D. LESESVRE, P. MONTAGNON
P. LE BARBENCHON, T. PIERRON

131 DÉVELOPPEMENTS POUR L'ORAL

AGRÉGATION EXTERNE
MATHÉMATIQUES / INFORMATIQUE

DUNOD

Conception de maquette de couverture : Hokus Pokus Création

11 Rue Paul Bert, 92240 Malakoff
ISBN 978-2-10-079556-7

Avant-propos

Préparation à l'agrégation. L'année de préparation à l'agrégation est riche en émotions et en découvertes. Elle marque un temps durant lequel la grande liberté laissée à l'agrégatif peut devenir un obstacle : il faut gérer de front l'apprentissage de contenus théoriques nouveaux, la préparation d'écrits techniques, l'entraînement aux épreuves de modélisation et la cartographie d'une immense bibliographie requise pour pouvoir présenter pas moins d'une centaine de leçons spécialisées à l'oral. L'ambition de ce livre est d'accompagner le candidat dans ce cheminement en proposant une gamme variée de développements de mathématiques et d'informatique taillés pour les oraux de l'agrégation externe. Les thèmes d'étude proposés illustrent de manière vivante et originale les concepts, en couvrant toutes les leçons du programme et en proposant des ouvertures dans de nombreuses directions d'approfondissement.

Prise de recul. Préparer l'agrégation ne revient pas à accumuler des connaissances érudites sans liens les unes avec les autres. Bien au-delà de la liste de leçons et de chapitres au programme, cette préparation constitue l'occasion d'une prise de recul fondamentale pour le futur enseignant. Que ce soit sur des sujets élémentaires abordés en première année d'université, tels que les espaces vectoriels ou les suites numériques, ou des sujets plus élaborés, comme les algèbres de Lie ou les variétés différentielles, l'agrégatif se doit d'acquérir une aisance tant théorique que pratique. L'objectif, bien sûr, n'est pas de devenir un expert de chaque domaine. Cela n'est ni possible compte tenu du temps disponible, ni souhaitable. L'évaluation porte sur la maîtrise des idées présentées : le candidat reste libre de choisir le niveau de difficulté de ses leçons et l'ampleur de leurs contenus, l'élément essentiel pris en compte étant indubitablement la maîtrise du corpus présenté et la clarté de l'exposition.

Ainsi, il vaut mieux (pour le candidat comme pour l'auditoire, qu'il s'agisse d'un jury d'agrégation ou d'une classe d'étudiants) présenter une leçon très élémentaire de façon vivante et parfaitement maîtrisée, illustrée par des exemples et des applications et faisant apparaître avec clarté l'enchaînement et l'entrelacement des idées, plutôt qu'un exercice de haute voltige technique et conceptuelle mal exécuté. L'un des défis de la préparation à l'agrégation est donc de trouver un chemin heureux entre le niveau de compréhension de l'étudiant, qui découvre pour la première fois les notions présentées, et celui de l'expert. Ce défi constitue aussi celui du présent ouvrage qui, loin d'une introduction au programme de l'agrégation, tisse des liens entre les différentes parties du programme et invite à prendre de la hauteur sur les notions déjà connues.

Ouverture culturelle. L'année passée à préparer le concours est également l'occasion d'une grande ouverture culturelle. Le candidat, qu'il sorte de quelques années d'études ou qu'il soit déjà professeur, n'a pas nécessairement eu l'occasion de lire des myriades d'ouvrages, de revenir sur des cours passés ou d'explorer des résultats et des domaines moins classiques bien qu'ils soient tout à fait accessibles. Dans ce livre, nous avons eu à cœur d'ouvrir autant de portes que possible vers de tels horizons.

Les auteurs, agrégés et pour la plupart docteurs dans différentes branches des mathématiques ou de l'informatique, ont voulu mettre à profit leurs cultures particulières ainsi que leur goût pour la pédagogie de sorte à proposer un corpus polychrome de développements originaux. Ceux-ci, souvent construits à partir de la littérature spécialisée, ont été sélectionnés pour leur pertinence ou leur importance, puis adaptés au format de l'épreuve orale. De nombreux thèmes généralement absents des contenus de l'agrégation, mais pourtant tout à fait naturels pour illustrer les leçons et mettre en contact des idées trop souvent séparées, sont ainsi développés : théorie analytique des nombres, utilisation de l'analyse complexe en algèbre linéaire, actions de groupes en géométrie, études de permutations aléatoires, principes d'incertitude pour les groupes, analyse p-adique, ou encore étonnantes relations entre nombres premiers et polynômes irréductibles, parmi tant d'autres merveilles. Lorsque le thème s'y prête, nous présentons des développements à l'interface avec d'autres disciplines, peu abordées dans un cursus universitaire de mathématiques et donc rarement connues des agrégatifs, comme l'économie, la théorie des jeux, la biologie, la physique ou l'épidémiologie.

