un endomorphisme, et à la résolution de systèmes linéaires à coefficients entiers.

Dans un second temps : s'intéresser à d'autres thématiques au choix

3) Démontrer le théorème de Wedderburn sur la structure de k-algèbres de centre k, et n'ayant pas d'idéaux bilatères non triviaux.

4) S'intéresser à la notion de module projectif, stablement libre, etc...et fournir des exemples et contre-exemples, ou d'autres applications.

5) S'intéresser à la théorie des entiers algébriques et à ses applications .

Remarque. Il est attendu que l'étudiant(e) comprenne les points 1) et 2), puis s'intéresse à au moins une autre thématique parmi 3) ,4) ou 5).

Prérequis

Aucun, même si une bonne connaissance de l'algèbre linéaire est la bienvenue.

20 Jeux à tours aléatoires

On s'intéresse à des jeux à deux joueurs où il y a un et un seul gagnant (pas d'ex-aequo) et dont le nombre de coups est borné.

En général les joueurs jouent alternativement, ici, nous considérerons des jeux du même type mais le joueur est désigné à chaque coup par le lancer d'un dé.

Déterminer des stratégies optimales quand on joue alternativement peut être très difficle. Etonnamment, la situation est différente dans les jeux à tours aléatoires.

Différents jeux peuvent être étudiés, le jeu de Hex, des jeux sur des graphes, etc.

On s'interessera aussi à la longueur d'un jeu ou plutôt à son espérance.

Prérequis

Aucun.

Bibliographie

1. Random-turn Hex and other selection games, Yuval Peres, Oded Schramm, Scott Sheffield, and David B. Wilson, Amer. Math. Monthly 114 (2007), no. 5, 373387.
   file :///C :/Users/Utilisateur/Downloads/math0508580.pdf
2. Game Theory, Alive ; Anna R.Karlin, Yuval Peres ; AMS
   https ://homes.cs.washington.edu/ karlin/GameTheoryBook.pdf

21 Le théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques

Euclide a donné dans ses Éléments la première démonstration connue de l'infinité des nombres premiers. Une façon standard de la présenter est la suivante : on suppose au contraire qu'il n'y en a qu'un nombre fini $p_1, \ldots, p_k$, il existe ensuite un nombre premier qui divise $p_1 p_2 \cdots p_k + 1$ et comme il est nécessairement distinct de $p_1, \ldots, p_k$ (sinon il diviserait aussi 1), on a une contradiction.

On peut maintenant se demander s'il existe une infinité de nombres premiers de la forme $4n + 1$ ou $4n + 3$ par exemple, où n est un entier naturel. Plus généralement, on veut savoir s'il y a une infinité de nombres premiers dans les *progressions arithmétiques* $(an + b)_{n\geq 0}$ où a et b sont des entiers ≥ 1 fixés, pas tous les deux égaux à 1 (sinon on connaît déjà le résultat). Une condition nécessaire pour qu'il y ait une infinité de nombres premiers dans une telle progression arithmétique est que a et b soient premiers entre eux. En effet, dans le cas contraire, le pgcd de a et b, qui est donc > 1, divise tous les nombres $an + b$ lorsque n parcourt $\mathbb{N}$. Il est naturel de se demander si, réciproquement, la condition que a et b soient premiers entre eux est suffisante pour que la progression arithmétique $(an + b)_{n\geq 0}$ prenne une infinité de fois une valeur qui soit un nombre premier.

Pour cela, on peut essayer d'adapter la méthode d'Euclide. On y parvient pour la progression arithmétique $(4n + 3)_{n\geq 0}$. En effet, supposons qu'il n'existe qu'un nombre fini de nombres premiers $p_1, \ldots, p_k$ congrus à 3 modulo 4 et considérons alors l'entier $m = 4p_1 p_2 \cdots p_k - 1$. Ni 2 ni aucun des p_j ne peut diviser m (sinon ils seraient aussi des diviseurs de 1). Donc les diviseurs premiers de m sont de la forme $4n+1$, de sorte que le reste de la division euclidienne de m par 4 vaut 1, ce qui est absurde puisqu'il vaut 3 par définition de m. On sait cependant que la méthode d'Euclide (convenablement formalisée) permet de prouver l'existence d'une infinité de nombres premiers congrus à $b \mod a$ si et seulement si $b^2 \equiv 1 \mod a$ (théorème de Murty-Schur). La méthode d'Euclide fonctionne donc aussi pour la progression arithmétique $(4n + 1)_{n\geq 0}$, ce que l'on vérifie en considérant le polynôme $4X^2 + 1$ à la place de $4X - 1$ ci-dessus, mais elle ne fonctionne pas pour $(5n + 3)_{n\geq 0}$ par exemple. Il faut donc trouver une autre méthode pour aborder les autres cas.

L'objectif du TER est de comprendre et présenter la démonstration que la coprimalité de a et b est bien une condition suffisante :

Théorème de Dirichlet (1837). *Fixons a et b deux entiers ≥ 1 et premiers entre eux. Alors la progression arithmétique $(an + b)_{n\geq 0}$ prend une infinité de fois une valeur première.*

Dirichlet a introduit des notions très novatrices pour l'époque et sa démonstration n'a pas été fondamentalement simplifiée depuis. (Il existe toutefois une démonstration complètement différente, qualifiée d'"élémentaire"

pour des raisons historiques, mais elle est en fait beaucoup plus compliquée.) La démonstration de Dirichlet est une très belle généralisation de la preuve d'Euler de l'infinité des nombres premiers, qui a donné naissance à la *Théorie analytique des nombres*. Euler avait en effet montré exactement un siècle plus tôt en 1737 que l'on a, pour tout réel $s > 1$,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ premier}} \frac{1}{1 - p^{-s}}, \tag{1}$$

qui est une reformulation analytique de l'existence et l'unicité de la factorisation des entiers en nombres premiers, puis il avait observé que le membre de gauche tend vers l'infini quand $s \to 1^+$, ce qui force le membre de droite à en faire de même et donc le produit ne peut pas porter sur un nombre fini de nombres premiers. À noter que la série à gauche est la célèbre fonction zêta de Riemann $\zeta(s)$.

