Université Grenoble Alpes **2017-2018**
M1 Mathématiques générales

Sujets de TER 2017-2018

Envoyer un mail au responsable du M1 (`didier.piau@univ-grenoble-alpes.fr`), avec le titre `M1 MG TER`, indiquant votre nom et les numéros des quatre sujets que vous souhaiteriez obtenir, par ordre de préférence décroissante, avant le **jeudi 30 novembre à minuit**.

Liste des sujets :

1. Algèbre des polynômes invariants sous l'action d'un groupe fini
2. Compression de données sans perte
3. Corps non commutatifs
4. Courbes algébriques réelles maximales
5. Courbes nodales aléatoires
6. Des inégalités isopérimétriques à la géométrie sous-riemannienne de contact
7. Diagrammes de Coxeter
8. Estimation à noyau de la densité
9. Facteurs premiers de certaines formes polynomiales
10. Films de savon et théorie des courants
11. Fonctions harmoniques, graphes de Cayley et propriété de Liouville
12. Graphes aléatoires et fonctions de seuil
13. Groupe de Witt d'un corps
14. Groupe fondamental et SO(3)
15. Inégalités de concentration et applications
16. Inégalités géométriques et courbure positive
17. Intégration numérique par méthode de quasi Monte Carlo
18. K-théorie de Milnor
19. Le lemme des mariages vu par les graphes, la moyennabilité des groupes et les décompositions paradoxales
20. Le problème de Waring
21. Marches auto-évitantes, constante de connectivité
22. Magnétisation spontanée
23. Méthodes modernes de factorisation des entiers
24. Orbites de familles de champs de vecteurs
25. Problème de Kakeya
26. Problème de Schwarz
27. Théorème de Poincaré-Bendixson
28. Topologie du plan
29. Un schéma de chiffrement basé sur les systèmes polynomiaux : HFE et sa cryptanalyse

1 Algèbre des polynômes invariants sous l'action d'un groupe fini

Il est connu que les polynômes en n indéterminées invariants sous l'action du groupe symétrique S_n forment une *algèbre de polynômes* en les polynômes symétriques élémentaires (voir le cours d'Algèbre 1 du M1).

Plus généralement, si k est un corps, tout sous-groupe fini G de $\mathrm{GL}_n(k)$ agit naturellement par automorphismes d'algèbres sur $A = k[X_1, \ldots, X_n]$, en stabilisant les composantes homogènes. On s'intéressera à l'algèbre A^G des polynômes invariants par G, dont un exemple simple montre qu'elle n'est pas toujours un anneau factoriel.

On cherchera à déterminer cette algèbre pour certains exemples de groupes G (petits groupes d'isométries, groupes A_n), et on en verra quelques propriétés générales : existence d'un nombre fini de générateurs, théorèmes de Noether et Molien pour aider à les trouver, etc.

On étudiera notamment le théorème de Chevalley-Shephard-Todd (en caractéristique nulle) selon lequel A^G a une structure d'*algèbre de polynômes* si et seulement si le groupe fini G est engendré par des pseudo-réflexions de k^n. On verra que dans ce cas les degrés des générateurs de A^G sont liés à la structure de G.

Pré-requis

On utilisera pour ce travail des notions vues dans le cours d'Algèbre 1 du M1, et aussi, de manière limitée, dans le cours d'Algèbre 2 du M1, dont ce sujet donne une illustration naturelle.

Bibliographie

Benson-Grove, *Finite reflection groups*, deuxième édition, chapitre VII.

Cox-Little-O'Shea, *Ideals, varieties and algorithms*, chapitre VII.

Arnaudiès-Bertin, *Groupes et géométrie*, tome 2, chapitre XXI.

2 Compression de données sans perte

Le stockage de données redondantes (lettres dans un texte, bases d'acides aminés dans une séquence ADN) écrites via un alphabet $\mathcal{A}$ commence par une opération de traduction. Par exemple, le stockage de données informatiques revient à se donner une application injective

$$c : \mathcal{A} \to \bigcup_{k \in \mathbb{N}^*} \{0,1\}^k$$

appelée *code*. Le but de la compression (optimale) de données est de trouver un code c qui minimise la longueur de la suite de 0 et de 1 utilisée pour stocker une suite de mots.

Supposons que les lettres que l'on souhaite stocker sont générées par une loi de probabilité p sur l'alphabet $\mathcal{A}$. Une lettre est donc modélisée par une variable aléatoire A de loi p. On peut montrer que pour tout code « raisonnable » c, la longueur moyenne d'une lettre codée est minorée par l'entropie de p, c'est-à-dire

$$E\left[\ell(c(A))\right] \geqslant H(p),$$

où ℓ est la fonction longueur et $H(p)$ est l'entropie de p, définie par

$$H(p) = -\sum_{a \in \mathcal{A}} p(\{a\}) \log_2 p(\{a\}).$$

Le travail proposé consiste à étudier les codes optimaux, dits codes de Huffman, et leur facteur de compression. On pourra également implémenter ces algorithmes de codage/décodage.