L'oral de l'agrégation. Le format des oraux de l'agrégation (3 heures de préparation, 6 minutes de présentation du plan, 15 minutes de développement et 40 minutes de discussion et questions environ) ne doit pas mener à apprendre par cœur des dizaines de développements pointus et des condensés entiers de théorie, mais exige une aisance certaine avec les idées présentées et la bibliographie. La longue durée de préparation avant l'oral, avec un accès à une bibliothèque et à des livres personnels, donne clairement le ton de l'épreuve : en consultant une démonstration, l'agrégatif doit se remettre en tête en quelques dizaines de minutes la marche des idées et l'enchaînement des arguments qui forment la preuve. Il ne faut pas s'y tromper : la réussite de l'épreuve ne dépend pas seulement du niveau en mathématiques du candidat, mais également de sa capacité à mobiliser efficacement des sources sur lesquelles fonder son travail.

Dans l'optique de servir au mieux les candidats y compris le jour de l'oral, nous avons souhaité proposer un outil pensé pour cette épreuve, regorgeant de références internes. Si chaque développement est autocontenu, les notations et définitions moins habituelles restent toujours rappelées, des chapitres thématiques organisent les différents sujets, une table de correspondances relie leçons et développements, et un index complet des notions abordées permet de retrouver rapidement les passages recherchés.

L'espoir de ce livre. Sans exiger de l'agrégatif qu'il passe une année à naviguer à travers une éclectique bibliographie spécialisée, nous souhaitons partager des résultats que nous trouvons intéressants et enthousiasmants tant sur le plan mathématique que pédagogique, en les regroupant dans un ouvrage qui nous a semblé faire cruellement défaut pendant notre préparation à l'agrégation.

Nombre de livres considérés comme des sources classiques de développements sont soit obsolètes, soit introuvables, soit cantonnés aux rappels de cours, et ne proposent que très peu de développements dans un format directement exploitable pour l'oral. Nous espérons que ce nouvel ouvrage, constitué de 131 développements pensés comme tels, saura suppléer à ce manque et apporter une solution pratique et efficace pour beaucoup d'agrégatifs. Ainsi, chaque leçon du programme actuel de l'agrégation s'y trouve illustrée par au moins trois développements, et souvent davantage. L'informatique n'a pas été oubliée, toutes les leçons étant illustrées par au moins deux développements, de sorte à constituer une référence unique à partir de laquelle préparer un plan de bataille pour les oraux.

Par-delà le public des agrégatifs, le taupin curieux trouvera indubitablement dans ce livre un bon entraînement pour les notions qui le concernent, l'enseignant de premier cycle universitaire en tirera des idées pour faire vivre des concepts de manière originale, et tout amoureux des mathématiques pourra se régaler de ces lectures brèves mais intenses.

Investissement personnel de l'agrégatif. L'existence de ce livre, comme de tout autre recueil de développements que l'on trouverait sur les étals ou sur Internet, ne saurait dispenser l'agrégatif d'un travail fondamental : celui d'appréhender chaque développement de manière consciencieuse et personnelle. C'est également une saine discipline d'apprentissage : les développements proposés mobilisent des mathématiques en tout genre, jetant souvent des ponts entre différents domaines et utilisant des résultats et arguments plus ou moins classiques. Certains lecteurs seront à l'aise avec des arguments qu'ils estimeront même trop détaillés sur tel thème, et devront reconstruire toute la démarche pourtant standard sur tel autre. La préparation à l'agrégation constitue l'occasion parfaite d'orienter ses efforts et d'investir du temps pour comprendre et assimiler les sujets les moins maîtrisés, jusqu'à pouvoir présenter les développements associés avec aisance et conviction. Seule la maîtrise des détails des développements permettra, lors de la préparation de l'épreuve, de retrouver les idées sans encombres et de ne pas devoir redécouvrir les difficultés qui étaient restées cachées.

Nul livre ni professeur ne saurait suppléer à cette quête d'une compréhension profonde et personnelle qui doit être ultimement transmise à l'oral. Il est naturel de passer plusieurs heures à découvrir et à digérer un développement. Comprendre les mathématiques ou savoir faire les calculs ne sont pas les seuls ingrédients pour une présentation claire et convaincante. Nous mettons fortement en garde contre cet écueil et espérons que ce livre sera un juste compagnon en ce sens : une référence qui donnera des idées et des sujets, mais qui n'empêchera pas le lecteur d'adapter la présentation de chaque développement avec ses propres mots et moyens, et l'aidera à affronter ses difficultés de compréhension grâce aux commentaires et aux exercices.

La rédaction de cet ouvrage. Ce livre arrive au terme d'une aventure de nombreuses années. Nous avons souhaité que chaque développement soit finement abouti, calibré en termes de longueur et de difficulté, rédigé de manière limpide et complète, et éclairé de plusieurs commentaires et questions d'approfondissement. Pour cela, chaque développement a été affiné par au moins trois phases de relectures indépendantes par les auteurs ou par des collègues et professeurs extérieurs. Ces échanges, représentant une grande partie du travail de rédaction, ont suscité de nombreuses discussions critiques et constructives qui ont contribué à la richesse et à la qualité du contenu final de l'ouvrage. Cette dialectique a permis de parfaire la rédaction des développements, de clarifier des arguments passés sous silence, d'approfondir certains sujets par des commentaires utiles (parfois susceptibles de constituer des développements à part entière) et d'enrichir l'exposition par des remarques culturelles et heuristiques. Tous ces compléments, nous l'espérons, permettront au lecteur de prendre le recul nécessaire sur les sujets et les méthodes abordés sans avoir à consulter de nombreux autres ouvrages. Nous sommes donc infiniment reconnaissants, pour les nombreuses propositions et discussions qu'ils ont permises, à nos relecteurs et relectrices : Vincent Bansaye, Lilian Besson, Maxence Brévard, Mathias Déhais, Clarence Kineider, Thomas Lévy, Julie Parreaux, Luc Pellissier, François Wawrzyniak et David Xu.