Sommairement, Dirichlet a introduit des généralisations de la fonction zêta (que l'on appelle aujourd'hui séries L de Dirichlet) :

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

où χ est un caractère du groupe multiplicatif $(\mathbb{Z}/a\mathbb{Z})^*$ (a étant fixé a priori), c'est-à-dire un homomorphisme de groupes de $(\mathbb{Z}/a\mathbb{Z})^*$ vers le groupe multiplicatif $\mathbb{C}^*$. La série $L(s, \chi)$ permet donc de faire intervenir les suites $(an + b)_{n\geq 0}$ avec a et b premiers entre eux. Par ailleurs, Dirichlet a obtenu une identité analoque à l'équation (1), ce qui permet de considérer les nombres premiers qui sont des valeurs prises par les suites $(an + b)_{n\geq 0}$. La conclusion est obtenue en étudiant la limite de $L(s, \chi)$ quand $s \to 1$.

Prérequis
Analyse réelle (séries, intégrale de Lebesgue), Analyse complexe (propriétés usuelles des fonctions analytiques d'une variable complexe), Algèbre (théorie des caractères des groupes finis).

Bibliographie

1. T. Apostol, Introduction to analytic number theory, *Undergraduate Texts in Mathematics*, New York-Heidelberg : Springer-Verlag, 1976.
2. R. Descombes, Élements de théorie des nombres, *Presses Universitaires de France*, 1986.
3. P. G. L. Dirichlet, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, *Abhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin* **48** (1837), 45–71.

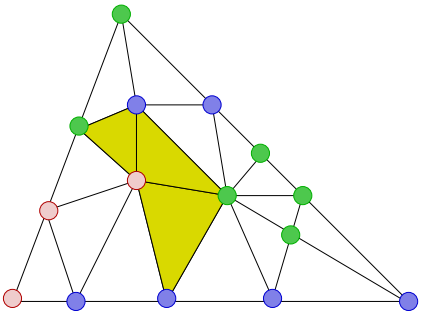
   Traduction en anglais dans `https://arxiv.org/abs/0808.1408`
4. J.-P. Serre, Cours d'arithmétique, 4ème édition, *Presses Universitaires de France*, 1994.

22 Lemme de Sperner et applications

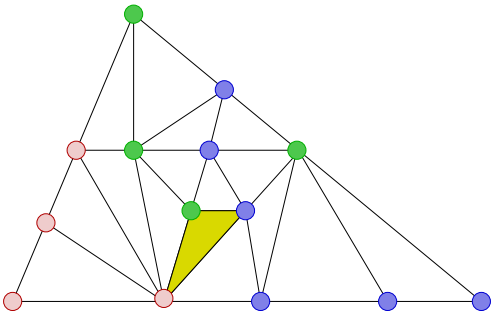
Le lemme de Sperner est un résultat combinatoire simple à énoncer. **Proposition (Lemme de Sperner)** On considère un triangle dont on colorie les trois sommets de trois couleurs différentes, disons 1, 2 et 3. On

triangule le grand triangle, c'est-à-dire qu'on le découpe en petits triangles de telle façon qu'une arête n'est commune qu'à au plus deux des petits triangles. Puis, on colorie chaque sommet de la triangulation avec comme seule règle qu'un sommet sur l'arête $i - j$ du grand triangle ne peut être colorié qu'avec la couleur i ou j.

Alors, il existe au moins un petit triangle dont les trois sommets sont de couleurs différentes.



un exemple avec trois triangles tricolores



un exemple avec un triangle tricolore

Il existe plusieurs preuves de ce résultat, certaines étant accessibles même à des collégiens. Une fois que l'on a compris le principe de la preuve, des variantes de ce résultat sont possibles, avec d'autres configurations et des conclusions plus ou moins fortes.

Sous ses apparences simples, il s'agit d'un résultat profond qui permet de montrer le théorème de point fixe de Brouwer (toute fonction continue de la boule de $\mathbb{R}^d$ dans elle-même admet un point fixe). Les idées derrière ce lemme permettent aussi de comprendre quel domaine peut-être coiffé, c'est-à-dire recouvert par un champ de vecteurs continu tangent aux bords, de démontrer que tout polynôme a autant de racines que son degré, de partager équitablement les gâteaux d'anniversaire ou de montrer qu'il y a forcément un gagnant au jeu du Y.

Ce stage permettra de s'initier à la topologie. Il s'appuiera en partie sur des articles écrits mais on pourra effectuer quelques recherches personnelles, à la recherche d'exemples ou d'applications qu'on trouve peu dans la littérature.

Prérequis
Aucun.

Bibliographie

1. A. Monier, *Deux démonstrations du théorème de Brouwer*, Le journal de maths des élèves de l'École Normale Supérieure de Lyon, Volume 4 (1998).
2. M. Aigner et G.M. Ziegler, *Proofs from THE BOOK*. Berlin : Springer, 1998.

23 Limite semi-classique pour l'équation de Schrödinger

On étudiera la propagation d'ondes haute fréquence, solutions de l'équation de Schrödinger

$$i\varepsilon\partial_t u + \frac{\varepsilon^2}{2}\Delta u = 0, \quad \text{sur } \mathbb{R}\times\mathbb{R}^d \,(\ni (t,x)).$$

Ici, ε est un petit paramètre (correspondant à la longueur d'onde). On prouvera que pour une donnée initiale sous la forme d'un "paquet d'ondes",

$$u(0,x) = a_0(x)\, e^{i\phi_0(x)/\varepsilon},$$

la solution est décrite assez simplement par l'optique géométrique :

$$u(t,x) \underset{\varepsilon\to 0}{\sim} a(t,x)\, e^{i\phi(t,x)/\varepsilon},$$

où la phase ϕ est solution d'une équation dite "eikonale", et l'amplitude a est solution d'une équation de transport (et suit les "rayons lumineux").
On commencera par le cas d'une phase plane ($\phi_0(x) = \xi_0 \cdot x$, pour un vecteur donné $\xi_0 \in \mathbb{R}^d$), et on pourra s'inspirer de la méthode présentée dans le livre de J. Rauch pour l'équation des ondes (section 1.4).
Pour passer au cas d'une phase initiale non plane (sans doute avec $d = 1$, pour simplifier), on se réfèrera au livre de R. Carles (chapitre 1). On pourra également aborder le cas d'une équation de Schrödinger non linéaire.