Pré-requis

Probabilités discrètes.

Bibliographie

O. Catoni (2004). *Statistical learning theory and stochastic optimization.* École d'été de Probabilités de Saint-Flour XXXI-2001 (Chapitre 1).

T.M. Cover, J.A. Thomas (2012). *Elements of information theory.* John Wiley & Sons (Chapitre 5).

3 Corps non commutatifs

La définition française d'un corps n'impose pas qu'il soit commutatif. Le corps non commutatif le plus connu est le corps $\mathbf{H}$ des quaternions, défini comme la $\mathbf{R}$-algèbre associatice et unifère engendrée par deux éléments I et J vérifiant les relations

$$I^2 = -1, \qquad J^2 = -1 \qquad \text{et} \qquad IJ = -JI.$$

Ce corps des quaternions est utilisé dans différents contextes : ainsi en arithmétique il permet de démontrer que tout nombre entier positif est somme de quatre carrés. En physique, la forme bilinéaire trace $(z, z') \mapsto \mathrm{tr}(zz')$, où la trace d'un élément z est la trace de l'opérateur de multiplication par z, correspond à l'espace-temps de Minkowski : elle est donnée dans la base $(1, I, J, IJ)$ par l'expression $4(tt' - xx' - yy' - zz')$.

Sur le corps des réels, une classification est donnée par le théorème de Frobenius :

Théorème (Frobenius). *Une* $\mathbf{R}$*-algèbre de dimension finie qui est un corps est isomorphe à* $\mathbf{R}$*,* $\mathbf{C}$ *ou* $\mathbf{H}$*.*

Si on se place sur un autre corps commutatif, comme celui des rationnels $\mathbf{Q}$, alors il est facile d'obtenir diverses algèbres non commutatives qui sont des corps et qui ne sont pas isomorphes, en considérant les relations

$$I^2 = a, \qquad J^2 = b \qquad \text{et} \qquad IJ = -JI$$

avec $a, b \in \mathbf{Q}$, et il est naturel d'essayer d'en trouver une classification.

De manière plus précise, soit $\mathbf{K}$ un corps. Les classes d'isomorphismes des algèbres de dimension finie sur $\mathbf{K}$ qui sont un corps et dont le centre est $\mathbf{K}$ forment un ensemble. Ce qui est remarquable est que cet ensemble peut être muni naturellement d'une loi de groupe. On obtient ainsi le groupe de Brauer $\mathrm{Br}(\mathbf{K})$.

Ce groupe est un invariant fondamental qui revient dans de très nombreux contextes en mathématiques, aussi bien pour la classification des quadriques sur un corps quelconque, qu'en théorie des nombres ou même en géométrie.

Pré-requis

Le contenu des unités d'algèbres du L3 et du premier semestre de M1.

Bibliographie

[1] A. Blanchard, *Les corps non commutatifs*, Presses Universitaires de France, Paris (1972).

[2] N. Bourbaki, *Algèbre, Chapitre III, §2*, Springer-Verlag, Berlin (1970).

[3] N. Bourbaki, *Algèbre, Chapitre VIII*, Springer-Verlag, Berlin (2012).

4 Courbes algébriques réelles maximales

Un polynôme réel en une variable réelle de degré d possède au maximum d racines réelles, et cette borne est toujours atteinte. Qu'en est-il en deux variables ? Cette fois le lieu d'annulation est la réunion d'un certain nombre de courbes, des cercles topologiques pour les composantes bornées. Peut-on borner le nombre de ces composantes par une fonction du degré ? Cette borne est-elle toujours atteinte ?

Cette vieille et jolie question a été résolue élégamment par Axel Harnack en 1876. Le travail proposé montre qu'on peut résoudre des problèmes d'algèbre avec de l'analyse, de la topologie et de la géométrie.

Pré-requis

Cours de L3, surtout calcul différentiel.

Bibliographie

Bochnak, Jacek, Coste, Michel, Roy, Marie-Françoise, *Géométrie algébrique réelle*, Springer Science & Business Media, 1987.

5 Courbes nodales aléatoires

Le laplacien sur la sphère ronde possède un spectre discret, infini, tendant vers l'infini et de plus en plus dégénéré. Nazarov et Sodin ont démontré qu'il existe une constante $a > 0$ telle que, si l'on tire au hasard une grande valeur propre L, alors, avec grande probabilité, le nombre de composantes connexes du lieu d'annulation de la fonction propre associée à la valeur propre L est très proche de aL.

Le travail proposé consiste à comprendre la démonstration de ce résultat.

Pré-requis

Cours de L3 d'analyse, calcul différentiel et probabilités.