Certains développements ont été rédigés par des contributeurs extérieurs avec le même soin que nous avons passé à rédiger les autres développements ; ce livre ne serait pas complet sans leurs contributions, et nous témoignons donc notre sincère gratitude à Benjamin Dadoun, Julie Gauthier, Marc Pegon, Marcin Pulkowski, Antonin Riffaut et François Wawrzyniak.
Notre reconnaissance va enfin aux soutiens et conseils mathématiques et typographiques de Simon Coste, Benjamin Dadoun et Vojislav Petrov, qui ont permis à ce livre de voir le jour sous une forme bien meilleure qu'elle ne l'aurait été originellement.

Si les efforts et le cœur mis dans la rédaction de cet ouvrage permettent aux lecteurs, agrégatifs et curieux, d'enrichir leur culture et d'embrasser certains sujets d'un regard un peu plus élevé, de trouver des chemins de traverse moins fréquentés pour explorer les mathématiques, ou de rendre la préparation à l'agrégation plus naturelle, efficace et aisée, les années passées à peaufiner ce livre auront été couronnées de succès.
Nous espérons que vous profiterez pleinement de cette année de préparation à l'agrégation et vous souhaitons une belle réussite au concours.

Bon courage et bonne lecture !

Le 12 juin 2020,
à travers le monde,

Pierre Le Barbenchon, Didier Lesesvre,
Pierre Montagnon et Théo Pierron

Organisation de ce livre

Chapitres thématiques. Cet ouvrage a été organisé dans l'optique de faciliter sa consultation. Les développements sont regroupés par chapitres thématiques, qui correspondent essentiellement à la classification des leçons dans le programme. Ce choix d'organisation a été dicté par le thème principal et les méthodes mobilisées. Il ne restreint toutefois pas les développements au thème indiqué : un chapeau plus précis détaille la façon dont chaque sujet s'insère dans les différentes leçons qu'il est susceptible d'illustrer.

Structure des développements. Les développements ont été rédigés sous forme d'exercices, ce qui nous a paru pertinent pour plusieurs raisons. Le découpage en questions permet de donner une vision à plus haut niveau de la structure de la preuve et de l'enchaînement des arguments. Il est primordial pour l'agrégatif qui étudie un développement de trouver un juste milieu entre son apprentissage par cœur et sa relecture complète le jour de l'oral. Présenter le développement sous forme d'exercice permet d'éviter ces extrêmes : le candidat qui prépare le développement pendant l'année est invité à s'appuyer sur ces jalons pour le comprendre, et ces questions fournissent à leur tour un moyen efficace de retrouver la trame du développement lors de l'épreuve. Nous espérons ainsi avoir choisi un mode de présentation pédagogique et pratique, forçant à condenser chaque démonstration en l'enchaînement de quelques étapes clés scandées par les questions.

Chaque développement est suivi de commentaires tantôt mathématiques, tantôt culturels, ou discutant de l'organisation de la présentation au tableau et des variations possibles. Ces commentaires ont été écrits dans l'esprit d'ouverture que nous souhaitons conserver : chacun demeure libre de présenter différemment chaque résultat, par exemple en ne sélectionnant qu'une partie de l'exercice proposé ou en développant plus avant un point abordé en commentaire. Nous ne pouvons qu'encourager ces divergences, qui participent à une présentation plus personnelle et donc plus adaptée.

Enfin, des exercices sont présents à la fin de chaque développement, et représentent des questions qui pourraient être posées par le jury. Notre but est d'aider le lecteur à s'assurer de sa bonne compréhension des détails du raisonnement, notamment lorsque la correction passe un peu rapidement sur un point ou contourne une difficulté dont il est important d'être conscient. Les questions posées invitent donc tantôt à éclaircir un argument classique utilisé dans la preuve, tantôt à en proposer une variation, et parfois, à des fins d'approfondissement, à considérer une question indépendante mais sur le même thème. Nous nous sommes également

efforcés de donner une indication lorsque les arguments nécessaires à la résolution de la question posée nous ont semblé moins immédiats.