Prérequis
Cours d'analyse du premier semestre de M1.

Bibliographie

1. R. Carles, *Semi-classical analysis for nonlinear Schrödinger equations*.
2. J. Rauch, *Hyperbolic partial differential equations and geometric optics*.

24 Loi Zéta pour l'arithmétique

Il s'agit de détailler les preuves et faire quelques généralisations, faciles, de quelques résultats de l'article [Garet].
En utilisant la loi Zêta, O. Garet fournit plusieurs jolies démonstrations de résultats classiques. A titre d'exemple :

1. Pour $s > 1$,
$$\frac{1}{\zeta(s)} = \prod_{p \text{ premier}} (1 - p^{-s}) \quad \text{(résultat du à Euler)}$$
2. On tire $k \geq 2$ entiers dans l'ensemble $\{1, 2, \ldots, n\}$ et on note $p_n(k)$ la probabilité que ces entiers soient premiers entre eux. On peut prouver (résultat du à Dirichlet) que $p_n(2) \to 6/\pi^2$ lorsque $n \to +\infty$. Ce résultat peut être facilement généralisé à $p_n(k) \to 1/\zeta(k)$ quand $n \to +\infty$.
3. Une généralisation du résultat de 2. :
Si X_n et Y_n sont deux variables aléatoires suivant la loi uniforme sur $\{1, 2, \ldots, n\}$, alors le $PGCD(X_n, Y_n)$ converge en loi vers la loi $\zeta(2)$.

4. Soit $Z' = \{a + ib \text{ avec } (a, b) \in \mathbb{N} \times \mathbb{N}^*\}$ et soient X_n et Y_n deux variables aléatoires suivant la loi uniforme sur l'ensemble $\{z \in Z' \text{ tel que } N(z) = z\bar{z} \leq n^2\}$. Alors on a le résultat de convergence suivant, démontré par Collins et Johnson (1989),

$$\lim_{n\to+\infty} \mathbb{P}\left(PGCD(X_n, Y_n) = 1\right) = \frac{1}{\zeta(2)\,\beta(2)},$$

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

Prérequis
Aucun.

Bibliographie

1. O. Garet (2015). Les lois Zêta pour l'arithmétique. *Quadrature*, **96**, 1-20.

25 Marche aléatoire renforcée

La marche aléatoire simple sur le réseau $\mathbb{Z}^d$ est un des processus aléatoires les plus naturels : on part de $X_0 = 0$ et sachant $X_n = x$, X_{n+1} est un voisin de x choisi uniformément, indépendamment des choix précédents. On peut voir X_n comme une somme de pas aléatoires indépendants, et le théorème central limite nous dit que $\|X_n\|$ est d'ordre $\sqrt{n}$ et que $n^{-1/2}X_n$ converge en loi vers une variable gaussienne.

Une marche interagissante est une modification de la marche simple pour laquelle X_{n+1} est toujours un voisin aléatoire de X_n, mais dont la loi dépend de la trajectoire de la marche jusqu'au temps n. La marche est dite renforcée si elle est biaisée vers les sommets qu'elle a déjà visités. Il n'y a pas de théorie générale satisfaisante pour ce genre de processus, mais deux cas particuliers sont bien étudiés, le sujet du TER est de s'intéresser à l'un des deux :

- la marche renforcée linéairement, pour laquelle la probabilité d'utiliser une arête dépend linéairement du nombre de visites précédentes : dans ce cas, on peut réinterpréter le problème comme celui d'une marche aléatoire en milieu aléatoire, un cadre pour lequel des outils théoriques généraux peuvent s'appliquer ; - la marche renforcée une fois, pour laquelle la conductivité d'une arête augmente lors de sa première visite et ne change plus ensuite : dans ce cas la marche ne voit que sa trajectoire passée mais pas les nombres de visites. Ce cas semble plus simple, mais reste essentiellement mystérieux.

Prérequis
Les probabilités de L3 et du premier semestre du M1. L'UE de probabilités du second semestre peut être utile mais n'est pas indispensable.

Bibliographie

1. Daniel Kious, Bruno Schapira et Arvind Singh, Once reinforced random walk on $\mathbb{Z} \times \Gamma$, Ann. Inst. H. Poincaré Probab. Statist. 57(2021), 2219-2242
2. Vlada Limic et Pierre Tarrès, Attractive edge and strongly edge reinforced walks, Annals of Probability 35(2007), 1783-1806

26 Marche quantique sur un graphe

Une marche quantique définit un système dynamique en temps discret sur un graphe sous-jacent, dont la construction est inspirée par le formalisme de la mécanique quantique.

Du point de vue mathématique, une marche quantique est une application linéaire unitaire définie sur un espace de Hilbert naturellement associé à un graphe fini ou infini. Cet unitaire doit également satisfaire une condition de localité pour définir une marche quantique, et il décrit une étape de temps de la dynamique sur l'espace associé au graphe. Le formalisme quantique permet de plus d'associer à une marche quantique une suite de lois de probabilités discrètes sur le graphe, analogue à celle définie par l'évolution d'une marche aléatoire sur le graphe.