Bibliographie

F. Nazarov, M. Sodin, *On the number of nodal domains of random spherical harmonics*, Amer. J. Math. 131 (2009), no. 5, 1337-1357.

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

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

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

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

Ce sujet est lié au thème du M2R Mathématiques fondamentales proposé en 2018-2019.

Bibliographie

L. Pontriaguine, V. Boltianski, R. Gamkrelidze, E. Michtchenko, *Théorie mathématique des processus optimaux*. Traduit du russe par Djilali Embarek. (French), Moscou, Editions Mir (1974).

D. Barilari, *Introduction to Riemannian and sub-Riemannian geometry*, preprint.

7 Diagrammes de Coxeter

La théorie des diagrammes de Coxeter établit des liens remarquables entre trois classes d'objets :

1. combinatoires (des graphes dont les arêtes sont étiquetées par des entiers)
2. algèbriques (des groupes abstraits, appelés groupes de Coxeter, engendrés par des involutions et des relations entre celles-ci)
3. géométriques (des groupes de symétries de l'espace euclidien engendrés par des réflexions)

Le travail proposé consiste à utiliser la théorie des diagrammes de Coxeter pour classer les groupes de réflexions finis. Selon le temps et l'envie, on pourra aller jusqu'à étudier les liens entre cette théorie et les algèbres de Lie.

Pré-requis Cours d'algèbre de L3 et une bonne visualisation géométrique.

Bibliographie

Coxeter, H.S.M. (1934), *Discrete groups generated by reflections*, Ann. of Math., 35 (3) : 588-621.

Coxeter, H.S.M. (1935), *The complete enumeration of finite groups of the form* $r_i^2 = (r_i r_j)^{k_{ij}} = 1$, J. London Math. Soc., 1, 10 (1) : 21-25.

Humphreys, James E. (1992) [1990], *Reflection Groups and Coxeter Groups*, Cambridge Studies in Advanced Mathematics.

8 Estimation à noyau de la densité

On souhaite estimer la densité f de la variable aléatoire X en un point x. Pour cela, on dispose d'un échantillon $X_1, X_2, \cdots, X_n$ de variables aléatoires indépendantes et identiquement distribuées selon la loi de X. Pour simplifier, on suppose que X est à valeurs réelles et que f est la densité par rapport à la mesure de Lebesgue λ sur $\mathbb{R}$. On souhaite construire un estimateur de f en n'importe quel point x sans hypothèse paramétrique sur la densité inconnue f.

Le travail proposé consiste à étudier et implémenter à l'aide du logiciel R la procédure dite à noyau de f et à étudier ses propriétés asymptotiques.

Bibliographie

A.B. Tsybakov, Introduction à l'estimation non-paramétrique (Chapitre 1).

9 Facteurs premiers de certaines formes polynomiales

Il s'agit d'un sujet d'arithmétique. On étudiera les facteurs premiers des formes polynomiales $\Delta_m(P) = \prod_\alpha (1 - \alpha^m)$, où les nombres α énumèrent les racines d'un polynôme P unitaire de $\mathbb{Z}[X]$, de sorte que, pour tout m, $\Delta_m(P)$ est un entier.

Suivant [L], on établira des propriétés arithmétiques des facteurs premiers des $\Delta_m(P)$; un intérêt est que ces facteurs permettent de construire de grands nombres premiers. On verra aussi, suivant [P], un critère en terme de $\Delta_{p-1}(P)$ pour que la réduction de P modulo p premier admette une racine dans $\mathbb{F}_p$. On étudiera plus particulièrement le cas où P est de degré 2 ou 3.

Notons que [L] contient la formulation par Lehmer de son problème concernant la mesure de Mahler $M(P) = \prod_\alpha \max(1, |\alpha|)$ des polynômes unitaires P.

Pré-requis

Ce travail utilisera des éléments du cours d'Algèbre 1 (anneaux et corps) ainsi que la notion de résultant et la décomposition des idéaux premiers de $\mathbb{Z}$ dans l'anneau d'entiers d'une extension finie de $\mathbb{Q}$ (voir [S] chapitre V).

Bibliographie

[L] D. Lehmer, *Factorization of certain cyclotomic functions*, Annals of Mathematics 34 (1933), 461-479.

[P] T. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 - \alpha_i^n)$, Annals of Mathematics 18 (1919), 53-64.

[S] P. Samuel, *Théorie algébrique des nombres*, Hermann, 1971.

10 Films de savon et théorie des courants

Le problème de Plateau (du nom du physicien belge Joseph Plateau, 1801-1883), consiste à déterminer la surface d'aire minimale qui borde un contour donné. La question revient (à peu près) à déterminer le film de savon obtenu quand on plonge un fil électrique (le contour) dans une eau savonneuse. Une approche, due à Federer et Fleming, est de considérer la théorie des courants.