Niveau de difficulté. Nous avons déjà souligné que la grande liberté laissée lors des épreuves orales peut — et doit — mener à de nombreuses disparités de niveau quant aux contenus présentés. C'est la raison pour laquelle nous avons choisi de faire figurer un niveau de difficulté indicatif pour chaque développement, entre ★ et ★★★. Un développement de niveau ★ est élémentaire en tout point, dans son objet comme ses arguments, sans être particulièrement long et sans faire intervenir d'astuce ; nous avons par ailleurs fait un effort particulier pour détailler chaque étape du raisonnement dans ce cas. Un développement de niveau ★★★ est plus difficile, souvent à cause d'aspects techniques ou de passages sur lesquels il est nécessaire de passer rapidement pour se concentrer sur le cœur de la preuve, et parfois à cause de prérequis non triviaux ou moins classiques. Ces choix demeurent bien sûr subjectifs, et certains pourraient trouver ardu un développement marqué ★ portant sur des notions avec lesquelles ils sont peu familiers, ou aisé un développement marqué ★★★ et mobilisant des idées et techniques qu'ils maîtrisent déjà.

Par ailleurs, de nombreuses déclinaisons de chaque développement sont possibles : on peut choisir de n'en exposer qu'une partie, de varier le niveau de détails ou, dans certains cas, d'utiliser les commentaires fournis pour présenter une preuve alternative. Ces modulations peuvent changer le niveau de difficulté, et nous incitons le lecteur à consulter des développements sur des sujets ou leçons qui l'intéressent indépendamment du niveau de difficulté indiqué. Ainsi, certains développements indiqués comme étant de niveau ★★★ contiennent des parties autonomes ou admettent des variations de preuves fournies en commentaires qui pourraient constituer un développement ★ ou ★★, et réciproquement. Les choix de rédaction ont été faits pour respecter un équilibre entre les niveaux de difficulté à l'échelle du livre, de sorte que celui-ci puisse proposer à chacun des développements intéressants et adaptés à son niveau. Il fait toutefois partie du travail de chaque agrégatif de juger par lui-même du niveau auquel il souhaite placer sa présentation et de revisiter chaque développement à son gré.

Correspondances entre développements et leçons. L'objectif principal de ce livre demeure de permettre à chaque agrégatif de composer son corpus de développements en fonction de ses préférences et de ses besoins. Chaque leçon du programme doit être illustrée par au moins deux développements que le jury pourra demander d'exposer en détails après la présentation de la leçon. De manière à aider le candidat à faire son choix, comprendre ses possibilités et déterminer les développements les mieux adaptés pour illustrer ses leçons, nous avons présenté des tableaux de correspondance entre développements et leçons à la fin de l'ouvrage. Ainsi, il n'est pas nécessaire de consulter un développement pour retrouver les leçons correspondantes, ni de parcourir tout l'ouvrage pour trouver un développement adapté à une leçon donnée. Enfin, une présentation de cette correspondance a également été fournie sous forme de graphes, permettant une cartographie différente et utile pour choisir ses développements.

Table des matières

Avant-propos **iii**

Liste des notations **xiii**

Développements d'algèbre **1**

Groupes, actions et représentations 3

1. Incertitude de Heisenberg pour les groupes ★ 5
2. Théorème de Dixon ★ 10
3. Générateurs de $\mathrm{SL}_2(\mathbb{Z})$ ★ 14
4. Ensembles de transpositions engendrant $\mathfrak{S}_n$ ★ 18
5. Paires génératrices de sous-groupes de $\mathfrak{S}_n$ ★★ 23
6. Ordre maximum des permutations ★★ 28
7. Commutativité de permutations aléatoires ★★ 35
8. Cyclicité des groupes d'ordre pq ★ 41
9. Groupes d'ordre 105 ★★★ 44
10. Table des caractères des groupes diédraux ★ 49
11. Théorème p^aq^b de Burnside ★★★ 54

Anneaux, corps et théorie des nombres 61

12. Théorème de Cohn ★ 63
13. Lemme de Hensel ★ 69
14. Méthodes polynomiales en combinatoire ★★ 73
15. $\mathbb{C}$ est algébriquement clos ★ 78
16. Lemme d'intersection de Krull ★★ 81
17. Cyclicité de $\mathbb{F}_p^\times$ ★★ 84
18. Automorphismes de $\mathbb{F}_{p^m}$ ★ 89
19. Automorphismes d'un corps cyclotomique ★ 92
20. Automorphismes sauvages de $\mathbb{C}$ ★★★ 96
21. Théorème d'Artin ★★★ 103
22. L'unique entier entre un carré et un cube ★★ 109
23. Valeurs absolues sur $\mathbb{Q}$ ★★ 114
24. Théorème de Fermat et cyclotomie ★★★ 120
25. Problème de Waring modulo q ★★★ 128

Algèbre linéaire 133

26. Perturbation par des matrices de rang un ★ 135
27. Quaternions et isomorphismes ★ 138
28. Lemmes de Schwartz-Zippel et de Kakeya ★★ 147
29. Calculs de polynômes caractéristiques ★ 155
30. Endomorphismes conservant le déterminant ★ 163