Il existe de nombreuses marches quantiques associées à divers types de graphes, très souvent réguliers. L'objectif de ce stage est d'explorer les propriétés de base d'une proposition de construction de marche quantique adaptée à un graphe quelconque, et celles des lois de probabilité associées.

Il s'agira en particulier d'établir les propriétés spectrales et dynamiques de ces marches quantiques associées à différents cas emblématiques de graphes finis, voire infinis.

Prérequis
Algèbre linéaire, séries de Fourier, probabilités discrètes.

Bibliographie

1. Spectral mapping theorem of an abstract quantum walk, E. Segawa, A. Suzuki, Quantum Information Processing, Vol. 18, Article number : 333 (2019)
2. Discrete Quantum Walks on Graphs and Digraphs, C. Godsil, H. Zhao, London Mathematical Society Lecture Notes Series 484, 2023.
3. Quantum Walks and Search Algorithms, R. Portugal, Quantum Science and Technologies, Springer, 2013

27 Marches aléatoires et réseaux électriques

Il existe un lien étonnant et très fructueux entre deux domaines apparemment totalement disjoints : l'étude des marches aléatoires sur un graphe et l'étude des réseaux électriques. Par exemple, on a le résultat suivant :
Considérons un graphe, c'est-à-dire un ensemble de sommets liés par des arêtes, et regardons une marche aléatoire sur ce graphe, ce qui veut dire qu'on regarde une marche qui vit sur les sommets du graphe et qui, à chaque étape, choisit uniformément (et indépendamment du passé) un sommet voisin et se déplace dessus. Considérons aussi la même structure de graphe mais voyons les arêtes comme des résistances (toutes égales) d'un réseau électrique. Alors, si u et v sont des sommets du graphes, l'inverse de la résistance équivalente entre u et v est égale (à un détail important près !) à la probabilité qu'une marche aléatoire issue de u touche v avant de revenir en u. Le but du TER est de comprendre cet énoncé ainsi que sa preuve et d'étudier d'autres liens entre marches aléatoires et réseaux électriques. On verra que ce lien est très utile dans l'étude de marches aléatoires sur divers graphes.

Prérequis

Cours de probabilité de M1 des 1er et 2nd semestres.

Bibliographie

1. Asaf Nachmias, Planar Maps, Random Walks and Circle Packing, Springer
2. Peter G. Doyle and J. Laurie Snell, random walks abd ekectric networks

28 Mathématiques de l'origami

L'origami est un art pluri-millénaire, mais son étude mathématique ne commence qu'au 20e siècle. Dans ce TER, on s'intéressera aux théorèmes qui régissent la création d'origami, dont l'axiomatisation a été effectué par Justin et Huzita en 1989. On étudiera aussi les problèmes de géométrie qui peuvent être résolus « par origami », c'est-à-dire en utilisant des pliages pour construire des droites. On montrera en particulier comment certains problèmes classiques de géométrie, comme la duplication du cube ou la trisection de l'angle, peuvent être résolu par origami alors qu'ils ne peuvent pas l'être par les constructions traditionnelles à la règle et au compas. Pour aller plus loin, on pourra étudier l'ensembles des nombres « constructibles par origami ».

Prérequis
Extension de corps, rudiments de théorie de Galois.

Bibliographie

1. J.-P. Delahaye, « Les mathématiques de l'origami », Pour la Science, no 448, février 2015, p. 76-81
2. chap. 10.3 (« Origami ») dans D. Cox, « Galois Theory », Wiley, 2004.

29 Modes propres du Laplacien et harmoniques

Les opérateurs de type Laplacien admettent une base Hilbertienne composée de « modes propres » dans le sens suivant. **Proposition** Soit $\Omega \subset \mathbb{R}^d$ un ouvert borné et soit Δ l'opérateur Laplacien sur Ω avec des conditions aux bords de Dirichlet. Alors il existe des nombres

$$0 < \lambda_1 < \lambda_2 \leq \lambda_3 \leq \dots \lambda_n \to +\infty$$

et une base Hilbertienne $(\varphi_n)_{n\geq 1}$ de $L^2(\Omega)$ telles que

$$\forall n \geq 1\ ,\ \ \Delta\varphi_n = -\lambda_n \varphi_n.$$

Le lien avec l'équation des ondes montre que les valeurs propres (λ_n) correspondent aux fréquences de résonnance de la forme Ω et donc aux fréquences produites par un instrument de musique de cette forme. On pourra regarder trois cas particuliers :

1. Ω est un rectangle ou un pavé avec diverses conditions aux bords (lame d'un vibraphone par exemple).
2. Ω est un disque (timbale, gong...).

3. $\Omega =]0,1[$ mais on ajoute à l'opérateur $\Delta = \partial_{xx}^2$ une condition de type saut à une interface située en $a \in]0,1[$ (dans le but de modéliser l'ouverture d'un trou le long du tube d'une flûte).

Le but du stage est de comprendre la proposition ci-dessus, son lien avec l'équation des ondes et de l'appliquer aux exemples. En particulier, on ne connaît pas d'expression simple des fréquences (λ_n) dans les cas 2 et 3. Il faudra donc explorer des moyens numériques pour calculer les premiers modes propres. On utilisera un logiciel pour trouver ces valeurs et simuler les sons des instruments de musique associés (langage de programmation au choix du ou de la stagiaire).

Ce stage permettra en particulier de s'initier à l'analyse des EDP et aux simulations numériques. Le stage ne s'appuiera pas sur des documents pré-écrits et donc le ou la stagiaire devra faire preuve d'une certaine autonomie.

Prérequis
C'est mieux de connaître de l'analyse et/ou un langage de programmation.

Références

[1] H. Brezis, *Analyse Fonctionnelle : Théorie et Applications*. Masson, Paris (1983).