Le travail proposé consiste à comprendre cette formalisation et la solution du problème de Plateau dans ce cadre. Si le temps le permet, on considèrera aussi la formulation du problème due à Reifenberg (à la même période que Federer et Fleming) en termes d'homologie (topologie algébrique).

Pré-requis

Théorie de la mesure (L3), Calcul différentiel (L3), Analyse fonctionnelle (M1).

Bibliographie

M. Do Carmo, *Differential forms and applications*, Springer (1994).

F. Morgan, *Geometric measure theory : A beginner's guide*, Academic Press (2016).

11 Fonctions harmoniques, graphes de Cayley et propriété de Liouville

Une fonction à valeurs réelles définie sur un graphe est dite *harmonique* si elle vaut en chaque sommet la moyenne de ses valeurs sur les sommets voisins. Sur un graphe fini et connexe, il n'est pas difficile de montrer que toutes les fonctions harmoniques sont constantes, mais le cas de graphes infinis (par exemple les réseaux $\mathbb{Z}^d$, les arbres, etc.) est plus intéressant. On dit qu'un tel graphe a la propriété de Liouville si toutes les fonctions harmoniques *bornées* y sont constantes ; savoir si un graphe donné possède cette propriété est en général difficile, et exhiber un graphe qui ne l'a pas demande déjà un peu de réflexion.

Le travail proposé consiste tout d'abord à comprendre ces notions et la preuve du fait que les réseaux $\mathbb{Z}^d$ ont la propriété de Liouville, ce qui peut se faire de plusieurs façons et notamment en utilisant comme outils des marches aléatoires, puis la construction d'un arbre qui porte une fonction harmonique bornée non constante. On étudiera ensuite une classe de graphes dits *graphes de Cayley*, construits à partir de groupes et qui fournissent des exemples intéressants de graphes ayant des propriétés variées.

Le but final est de comprendre un résultat de Amir et Kozma qui énonce que tout graphe de Cayley à croissance exponentielle porte une fonction harmonique positive.

Pré-requis

Le programme de L3.

Bibliographie

Djalil Chafaï, Florent Malrieu, Recueil de modèles aléatoires, Springer, 2016.

G. Amir, G. Kozma, Every exponential group supports a positive harmonic function, arXiv 1711.00050 (2017).

12 Graphes aléatoires et fonctions de seuil

On considère le modèle de graphes aléatoires dit d'Erdős-Rényi, dans lequel un graphe G possède un nombre N de sommets et des arêtes apparaissent entre ces sommets avec une certaine probabilité p. On se propose d'étudier le comportement de la probabilité

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

où M est une caractéristique donnée du graphe G, par exemple : G est connexe, G possède un sommet isolé, G admet un cycle qui visite chaque sommet une fois, etc. Plus précisément, on fixe une fonction probabilité $p(N)$ variant avec N et on considère le comportement de $P(N, p(N), M(G))$ quand $N \to \infty$.

Depuis le travail fondateur d'Erdős, on sait 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 la propriété M.

Le travail proposé consiste à étudier la notion de fonction seuil et à établir son existence et sa valeur pour certaines propriétés M importantes, notamment le fait d'être connexe, ou de contenir un sous-graphe donné, ou d'admettre une composante géante.

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

Le cas écheant, ce travail pourra être étendu à d'autres propriétés des graphes aléatoires, comme l'existence de certains cycles, la k-connectivité, ou les coloriages du graphe.

Pré-requis

Cours de probabilité de L3 et L2.

Bibliographie

B. Bollobas, *Random Graphs.*

P. Erdős, A. Rényi (1959), *On Random Graphs I*, in Publ. Math. Debrecen 6, p. 290-297.

13 Groupe de Witt d'un corps

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

Le projet est basé sur le livre de T.Y. Lam, *Introduction to quadratic forms over fields* (AMS, Graduate Studies in Mathematics, 67, 2005).

14 Groupe fondamental et SO(3)

Ou :

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

Le groupe fondamental $\pi_1(T, t)$ d'un espace topologique T contenant un point t est un invariant qui donne une réponse rigoureuse à la question floue : combien l'espace T contient-il de trous ? Par ailleurs, lorsque l'espace T est « assez gentil », on peut construire à l'aide du groupe fondamental un recouvrement universel $V \to T$ qui a la propriété de « déplier » totalement l'espace T.

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

Pré-requis

Cours d'algèbre et topologie du L3.

Bibliographie

Massey, *Algebraic Topology.*

Rotman, *An introduction to Algebraic Topology.*

Berger, *Géométrie.*

15 Inégalités de concentration et applications

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

$$P\left(|X - E\left[X\right]| \geqslant a\right) \leqslant \frac{\mathrm{Var}(X)}{a^2}.$$

Le travail proposé consiste à étudier plusieurs inégalités de concentration (de Hoeffding, de Bernstein, etc) et les principales méthodes utilisées pour les obtenir. On pourra également s'intéresser à certains de leurs cadres d'application, comme les matrices aléatoires, les sommes permutées, ou certains problèmes statistiques.