31. Endomorphismes conservant le rang ★★ . . . 167
32. Théorème de Chebotarev ★★★ . . . 172
33. Images par l'exponentielle ★★ . . . 178
34. Décomposition polaire ★ . . . 185
35. Réduction des endomorphismes nilpotents ★ . . . 190
36. Décomposition de Dunford ★ . . . 194
37. Forme normale de Smith ★★ . . . 201
38. Sous-algèbres réduites de $\mathcal{M}_n(\mathbb{C})$ ★★ . . . 207
39. Théorème d'Engel ★★★ . . . 212
Formes quadratiques et géométrie . . . 217
40. Billard circulaire ★ . . . 219
41. Le plongeoir le plus long ★★ . . . 225
42. Théorèmes de Helly et de Carathéodory ★ . . . 235
43. Théorème des trois réflexions ★ . . . 239
44. Théorème de Killing-Hopf ★ . . . 243
45. Isométries directes des solides de Platon ★★ . . . 251
46. Théorème d'Hermite ★ . . . 260
47. Formes quadratiques semi-réduites ★★ . . . 264
48. Théorème de Minkowski pour les formes quadratiques ★★★ . . . 268

Développements d'analyse **273**
Analyse fonctionnelle et topologie . . . 275
49. Compacts d'un espace de Hilbert séparable ★★ . . . 277
50. Opérateurs compacts d'un espace de Hilbert ★★ . . . 281
51. Décomposition de Mityagin ★★ . . . 285
52. Une isométrie de $L^2(\mathbb{R}_+)$ non surjective ★★ . . . 290
53. Logarithme et théorème de Brouwer ★★ . . . 296
54. Théorème de Riesz-Fischer ★ . . . 303
Calcul différentiel, équations différentielles et EDP . . . 309
55. Théorème de Cartan-von Neumann ★ . . . 313
56. Théorème de stabilité de Liapounov ★ . . . 318
57. Des extrema liés au consommateur ★★ . . . 323
58. Théorème de Cauchy-Peano ★★ . . . 332
59. Modèle de croissance de Solow-Swan ★ . . . 341
60. Croissance logistique et prédation ★ . . . 347
61. Modèle épidémiologique SIS ★★ . . . 353
62. Modèle épidémiologique SIR ★★ . . . 361
63. Étude qualitative d'une équation de Riccati ★★ . . . 367
64. Modèle de Lotka-Volterra ★★★ . . . 372
65. Équation des ondes pour une corde vibrante ★ . . . 381
66. Caractère bien posé : équation de transport ★★★ . . . 388
67. Dualité contrôlabilité-observabilité ★★★ . . . 396
Analyse classique et complexe . . . 407
68. Une méthode archimédienne pour approcher π ★ . . . 409
69. Convergence d'une suite de polygones ★★ . . . 413

70. Développement en fractions continues ★★ . . . 417
71. Théorèmes de Choquet et de Birkhoff ★★ . . . 423
72. Théorème de Nash ★★ . . . 429
73. Formules de Frenet-Serret ★ . . . 437
74. Méthode de descente de gradient ★ . . . 441
75. Méthode de Gauss-Seidel ★ . . . 445
76. Méthode de relaxation ★ . . . 451
77. Méthode de Kaczmarz ★ . . . 455
78. Prolongement analytique suivant une courbe ★ . . . 461
79. Domaines d'holomorphie à une variable ★★ . . . 464
80. Forme normale de Jordan et résidus ★★★ . . . 469
81. Espace des formes modulaires ★★★ . . . 477
Intégration et approximation de fonctions . . . 485
82. Calcul des intégrales de Fresnel ★ . . . 487
83. Racine carrée de la primitivation ★ . . . 496
84. Méthode de la phase stationnaire ★ . . . 502
85. Théorème de Paley-Wiener ★ . . . 509
86. Théorème de Plancherel ★★ . . . 514
87. Prolongement de la fonction ζ de Riemann ★★ . . . 522
88. Théorème de Fejér-Cesàro ★ . . . 531
89. Théorème de Minkowski pour les réseaux ★★ . . . 539
90. Théorème taubérien de Hardy-Littlewood ★ . . . 545
91. Divergence de l'interpolation de Lagrange ★★ . . . 552
92. Meilleure approximation polynomiale ★★ . . . 557
Probabilités et statistiques . . . 563
93. Aiguille de Buffon ★ . . . 565
94. Paradoxe de Penney ★ . . . 570
95. Formule de Stirling par la limite centrale ★ . . . 580
96. Une marche aléatoire sur $[0, 1]$ ★★ . . . 588
97. Loi forte des grands nombres ★★ . . . 594
98. Théorème de Pólya — version dénombrement ★★ . . . 599
99. Théorème de Pólya — version analytique ★★ . . . 606
100. Un théorème de grandes déviations ★★ . . . 613
101. Théorème de Cramér-Chernoff ★★★ . . . 617

Développements d'informatique **623**
Algorithmique . . . 625
102. Autour du tri rapide ★★ . . . 627
103. Tri par tas ★ . . . 634
104. Distance de Kendall et tri par insertion ★★ . . . 640
105. Tirage aléatoire de population ★★ . . . 644
106. Transformée de Fourier rapide ★★ . . . 651
107. B-arbres ★★ . . . 658
Modèles de calcul . . . 665
108. Complexité du langage des palindromes ★ . . . 683