30 Mouvements par courbure

Le mouvement par courbure est une manière de faire "évoluer" des courbes dans le plan, de manière que chaque point se déplace orthogonalement à la courbe et proportionnellement à sa courbure. On peut faire des expériences ici : https ://a.carapetis.com/csf/ Le but du stage est d'un côté de comprendre quelques résultats qui décrivent le comportement d'une courbe simple fermée lors qu'elle évolue par mouvement par courbure, par exemple le fait qu'elle devient d'abord convexe, et ensuite elle converge vers un point en devenant de plus en plus "ronde" ; de l'autre, d'étudier des applications, notamment une preuve de l'inégalité isopérimétrique.

Prérequis
Calcul différentiel. Il sera utile de suivre Géométrie Différentielle en M1.

Bibliographie

1. Chou, Zhu, The curve shortening problem, Chapman & Hall
2. Haslhofer, Lectures on curve shortening flow
3. Mantegazza, Novada, Pluga, Lectures on curvature flow of networks

31 Nombres premiers chanceux d'Euler et factorialité

En 1772 Euler remarquait 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.
Par ailleurs l'expérimentation montre qu'une proportion remarquable des $f(n)$ sont premiers. D'où leur dénomination "lucky Euler primes". Mais actuellement on ne sait pas prouver s'il y en a une infinité.

La stratégie d'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 quels entiers sont somme de deux carrés, et une première étape dans la preuve du grand théorème de Fermat est de passer dans l'anneau $\mathbb{Z}[\zeta]$ engendré par une racine p-ième de l'unité, où l'expression $z^p - y^p$ est produit de p facteurs ; malheureusement pour $p \geq 23$ cet anneau n'est pas factoriel..

Concernant ces nombres chanceux, ils sont 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 $1 \leq d \leq 200$ (seuls sept le sont), 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 0 dans un réseau.

Prérequis
cours d'Algèbre de L3 et M1.

Bibliographie

1. D. Perrin, *Anneaux d'entiers des corps quadratiques imaginaires*
   https ://www.imo.universite-paris-saclay.fr/ daniel.perrin/TER/anneauxd%27entiers.pdf
2. D. Perrin, *Pourquoi y a-t-il beaucoup de nombres premiers de la forme* $n^2 + n + 41$ *?*
   https ://www.imo.universite-paris-saclay.fr/ daniel.perrin/journeedu2311/redaction2311e.pdf
3. G. Chenevier, *Théorie géométrique des nombres, cours à l'X* 2011-2019
   http ://gaetan.chenevier.perso.math.cnrs.fr/TAN_chenevier.pdf
4. I. Stewart, D. Tall, *Algebraic number theory and Fermat's last theorem*, (AK Peters 2002), ch 7.

32 « Oil and Vinegar » : les évolutions d'un cryptosystème

Les protocoles de chiffrement à clé publique sont omniprésents aujourd'hui : https, CB, etc. On sait cependant depuis les travaux de Shor en 1994 que les systèmes actuellement employés (RSA, courbes elliptiques) sont vulnérables face à des ordinateurs quantiques. Contre cette menace, Patarin propose en 1997 le protocole de signature numérique « Oil and Vinegar », basé sur la difficulté de résoudre des systèmes polynomiaux multivariés. Ce schéma originel est cependant cassé dès 1998 par Kipnis et Shamir. En 1999, Kipnis, Goubin et Patarin proposent une variante appelée « Unbalanced Oil and Vinegar » (UOV), qui reste inattaquée actuellement, même par des ordinateurs quantiques, mais qui a le défaut d'avoir des clés publiques de taille importante. Pour pallier ce problème, Ding et Schmidt propose en 2005 le protocole « Rainbow » qu'on peut décrire comme une superposition de plusieurs schémas UOV. Mais ce cryptosystème modifié est à son tour cassé par Beullens en 2022, et c'est une nouvelle variante d'UOV à petite taille de clés, appelée « Mayo », qui reste en lice actuellement.

Le but de ce TER consiste dans un premier temps à comprendre le schéma de signature numérique (unbalanced) oil and vinegar basé sur des systèmes polynomiaux « à trappe », ainsi que l'attaque de Kipnis et Shamir sur la version équilibrée ; on essayera implémenter cette dernière. Dans un deuxième temps, on pourra s'intéresser au protocole Rainbow ainsi qu'à sa cryptanalyse.

Prérequis
Formes quadratiques, algèbre linéaire, réduction des endomorphismes.

Bibliographie

1. Cryptanalysis of the Oil and Vinegar signature scheme, A. Kipnis et A. Shamir, in Advances in Cryptology - CRYPTO '98, LNCS vol. 1462, Springer
2. Unbalanced Oil and Vinegar Signature Schemes, A. Kipnis, J. Patarin et L. Goubin, in Advances in Cryptology - CRYPTO '99, LNCS vol. 1592, Springer

33 Opérades et espaces des lacets

Étant donné un espace topologique X et un point $x \in X$, on peut considérer l'espace ΩX des lacets dans X basés en x, c'est- à-dire l'espace des applications continues $\gamma : [0,1] \to X$ tels que $\gamma(0) = \gamma(1) = x$. Deux lacets peuvent être concaténés pour en obtenir un nouveau, ce qui définit une multiplication sur ΩX. Cette multiplication n'est pas associative, mais elle l'est "à homotopie près". La notion d'opérade a été inventée pour appréhender ce genre de difficulté : l'espace ΩX est muni naturellement d'une action d'une opérade dite A_∞, ce qui encode le défaut d'associativité. Un théorème de P. May donne une réciproque : si un espace topologique connexe Y admet une action d'une operade A_∞ alors il existe un espace X tel que Y soit homotopiquement équivalent à ΩX. L'espace X peut être un peu compliqué : si Y est le cercle S^1, l'espace X est l'espace projectif complexe infini CP^∞.

Le TER mêlera algèbre et topologie autour de ces notions.

Prérequis
C'est mieux, mais pas obligatoire, d'avoir suivi le cours de magistère en L3 "Éléments de théorie des groupes et de topologie algébrique".