Pré-requis

Probabilités (L3).

Bibliographie

S. Boucheron, G. Lugosi, P. Massart (2013). *Concentration inequalities : A nonasymptotic theory of independence*, Oxford University Press, 2013 (Chapitres 1 et 2).

16 Inégalités géométriques et courbure positive

En géométrie riemannienne, la positivité de la courbure implique des inégalités géométriques comme celles de Poincaré ou de Brunn-Minkowski, aux applications nombreuses.

Le travail proposé consiste à étudier comment, dans un espace métrique mesuré, on peut étendre ces résultats sous une condition de courbure positive au sens du transport optimal.

Pré-requis

Théorie de la mesure (L3), Calcul différentiel (L3), Analyse fonctionnelle (M1). Aucun pré-requis : en géométrie différentielle.

Bibliographie

C. Villani, *Optimal transportation : old and new*, Springer (2008).

17 Intégration numérique par méthode de quasi Monte Carlo

La méthode de quasi Monte Carlo (QMC) permet l'intégration numérique par l'utilisation de suites dites à discrépance faible. Elle est une alternative à la méthode de Monte Carlo (MC) qui utilise des suites de nombres pseudo-aléatoires.

Les méthodes MC et QMC permettent d'approcher l'intégrale d'une fonction f par la moyenne des valeurs de la fonction évaluée en un ensemble de points $x_1, \ldots, x_N$, c'est-à-dire

$$\int_{[0,1]^d} f(u)du \approx \frac{1}{N}\sum_{i=1}^{N} f(x_i).$$

La différence entre MC et QMC tient dans le choix des points x_i dans $[0,1]^d$. Alors que MC utilise une suite de nombres pseudo-aléatoires, QMC utilise des suites déterministes telles que la suite de Halton, la suite de Sobol ou la suite de Faure, connues pour leur discrépance faible, c'est-à-dire leur capacité à bien remplir le cube unité en dimension d. L'un des avantages est de permettre une convergence plus rapide par QMC, pouvant aller jusqu'à $\mathcal{O}\left(\frac{1}{N}\right)$ alors que MC est en $\mathcal{O}\left(\frac{1}{\sqrt{N}}\right)$.

Bibliographie

C. Lemieux, Monte Carlo and quasi-Monte Carlo sampling, Springer, 2009.

18 K-théorie de Milnor

Si k est un corps, on définit l'anneau de K-théorie de Milnor comme l'algèbre tensorielle du groupe abélien k^* modulo une certaine relation appelée relation de Steinberg. Le résultat est un anneau gradué et les composantes homogènes de degré n, notées $K_n^M(k)$, sont les groupes de K-théorie de Milnor en poids n. Bien que définie de manière élémentaire, la K-théorie de Milnor est paradoxalement devenue l'un des objets centraux de la K-théorie algébrique et par extension joue un rôle très important en géométrie algébrique et en théorie des nombres. Une des questions fondamentales est de proposer des méthodes de calcul, et la manière naturelle de le faire est d'étudier les propriétés fonctorielles des groupes $K_n^M(k)$ ainsi que leurs relations avec d'autres objets classiques des mathématiques comme la cohomologie galoisienne ou les groupes de Witt. Ces relations ont d'ailleurs fait l'objet des fameuses conjectures de Milnor et de Bloch-Kato, résolues récemment par Voevodsky.

Le but du projet est de lire l'article fondateur de Milnor, *Algebraic K-theory and quadratic forms* (Invent. Math., 1970, 9, 318-344).

19 Le lemme des mariages vu par les graphes, la moyennabilité des groupes et les décompositions paradoxales

« Tout le monde » connaît le théorème de Cantor-Bernstein : si A et B sont deux ensembles, et s'il existe une injection de A dans B et une injection de B dans A, alors il existe une bijection entre A et B. L'énoncé semble évident, mais sa preuve est parfois vécue comme une épisode obscur et embarrassant de la théorie des ensembles.

Il existe une preuve de ce résultat, qu'on peut juger éclairante, à base de théorie des graphes. Un graphe est la donnée d'un ensemble V (de sommets) et d'un ensemble E (d'arêtes) avec des applications d'attachement (qui disent quels sont les sommets extrêmités de chaque arête). Le vocabulaire de la topologie (chemin, composante connexe, etc.) s'y trouve pratique. Une traduction de l'énoncé de Cantor-Bernstein en terme de graphes nous procure un graphe dont les composantes connexes sont très simples, et qui donne très intuitivement la bijection cherchée, composante par composante. Ce sera le point de départ du travail proposé.