109. Turing-calculable implique μ-récursive ★★ 687
110. Caractérisation de RE ★★ 692
111. μ-récursive implique λ-définissable ★★ 696
112. Théorème de Scott-Curry ★★ 700
Théorie des graphes 705
113. Polynôme chromatique ★ 717
114. Théorème de Turán ★★ 724
115. Formule d'Euler par déchargement ★★ 731
116. Problème du voyageur de commerce ★ 738
117. Tri topologique ★ 743
118. Séquençage ADN et graphe de De Bruijn ★ 747
Langages réguliers et algébriques 753
119. Recherche de motif ★★ 763
120. Problème de séparation par automate ★ 768
121. Universalité d'un automate ★★ 774
122. Algorithme de Cocke-Younger-Kasami ★ 779
123. Caractérisation de Premier en analyse LL(1) ★★ 783
Logique et preuves 789
124. Théorème de Cook-Levin ★ 791
125. Transformation de Tseitin ★ 797
126. 2Sat est NL-dur ★★ 802
127. Compacité de la logique propositionnelle ★ 807
128. Indécidabilité du problème ValidFO ★★ 812
129. Indécidabilité du problème RelSat ★★★ 817
130. Complétude de la logique de Hoare ★★★ 824
131. Équivalence entre deux sémantiques ★★★ 830

Compléments d'informatique **835**
Schémas algorithmiques 836
Bases de données 839
Sémantiques des langages de programmation 847
Problèmes indécidables 855
Réductions classiques 859
Problèmes NP-complets 863

Annexes **869**
Liste des leçons 871
Correspondances entre leçons et développements 881

Bibliographie **897**

Index **901**

Liste des notations

Ensembles, fonctions et nombres

δ_a	symbole de Kronecker : 1 si a est le neutre et 0 sinon
$\delta_{a=b}$	symbole de Kronecker : 1 si $a = b$ et 0 sinon
Γ	fonction Gamma d'Euler
$[\![m, n]\!]$	ensemble des entiers de m à n
$\mathrm{Im}(z)$	partie imaginaire du nombre complexe z
$\mathbb{K}^*$	ensemble $\mathbb{K}$ privé de l'élément nul
$\lceil \cdot \rceil$	partie entière supérieure
$\lfloor \cdot \rfloor$	partie entière inférieure
$\mathcal{P}_f(E)$	ensemble des parties finies de l'ensemble E
$\mathcal{C}$, $\mathcal{C}^k$, $\mathcal{C}^\infty$	ensemble des fonctions continues, de classe $\mathcal{C}^k$, de classe $\mathcal{C}^\infty$
$\mathcal{F}(X, Y)$	ensemble des fonctions de X dans Y
$\mathbb{1}_X$	fonction caractéristique (ou : indicatrice) de l'ensemble X
argmax f	valeur ou ensemble de valeurs maximisant la fonction f
$\mathrm{pgcd}(p, q)$	plus grand commun diviseur de p et q
$\mathrm{ppcm}(p, q)$	plus petit commun multiple de p et q
$\mathrm{Re}(z)$	partie réelle du nombre complexe z
$\lvert X \rvert$	cardinal de l'ensemble X
ζ	fonction zêta de Riemann
$A \setminus B$	ensemble des éléments de A qui n'appartiennent pas à B
$f \equiv a$	fonction identiquement égale à une constante
$p^k \| n$	puissance de p maximale divisant n, *i.e.* $p^k \mid n$ et $p^{k+1} \nmid n$
S_k	somme de Newton
x^+	partie positive $\max(0, x)$
x^-	partie négative $\max(0, -x)$

Y^X	ensemble des fonctions de X dans Y

Groupes, anneaux, corps

1_G	élément neutre du groupe G (notation multiplicative)
$[E : F]$	degré de l'extension de corps E/F
$[G : H]$	indice de H dans G, *i.e.* nombre de H-classes dans G
$\mathbb{K}^\times$	ensemble des éléments inversibles de $\mathbb{K}$
$\langle \mathcal{F} \rangle$	groupe ou structure engendrée par la famille $\mathcal{F}$
$\mathbb{H}$	algèbre des quaternions de Hamilton
$\mathfrak{g} = \mathrm{Lie}(G)$	algèbre de Lie associée au groupe de Lie G
$\mathfrak{S}_n$	groupe symétrique d'ordre $n!$
$\mathrm{Aut}(E)$	groupe des automorphismes de E (pour la structure considérée)
$\deg P$	degré du polynôme $P \in K[X]$
$\deg_X P(X, Y)$	degré partiel du polynôme $P(X, Y)$ en l'indéterminée X
$\mathrm{Gal}(\mathbb{L}/\mathbb{K})$	groupe de Galois de l'extension $\mathbb{L}/\mathbb{K}$
$\simeq$	isomorphe (pour la structure considérée)
$C_G(x)$	centralisateur de l'élément $x \in G$ dans le groupe G
D_{2n}	groupe diédral d'ordre $2n$
E/F	extension de corps $F \subset E$
$G \cdot x$	orbite de x sous l'action de G
G_x	stabilisateur de x sous l'action de G
$Z(X)$	centre de X, *i.e.* éléments commutant avec tous les autres