Bibliographie

1. P. May, "The geometry of iterated loop spaces", LNM 271, 1972.
2. A. Hatcher, "Algebraic Topology"
3. M. Markl, S. Shnider, J. Stasheff, "Operads in Algebra, Topology and Physics, AMS monograph, 2002.

34 Processus de Galton Watson

Les processus de Galton Watson aussi appelés processus de branchement sont des modèles de reproduction de population.

Historique (Wikipedia) :

À l'origine, ce modèle a été introduit par Bienaymé en 1845 et indépendamment par Galton en 1873 en vue d'étudier la disparition des patronymes.

Supposons que chaque adulte mâle transmette son patronyme à chacun de ses enfants. Supposons également que le nombre d'enfants de chaque homme soit une variable aléatoire entière (et que la distribution de probabilité soit la même pour tous les hommes dans une lignée). Alors, un patronyme dont les porteurs ont un nombre d'enfant inférieur à 1 en moyenne est amené à disparaître. Inversement, si le nombre moyen d'enfants est stritement supérieur à 1, alors la probabilité de survie de ce nom est non nulle et en cas de survie, le nombre de porteurs du patronyme connaît une croissance exponentielle.

Si la loi de reproduction μ a une espérance m et une fonction génératrice g, en notant q la probabilité d'extinction, on montrera les résultats suivants :

Théorème 1

1. Cas sous-critique
   Si $m < 1$, $q = 1$
2. Cas critique
   Si $m = 1$ et $\mu \neq \delta_1$, $q = 1$.
3. Cas sur-critique
   Si $m > 1$, $q < 1$ est le plus petit point fixe de g et le seul dans $[0, 1[$.

On note Z_n l'effectif de la n$^{\text{ème}}$ génération. Alors $\frac{Z_n}{m^n}$ est une martingale qui converge p.s. vers une variable aléatoire W.

On se demande alors si $P(W = 0) = q$. Ce n'est pas toujours le cas ainsi que l'énonce le théorème suivant :

Théorème 2, Kesten-Stigum (1966) On suppose $m > 1$. Les propriétés suivantes sont équivalentes :

1. $P(W = 0) = q$
2. $E[W] = 1$
3. $\sum_{k \geq 2} k \log k \mu(k) < +\infty$

On pourra étudier plusieurs preuves de ce résultat, probabilistes, analytiques.

L'une de ces preuves utilisera la notion de processus de branchement avec immigration.

On établira aussi des résultats plus fins sur les vitesses de convergence de $P(Z_n > 0)$ vers 0 dans les cas sous-critiques et critiques.

Prérequis

Le cours de probabilité du premier semestre.

Bibliographie

1. Lyons, R., Pemantle, R. and Peres, Y. (1995). Conceptual proofs of Llog L criteria for mean behavior of branching processes. Ann. Probab. 23, 1125–1138.
2. Lyons, R. and Peres, Y. Probability on Trees and Networks. https ://www.uni-due.de/ hm0110/book.pdf
3. Asmussen, S. and Hering, H. (1983). Branching Processes. Birkhäuser, Basel.

35 Processus des retenues

Pour additionner n nombres écrits en base 10, on les écrit en colonne, la colonne de droite étant celle des unités, la suivante celle des dizaines, etc $\cdots$, puis on ajoute les chiffres colonne par colonne, en commençant par les unités, les dizaines suivent, puis les centaines, et ainsi de suite. Quand le total des chiffres d'une colonne dépasse 9, une retenue se forme, qu'il faut reporter sur la colonne suivante. La même méthode s'applique pour additionner des nombres écrits en base b, où b est un entier ≤ 2. 1. Une grande partie du temps transfert des retenues dans ses On va s'interroger sur le nombre moyen de reports de retenues nécessaires, et sur la valeur moyenne de ces retenues. Il se trouve que ces questions soulèvent des problèmes mathématiques non triviaux, dont la résolution fait intervenir des outils probabilistes, combinatoires et analytiques intéressants.

On sera amené à parler d'un battage de cartes particulier, le battage-mitraillette et de processus déterminental.

On pourra aussi programmer en Python le processus des retenues et illustrer certains résultats avec des simulations

Prérequis
Le cours de probabilité du premier semestre.

Bibliographie

1. Carries, Shuffling, and an Amazing Matrix, Persi Diaconis and Jason Fulman, The American Mathematical Monthly, Vol. 116, No. 9 (Nov., 2009), pp. 788-803
   https ://statweb.stanford.edu/ cgates/PERSI/papers/carriesshufflingrev-09.pdf
2. Carries, Combinatorics, and an Amazing Matrix, John M. Holte, The American Mathematical Monthly, Vol. 104, No. 2 (Feb., 1997), pp. 138-149
   https ://sites.math.washington.edu/ billey/classes/561.fall.2019/past.articles/holte.pdf
3. On adding a list of numbers (and other one-dependent determinantal processes), May 2009 Bulletin of the American Mathematical Society 47(4)
   https ://www.ams.org/journals/bull/2010-47-04/S0273-0979-2010-01306-9/S0273-0979-2010-01306-9.pdf

36 Semigroupes dynamiques quantiques et production d'entropie

La dynamique irreversible de systèmes quantiques ouverts est donnée dans l'approximation markovienne par une équation différentielle linéaire sur le C-espace vectoriel des matrices carrées. Cette dynamique donne lieu à ce qu'on appelle un semigroupe dynamique quantique dont les propriétés structurelles dictées par la physique imposent au générateur d'avoir une forme particulière, dite de Linbdblad.

A l'irréversibilité de la dynamique quantique sont associées de façon naturelle des notions d'état asymptotique en temps, de bilan détaillé, d'entropie (relative), et de production d'entropie, analogues à celles du cas des chaines de Markov classiques.

L'objectif du stage consistera, dans un premier temps, à se familiariser avec le formalisme des semi-groupes dynamiques quantiques. Dans un second temps, il s'agira d'étudier les propriétés de la production d'entropie pour des générateurs de Lindblad associés à des systèmes quantiques ouverts hors équilibre et de les illustrer par des exemples concrets.