Une amélioration de l'argument permet de montrer, de manière également agréable, le lemme des mariages de Hall, qui dit que, si l'on a deux ensembles d'individus, disons A et B, tels que :

— à chaque personne de A correspond un sous-ensemble fini de B préféré,

— pour chaque sous ensemble fini X de A, l'union des sous-ensembles de B préférés par les éléments de X est plus grande (en cardinal) que X,

alors il y a une application (dite, de mariage) de A vers B qui est injective, et telle que l'image de chaque élément appartient à la partie préférée de l'élément. Un certain nombre de variations sont possibles, dans lesquelles, par exemple, A et B jouent le même rôle.

Une application qui devrait être le but du travail proposé est de comprendre comment ce résultat est relié aux groupes moyennables. Un groupe est moyennable, s'il admet une moyenne invariante par multiplication (du groupe, à gauche). Une moyenne est une application de l'ensemble des parties dans $[0, 1]$ qui est finiment additive, et qui vaut 1 sur le groupe entier.

S'il est trivial que tout groupe fini est moyennable, il n'est pas si facile de le voir pour $\mathbb{Z}$. Cela peut être vu par une utilisation du théorème de Hahn-Banach. Enfin, l'existence de groupes non-moyennables est peut être surprenante, mais pas difficile du tout. L'exemple le plus simple est celui du groupe libre à deux générateurs. C'est le point clé du célèbre paradoxe de Banach-Tarski (le découpage de la boule unité de $\mathbb{R}^3$ (euclidien) en un ensemble fini de parties, qui, déplacées dans $\mathbb{R}^3$ (isométriquement !) reconstruisent précisément deux boules de même rayon que la première).

Le lemme des mariages, vu plus haut, nous place à l'entrée du théoreme de Tarski-Fölner, qui caractérise les groupes moyennables, en terme, par exemple, d'absence de décomposition paradoxale, comme celle de Banach-Tarski.

Le sujet est assez modulable/étirable. La référence qui sert à l'introduction, et au théorème de Tarski-Følner est une (petite) partie du livre récent en référence.

Saveurs :

Graphes, groupes, analyse fonctionnelle.

Bibliographie

Tullio Ceccherini-Silberstein, Michel Coornaert, *Cellular automata and groups*, Springer Monographs in Mathematics, Springer, 2010.

20 Le problème de Waring

En 1770, Edward Waring pose la question de savoir si, pour tout entier strictement positif d, il existe un entier s tel que tout entier positif s'écrive comme somme de s puissances d-èmes. Autrement dit :

$$\forall n \in \mathbf{N},\ \exists (x_1, \ldots, x_s) \in \mathbf{N}^n, \quad n = \sum_{i=1}^{s} x_i^d.$$

Une réponse positive est donnée par Hilbert en 1909. Depuis, la méthode du cercle a permis non seulement de montrer l'existence de solutions mais d'en estimer le nombre. Cette méthode repose sur une application simple de la formule élémentaire

$$\int_0^1 \exp(2i\pi kt)\mathrm{d}t = \begin{cases} 0 \text{ si } k \neq 0, \\ 1 \text{ si } k = 0. \end{cases} \quad .$$

Pré-requis

Modules d'analyse de la licence, modules d'algèbre de la licence et du premier semestre de M1.

Bibliographie

[1] *Épreuve commune de 6 heures ENS 2007.*
`www.ens.fr/IMG/file/concours/2007/MP/mp_math_mpi1.pdf`

[2] R. C. Vaughan, *The Hardy-Littlewood method*, Cambridge Tracts in Math. 125, Cambridge University Press (2003).

21 Marches auto-évitantes, constante de connectivité

Une *marche aléatoire auto-évitante* sur un réseau est un chemin sur ce réseau qui ne passe jamais deux fois par le même sommet. Si c_n désigne le nombre de tels chemins issus d'un sommet fixé et de longueur n, un argument de sous-multiplicativité implique qu'il existe une constante μ, qui dépend du réseau, pour laquelle

$$c_n = \mu^{n+o(n)}.$$

Cette constante porte le nom de *constante de connectivité* du réseau ; on ne sait pas en général calculer sa valeur.

Un résultat marquant obtenu récemment par Duminil-Copin et Smirnov est que, dans le cas du réseau hexagonal (en « nid d'abeille »),

$$\mu = \sqrt{2+\sqrt{2}}.$$

Le travail proposé consiste à comprendre la preuve de ce résultat, qui a la particularité d'être basée sur des méthodes élémentaires (mais très astucieuses).

Pré-requis

Aucun (il faut savoir ce qu'est un nombre complexe).

Bibliographie

N. Madras, G. Slade. The Self-avoiding Walk. Birkhäuser, 1993.

H. Duminil-Copin, S. Smirnov, The connective constant of the honeycomb lattice equals $\sqrt{2+\sqrt{2}}$. Annals of Mathematics, 175 (2010), 1653–1665.