Algèbre linéaire

χ_A	polynôme caractéristique de la matrice A
$\mathrm{com}(\cdot)$	comatrice
$\mathcal{A}_n(\mathbb{K})$	espace des matrices antisymétriques de taille n sur $\mathbb{K}$
$\mathcal{D}_n(\mathbb{K})$	espace des matrices diagonales de taille n sur $\mathbb{K}$
$\mathcal{M}_n(\mathbb{K})$	espace des matrices carrées de taille n sur $\mathbb{K}$
$\mathcal{S}_n(\mathbb{K})$	espace des matrices symétriques de $\mathcal{M}_n(\mathbb{K})$
$\mathcal{S}_n^{++}(\mathbb{K})$	ensemble des matrices symétriques définies positives de $\mathcal{M}_n(\mathbb{K})$
$\mathcal{L}(E)$	espace des endomorphismes de E

$\mathcal{L}(E,F)$	espace des applications linéaires de E dans F
$\mathcal{L}_c(E,F)$	espace des opérateurs linéaires continus de E dans F
$\mathrm{diag}(a_1,\ldots)$	matrice diagonale de $\mathcal{M}_n$ d'entrées $a_1,\ldots$
$\mathrm{GL}_n(\mathbb{K})$	groupe des matrices inversibles de taille n sur $\mathbb{K}$
$\mathrm{Sp}(A)$	spectre de la matrice $A \in \mathcal{M}_n(\mathbb{K})$ sur le corps $\mathbb{K}$
$\mathrm{Sp}_{\mathbb{L}}(A)$	spectre de la matrice $A \in \mathcal{M}_n(\mathbb{K})$ sur le corps $\mathbb{L}$
$\mathrm{Vect}(\mathcal{F})$	espace vectoriel engendré par la partie $\mathcal{F}$
μ_A	polynôme minimal de la matrice A
$\rho(u)$, $\rho(A)$	rayon spectral de l'endomorphisme u, de la matrice A
$\mathrm{tr}(\cdot)$	trace
I_n	matrice identité de taille n
$J_{n,r}$	matrice $\mathrm{diag}(1,\ldots,1,0,\ldots,0)$ de taille $n\times n$ et de rang r
u^*, A^*	adjoint de l'opérateur u, de la matrice A
${}^tA$	transposée de la matrice A

Géométrie, formes quadratiques

$\langle\cdot,\cdot\rangle$	produit scalaire
$\mathcal{O}_n(\mathbb{K})$	groupe orthogonal de $\mathcal{M}_n(\mathbb{K})$
$\mathcal{SO}_n(\mathbb{K})$	groupe spécial orthogonal de $\mathcal{M}_n(\mathbb{K})$
$\wedge$	produit vectoriel

Topologie, analyse fonctionnelle

$\asymp, \Theta$	domination dans les deux sens : $f \asymp g$ si $f = O(g)$ et $g = O(f)$
$\mathcal{B}(a,r)$	boule ouverte de centre a et de rayon r
$\mathcal{B}(H)$	espace des opérateurs bornés d'un espace de Hilbert H
$\mathcal{C}_c^\infty(I)$	espace des fonctions de classe $\mathcal{C}^\infty$ sur I et à support compact
$\mathcal{H}$	demi-plan de Poincaré
$\mathcal{K}(H)$	espace des opérateurs compacts d'un espace de Hilbert H
supess	supremum essentiel d'une fonction
$\mathrm{vol}(A)$	volume d'une partie A de $\mathbb{R}^n$ pour la mesure de Lebesgue
ω_f	module de continuité de la fonction f
$\|\|\|T\|\|\|$	norme de l'opérateur linéaire continu T

$\overline{\mathcal{B}}(a,r)$	boule fermée de centre a et de rayon r
∂A	bord topologique de l'ensemble A, soit $\partial A = \overline{A} \backslash A^\circ$
$\star$	opérateur de convolution
$\widehat{f}$	transformée de Fourier de f
$C(a,r)$	cercle de centre a et de rayon r
E'	dual topologique de E
E^*	dual de E
$f = \Omega(g)$	notation Ω de Landau : f/g est bornée
$f = \Theta(g)$	notation Θ de Landau : $f = O(g)$ et $f = \Omega(g)$
$f = O(g)$	notation O de Landau : f/g est bornée
H^1	espace de Sobolev

Calcul différentiel

Δ	opérateur laplacien
$\dot{x}$	dérivée par rapport au temps de la quantité x
$\mathrm{d}f(x)$	différentielle de f en x
∇f	gradient de f en x
$Df(x)$	matrice jacobienne de f en x