Prérequis
Algèbre linéaire, équations différentielles.

Bibliographie

1. Quantum Dynamical Systems, R. Alicki, M. Fannes, Oxford University Press 2001.

37 Sous-convexité explicite pour les fonctions L de Dirichlet

Objectifs

(a) Comprendre les définitions et propriétés des fonctions L de Dirichlet $L(\cdot, \chi)$, avec χ un caractère de Dirichlet (notamment le prolongement analytique et l'équation fonctionnelle), qu'on fixe de conducteur p pour la suite.

(b) Comprendre la notion (sans preuve pour l'instant) d'inégalité de *sous-convexité*, dans sa forme faible une inégalité de la forme

$$|L(1/2 + it, \chi)| \leq C(p)(1 + |t|)^{1/4-\varepsilon}, \qquad (t \in \mathbb{R})$$

avec $\varepsilon > 0$ et $C(p)$ polynomial en p , et son extension à la bande critique $0 < \Re(s) < 1$ par le principe de Phrägmen-Lindelof.

(c) Ensuite, travailler sur la base de l'article [Burgess] et de versions explicites issues de [Francis] pour retrouver des bornes explicites sur des sommes courtes de la forme

$$\left| S_{M,N}(\chi) := \sum_{n=M+1}^{M+N} \chi(n) \right| \leq c(r) N^{1-1/r} p^{\frac{r+1}{4r^2}} \log p$$

pour tout $r \in \mathbb{N}^*$, avec p le conducteur de χ, supposé premier et $c(r)$ explicite en r.

(d) Pour finir (si le temps le permet), déduire des inégalités de sous-convexité explicites, et/ou d'autres applications de ces résultats. Il s'agira d'insister surtout sur le caractère explicite et non pas l'optimalité des exposants rencontrés, contrairement aux articles (beaucoup plus sophistiqués) existants dans la littérature.

Prérequis
Un petit peu de familiarité avec les fonctions holomorphes est demandé, ainsi que si possible des notions de caractères de Dirichlet. Un certain intérêt pour la théorie analytique des nombres est recommandé (une bonne partie des preuves sont élémentaires mais techniques).

Bibliographie

1. D. A. Burgess, *On character sums and L-series. II*, Proc. Lond. Math. Soc. (3) 13, 524–536, 1963.
2. Forrest J. Francis, *An investigation into explicit versions of Burgess' bound*, Journal of Number Theory, vol.228, 2021.

38 Sous-décalages

Soit $\mathbb{A}$ un alphabet fini à au moins deux éléments. On munit $\mathbb{A}$ de la topologie discrète et $\mathbb{A}^{\mathbb{Z}}$ de la topologie produit, si bien que $\mathbb{A}^{\mathbb{Z}}$ est compact, métrisable.

Le décalage (en anglais, *shift*) sur $\mathbb{A}^{\mathbb{Z}}$ est la la transformation $\sigma : \mathbb{A}^{\mathbb{Z}} \to \mathbb{A}^{\mathbb{Z}}$ définie par

$$\sigma((x_i)_{i\in\mathbb{Z}}) := (x_{i+1})_{i\in\mathbb{Z}}.$$

Cette transformation est un homéomorphisme de $\mathbb{A}^{\mathbb{Z}}$.

Un sous-décalage est (la transformation induite sur) une partie fermée non vide de $\mathbb{A}^{\mathbb{Z}}$ stable par σ et σ^{-1}. Une telle partie peut toujours être définie par une famille (dénombrable) de mots (finis) interdits. Lorsqu'on peut la définir par une famille finie de de sous-mots interdits, on dit que le sous-décalage est de type fini. Lorsqu'on peut la définir par une famille de mots de longueur 2 interdits, il s'agit d'une chaîne de Markov topologique.

Les sous-décalages servent à comprendre des systèmes dynamiques plus complexes. Le but est de comprendre les premières propriétés des sous-décalages, des liens entre eux (facteurs, plongements, isomorphismes, codages), et plus si affinités.

Prérequis
Aisance en topologie et éventuellement en probabilités.

Bibliographie

1. Brin M., Stuck G. *Introduction to dynamical systems*, Cambridge University Press, (2002).

39 Systèmes de racines

Soit $(V, \langle\cdot,\cdot\rangle)$ un un espace euclidien. Pour tout vecteur non nul $a \in V$, notons σ_a la réflexion par rapport à l'hyperplan $(\mathbb{R}a)^\perp$:

$$\forall x \in V : \sigma_a(x) = x - 2[x : a]a, \text{ où } [x : a] := \frac{\langle a, x\rangle}{\langle a, a\rangle}.$$

Un système de racines dans V est une partie non vide finie Φ de V, dont les éléments sont appelés racines, tel que

1. Φ engendre V comme espace vectoriel,
2. pour tout $a \in \Phi$, $(\mathbb{R}a) \cap \Phi = \{a, -a\}$,
3. Φ est stable par les réflexions σ_a où $a \in V$,
4. pour tout $a \in \Phi$, $\sigma_a(b) - b \in \mathbb{Z}$, autrement dit $2[b : a] \in \mathbb{Z}$.

Les systèmes de racines les plus simples sont de la forme $\{a, -a\}$, où a est un vecteur non nul de V.

L'image d'un système de racines par une similitude vectorielle (directe ou inverse) est encore un système de racines.

Si V_1, V_2 sont des sous-espaces vectoriels supplémentaires et non triviaux de V et si Φ_1, Φ_2 des systèmes de racines dans V_1, V_2, alors $\Phi_1 \cup \Phi_2$ est un système de racines. Un tel système de racines est dit réductible.

Le but est de classifier à similitude près les systèmes de racines irréductibles. Dans $\mathbb{R}^n$, on trouve systématiquement quatre systèmes notés A_n, B_n, C_n, D_n. À ces quatre familles infinies s'ajoutent des systèmes de racines exceptionnels, appelés E_6, E_7, E_8, F_4, G_2.