22 Magnétisation spontanée

Le travail proposé consiste à comprendre la preuve donnée par le physicien théoricien Rudolf Peierls en 1936 du phénomène de magnétisation spontanée du modèle d'Ising dans le plan à basse température. Avant d'aborder la preuve proprement dite, on commencera par définir chacun de ces termes mathématiquement. Si le temps le permet, on pourra ensuite s'intéresser au calcul exact du point de Curie et à la solution du modèle d'Ising proposée par le physicien et chimiste Lars Onsager en 1942.

Pré-requis

Cours de probabilités de L2 et de L3. Une absence d'aversion pour les modèles mathématiques inspirés de la physique.

Bibliographie

Barry Cipra, An Introduction to the Ising Model, *Amer. Math. Monthly* 94, 937-959, 1987.

Sacha Friedli, Yvan Velenik, Statistical Mechanics of Lattice Systems : a Concrete Mathematical Introduction, Cambridge, 2017 (Chapitre 3).

Robert B. Griffiths, Peierls proof of spontaneous magnetization in a two-dimensional Ising ferromagnet, *Phys. Rev.* 136, A437-A439 (1964).

Ross Kindermann, J. Laurie Snell, Markov Random Fields and their Applications, Contemporary Mathematics 1, AMS, 1980 (Chapitre 1).

23 Méthodes modernes de factorisation des entiers

Il est (relativement) facile de déterminer si un grand nombre entier N est premier, mais beaucoup plus difficile de le factoriser en général. Les records actuels sont basés sur deux algorithmes. La première méthode, factorisation par courbes elliptiques, est efficace quand un des facteurs de N n'est pas trop gros. La deuxième méthode appartient à la famille des calculs d'indice, dont le principe de base est d'essayer de combiner des relations non triviales afin d'obtenir une congruence de carrés modulo N. Le crible des corps de nombres utilise les anneaux d ?entiers d'extensions des rationnels afin d'obtenir ces relations rapidement.

Pré-requis

Cours d'algèbre du premier semestre. Cours d'introduction à la cryptologie du deuxième semestre. Absence d'aversion pour l'algorithmique.

Bibliographie

H. Lenstra, *Factoring Integers with Elliptic Curves*, Annals of Mathematics 126, 1987.

C. Pomerance, *A Tale of two Sieves*, Notices of the AMS 43, 1996.

24 Orbites de familles de champs de vecteurs

Le travail proposé consiste à lire et à comprendre la preuve du théorème de Sussmann.

Soit M une variété connexe et $F_1, \ldots, F_k$ des champs de vecteurs sur M.

Le théorème de Sussmann (1973) établit que l'orbite de tout point q, c'est-à-dire ici l'ensemble des points que l'on peut obtenir à partir de q en intégrant alternativement les champs de vecteurs $F_1, \ldots, F_k$ en temps positifs ou négatifs, est une sous-variété immergée de M.

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

Ces deux théorèmes sont fondamentaux, en particulier en théorie du contrôle pour répondre à la question de la contrôlabilité, c'est-à-dire la possibilité effective de contrôler un système, d'amener le système d'un état à un autre.

Ce sujet est lié au thème du M2R Mathématiques fondamentales proposé en 2018-2019.

Bibliographie

H.J. Sussmann, *Orbits of Families of Vector Fields and Integrability of Distributions*, Transactions of the American Mathematical Society, Vol. 180, pp. 171-188 (1973).

W.L. Chow, *Űber Systeme von linearen partiellen Differentialgleichungen erster Ordnung* (en Allemand), Mathematische Annalen, 117 : 98-105 (1939).

P.K. Rashevskii, *About connecting two points of complete non-holonomic space by admissible curve* (en Russe), Uch. Zapiski ped. inst. Libknexta (2) : 83-94 (1938).

25 Problème de Kakeya

Voici deux questions de nature géométrique :

Question 1 (Kakeya, 1917) : Quelle est l'aire minimale nécessaire pour retourner une aiguille dans le plan ?

Question 2 (Conjecture de Kakeya) : Quelle peut être la dimension de Hausdorff d'un ensemble de Kakeya en dimension n ?

Un ensemble de Kakeya en dimension $n \geqslant 2$ est un sous-ensemble de $\mathbb{R}^n$ à l'intérieur duquel un segment unité peut être tourné continûment d'un tour complet, revenant à sa position initiale. Il existe des ensembles de Kakeya de mesure de Lebesgue nulle donc l'aire minimale pour retourner une aiguille est 0.

Le travail proposé consiste à donner des solutions aux deux questions précédentes (pour la seconde, seulement dans le plan). On construira en particulier un ensemble de Kakeya de mesure nulle à partir d'ensembles de Cantor. La réponse à la deuxième question est largement ouverte pour $n \geqslant 3$. On étudiera le cas plus simple des corps finis qui admet une solution simple et surprenante (due à Zvir en 2007).

Pré-requis

Théorie de la mesure (L3), quelques notions sur les corps finis (M1).