Prérequis
Aisance avec la géométrie dans un espace euclidien.

Bibliographie

1. Boyer P. *Algèbre et Géométries*, Calvage et Mounet, (2015).

40 The Poincaré-Hopf theorem

It is not possible to comb the surface of a hairy ball without leaving at least one cleric (or imperfection) behind. A mathematical formulation of this result can be obtained, where the surface of the ball is a 2-dimensional sphere and the "hairs" are a set of vectors "tangent" to the sphere. The theorem was first proved by Brouwer in 1912, and generalizations of the result have been obtained even for geometric spaces more complicated than the sphere.

It will precisely be a matter of studying a similar result for differentiable manifolds (Poincaré-Hopf theorem) and understanding how there is a deep relationship between the topology of the geometric space and other "differential" objects that can be defined on it. Some interesting consequences of the theorem will also be deduced.

Prérequis
Algèbre et topologie de L3. Ability to speak and read in english.

Bibliographie

1. John W. Milnor, *Topology from the differentiable viewpoint*, 1965, The University Press of Virginia Charlottesville
2. John W. Milnor, *Morse Theory*, 1963, Princeton University Press

41 The Uniformization Theorem

Problems of classifying geometric objects, up to some equivalence relation, have always fascinated mathematicians from the earliest times. The Poincaré-Koebe's uniformization theorem is among them and concerns, first, the classification of simply connected domains of the complex plane up to biolomorphisms and, second, allows one to deduce surprising properties for smooth compact (without boundary) surfaces of

genus g from a complex geometry point of view.

It will involve fully understanding the meaning of the theorem, studying its proof, and deducing consequences that may vary depending on the time available and the student's preferences.

Prérequis
Cours de fonctions holomorphes du M1MG. Ability to speak and read in english.

Bibliographie

1. John H. Hubbard, *Teichmüller theory and applications to geometry, topology and dynamics (Volume 1)*, 2006, Matrix Editions
2. Ernesto Girondo and Gabino Gonzàlez-Diez, *Introduction to Compact Riemann Surfaces and Dessins d'Enfants*, 2012, Cambridge University Press
3. Yoichi Imayoshi and Masahiko Taniguchi, *An introduction to Teichmüller spaces*, 1992, Springer-Verlag Tokyo

42 Théorie de Floquet

L'équation de Hill est définie par,

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

où $q : \mathbb{R} \to \mathbb{R}$ est une fonction continue et périodique de période $T > 0$. On peut citer comme exemple d'application de cette equation, l'étude de l'orbite de la Lune autour de la Terre.
On définit y_1 et y_2 les solutions de (H) avec pour conditions initiales,

$$\begin{cases} y_1(0) = 1, \\ y_1'(0) = 0, \end{cases} \qquad \begin{cases} y_2(0) = 0, \\ y_2'(0) = 1. \end{cases}$$

On définit par u_1 et u_2 les deux racines (possiblement égales) du polynôme du second degré,

$$(E) \qquad u^2 - (y_1(T) + y_2'(T))u + 1 = 0.$$

Le théorème de Floquet pour l'équation de Hill donne les résultats suivants :
— si $u_1 \neq u_2$, il existe deux solutions indépendantes z_1 et z_2 de (H) telles que :

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

pour tout $t \in \mathbb{R}$.
— si $u_1 = u_2$ alors $u_1 = u_2 = \pm 1$ et il existe deux solutions indépendantes z_1 et z_2 de (H) 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
Soient $A \in \mathbb{C}(\mathbb{R}, \mathbb{M}_n(\mathbb{C}))$ périodique de période $T > 0$, et $\Phi(t)$ une matrice fondamentale du système $y' = A(t)\, y$.

— Il existe $P \in \mathcal{C}(\mathbb{R}, GL_n(\mathbb{C}))$ T-périodique et $B \in \mathbb{M}_n(\mathbb{C})$ constante, telle que :

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

— On note λ_k les valeurs propres de B et m_k leur multiplicité, pour $1 \leq k \leq p$, où p est le nombre de valeurs propres distinctes de B. Les solutions de $y' = A(t)\, y$ sont de la forme suivante,

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

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

Le théorème de Floquet caractérise le cas d'existence de solutions périodiques, et permet d'en étudier la stabilité. On s'intéressera aussi au théorème de Massera et au théorème de Reissig sur les solutions périodiques.

Prérequis

Aucun.

Bibliographie

1. Berthelin, F. (2017). *Equations différentielles*. Edition Cassini. ISBN 978-2-84225-229-8
2. Gonnord, S. et Tosel, N. (1998). *Thèmes d'analyse pour l'agrégation : Calcul différentiel*. Edition Ellipse. ISBN-10 2729858520
3. Reinhard, H. (1992). *Equations différentielles : Fondements et applications (mB)*. Edition Dunod. ISBN-13 : 978-2040154318

43 Un peu de dynamique des populations.

L'article "https ://images.math.cnrs.fr/Modelisation-d-une-epidemie-partie-1.html" présente le modèle SIR, utilisé en épidémiologie.

On étudiera la dynamique des solutions de ce système d'EDO (on pourra aussi se faire la main sur le système proie-prédateur de Lotka et Volterra, très classique, et étudié en détails dans le livre de F. Berthelin).

On pourra s'intéresser à différentes variantes de ce modèle, en particulier en envisageant une structuration par âge, qui mène à un système d'EDP (voir par exemple "https ://images.math.cnrs.fr/Modelisation-d-une-epidemie-partie-2.html"). Et des calculs numériques pourront être envisagés.

Prérequis

Cours d'analyse du premier semestre de M1.

Bibliographie

1. F. Berthelin, *Équations différentielles*.
2. L. Di Menza, *Analyse numérique des équations aux dérivées partielles*.