Bibliographie

K. Falconer, *The geometry of fractal sets*, Cambridge University Press (1986).

T. Wolff, *Lectures on harmonic analysis*, American Mathematical Society (2003).

26 Problème de Schwarz

On s'intéressera à la monodromie des solutions de l'équation différentielle hypergéométrique, dans le but de classifier les exposants pour lesquels ces solutions sont algébriques (ce problème a été résolu par H.A. Schwarz en 1873). Il faudra comprendre l'analogue du théorème de Cauchy-Lipschitz dans le contexte des fonctions holomorphes, utiliser le principe de prolongement analytique et comprendre la notion de groupe fondamental pour définir le groupe de monodromie. On traduira ensuite la condition d'algébricité en un problème de géométrie sphérique assez élémentaire (à savoir, quand le groupe engendré par deux rotations sur la sphère est-il discret ?).

Pré-requis

Équations différentielles. Fonctions holomorphes.

Bibliographie

G. D. Mostow, Braids, hypergeometric functions, and lattices, Bulletin AMS (16) 2, 1987.

C. Moreau-d'Halluin, M.-C. Gaultier de Kermoal, Théorie de Galois des équations différentielles linéaires homogènes du second ordre à solutions algébriques, Thèses de l'université de Lille 1, 1982.

J. Gray, Linear Differential Equations and Group Theory from Riemann to Poincaré, Birkhäuser 1986.

27 Théorème de Poincaré-Bendixson

Il s'agit d'un théorème sur la théorie qualitative des systèmes d'équations différentielles dans le plan, qui prédit l'existence de solutions périodiques. La démonstration utilise entre autres le théorème de redressement du flot, et le théorème de Jordan (toute courbe fermée simple dans le plan sépare le plan en deux composantes connexes, l'une homéomorphe à un disque, l'autre non bornée), dont il faudra donner une preuve.

Pré-requis

Équations différentielles, champs de vecteurs, topologie élémentaire.

Bibliographie

S. Cantat, Théorème de Poincaré-Bendixson, Journal de maths des élèves de l'ENS Lyon (1) 1995, 140–145.

G. Teschl, Ordinary differential equations and dynamical systems, Graduate Studies in Mathematics 140 (2012).

S. Benzoni-Gavage, Calcul différentiel et équations différentielles, Dunod, 2010.

28 Topologie du plan

Le travail proposé consiste à démontrer quelques résultats de topologie dans le plan, à savoir :

Théorème de Brouwer : Toute application continue du disque unité fermé dans lui-même admet un point fixe.

Théorème de l'image ouverte : L'image de tout ouvert du plan par une application continue injective est ouverte.

Théorème de Jordan : Si Γ est l'image d'un lacet simple dans le plan, alors le complémentaire de Γ comporte exactement deux composantes connexes, et la frontière commune de ces composantes connexes est Γ.

Les outils nécessaires généralisent la notion d'indice d'un lacet de classe C^1 par morceaux dans le plan complexe et font appel aux notions d'homotopie et de détermination continue du logarithme, ainsi qu'au théorème de Tietze-Urysohn dans le cas d'un espace métrique.

Pré-requis

Topologie des espaces métriques, fonctions holomorphes (un peu), groupes (un peu).

Bibliographie

É. Amar, É. Matheron, *Analyse Complexe*, Cassini (2004).

29 Un schéma de chiffrement basé sur les systèmes polynomiaux : HFE et sa cryptanalyse

Étant donnée une application polynomiale de K^n dans K^m, déterminer un antécédent d'un élément de K^m revient à résoudre un système de m équations polynomiales en n variables. Mais la résolution d'un tel système est difficile en général, ce qui pourrait fonder la sécurité d'un protocole de cryptographie. Pour obtenir un schéma de chiffrement, Patarin a proposé en 1996 le système HFE (Hidden Field Equations), utilisant une transformation polynomiale de $(\mathbb{F}_p)^n$ dans $(\mathbb{F}_p)^n$ induite par une application facilement inversible de $\mathbb{F}_{p^n}$ dans $\mathbb{F}_{p^n}$, masquée par des transformations linéaires aléatoires. Il se trouve que les systèmes polynomiaux ainsi créés ne sont pas assez difficiles à inverser, ce qui a permis à Faugère et Joux de résoudre en 2002 plusieurs challenges HFE.

Pré-requis

Cours d'algèbre du premier semestre. Cours d'introduction à la cryptologie du deuxième semestre. Absence d'aversion pour l'algorithmique.

Bibliographie

J.-C. Faugère et A. Joux, *Algebraic Cryptanalysis of Hidden Field Equation (HFE) Cryptosystems Using Gröbner Bases*. Advances in Cryptology - CRYPTO 2003, LNCS 2729.

J. Patron, *Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP) : two new Families of Asymmetric Algorithms*. Advances in Cryptology - EUROCRYPT '96, LNCS 1070