Probabilités, statistiques

$\mathbb{E}(X)$	espérance de la variable aléatoire X
$\Gamma(k,\theta)$	loi Gamma de paramètres k et θ
$\mathcal{B}(n,p)$	loi binomiale de paramètres n et p
$\mathcal{B}(p) = \mathcal{B}(1,p)$	loi de Bernoulli de paramètre p
$\mathcal{E}(\lambda)$	loi exponentielle de paramètre λ
$\mathcal{G}(p)$	loi géométrique (sur $\mathbb{N}^*$) de paramètre p
$\mathcal{N}(\mu,\sigma^2)$	loi normale d'espérance μ et de variance σ^2
$\mathcal{P}(\lambda)$	loi de Poisson de paramètre λ
$\mathrm{Cov}(X,Y)$	covariance des variables aléatoires X et Y
$\mathbb{P}$	mesure de probabilité
$\mathbb{P}(A\|B)$	probabilité de A sachant B
$\xrightarrow[n\to+\infty]{\mathcal{L}}$	convergence en loi

$\xrightarrow[n\to+\infty]{\mathbb{P}}$	convergence en probabilité
$\xrightarrow[n\to+\infty]{\text{p.s.}}$	convergence presque sûre
L^p	ensemble des variables aléatoires admettant un moment d'ordre p

Théorie des graphes

$\ell(f)$	longueur de la face f dans un graphe planaire
$\overline{G}$	complémentaire du graphe G
$\mathbb{V}(X)$	variance de la variable aléatoire X
C_n	cycle à n sommets
$d_G(u)$	degré du sommet u dans le graphe G
$d_G^+(u)$	degré sortant du sommet u dans le graphe G
$d_G^-(u)$	degré entrant du sommet u dans le graphe G
$G - s$	suppression du sommet s dans le graphe G
$G - st$	suppression de l'arête ou arc st dans le graphe G
$G \cdot st$	identification des sommets s et t dans le graphe G
K_n	clique à n sommets
$N_G^+(u)$	voisinage sortant du sommet u dans le graphe G
$N_G^-(u)$	voisinage entrant du sommet u dans le graphe G
$N_G(u)$	voisinage du sommet u dans le graphe G
P_n	chemin à n sommets
uv	arête ou arc d'un graphe entre les sommets u et v

Logique, calculabilité, complexité

$[\ell_0, \ldots, \ell_{n-1}]$	liste (simplement chaînée) de longueur n
$\bot$	faux
$\ell :: L$	liste obtenue en ajoutant l'élément ℓ en tête de la liste L
$[\![t_0, \ldots, t_{n-1}]\!]$	tableau de longueur n
$\mathrm{L}(\mathcal{A})$	langage engendré par l'automate $\mathcal{A}$
$\mathrm{L}(G)$	langage engendré par la grammaire algébrique G
$\top$	vrai
$\lvert w\rvert$	longueur du mot w
$S \to aSb \mid \varepsilon$	règles de dérivation d'une grammaire algébrique
$T_{\mathcal{M}}$	complexité temporelle de la machine de Turing $\mathcal{M}$
$x := a$, $x \leftarrow a$	affectation de la valeur a à la variable x

Développements d'algèbre

Groupes, actions et représentations

Les prémices de la théorie des groupes remontent aux travaux de Lagrange autour de 1770 ; motivé par l'étude des racines d'équations polynomiales, il expose un *calcul des combinaisons* qui n'est autre que la loi de composition pour le groupe symétrique $\mathfrak{S}_n$. Le groupe symétrique demeure un exemple omniprésent et très riche de groupe (Développements 4, 5, 6, 7). C'est Galois qui, quelques décennies plus tard, introduit explicitement le terme de *groupe*, toujours dans le cadre des équations polynomiales. La première étude systématique de la structure de groupe est due à Cayley, en 1854 mais il faudra attendre la fin du XIX$^{\text{e}}$ siècle pour voir l'essor de la théorie des groupes.

Un groupe est une structure algébrique munie d'une opération binaire vérifiant de « bonnes propriétés ». Il peut être intuitivement pensé comme un ensemble de *mouvements* qui offre la possibilité de se déplacer de manière naturelle (en faisant un mouvement après l'autre : la loi est interne et associative), de demeurer au même point (existence d'un élément neutre) et de revenir en arrière (chaque élément admet un inverse). Cela donne une structure qui modélise de nombreux problèmes : Galois s'intéresse aux groupes de permutations de racines, Klein aux groupes d'isométries (Dév. 45) dans sa vision nouvelle de la géométrie, Kummer introduit le groupe des classes d'idéaux pour mieux comprendre les équations diophantiennes, les physiciens utilisent les groupes de symétries des molécules...

L'étude théorique des groupes, domaine immense et encore très actif, s'épanouit dans de nombreuses directions. Classifier ne serait-ce que les groupes finis fut l'une des grandes quêtes mathématiques du XX$^{\text{e}}$ siècle, et tout un univers s'ouvre des groupes discrets aux groupes continus, en passant par les groupes topologiques ou différentiels. Quelle que soit la particularité des groupes considérés, l'étude des groupes s'appuie sur la notion de quotient, permettant de « dévisser » les groupes pour les ramener à l'étude de groupes plus petits, idée particulièrement utile une fois combinée aux théorèmes de Sylow (Dév. 8, 9).

Plutôt qu'étudier les éléments d'un groupe, il est souvent plus riche de le faire agir sur d'autres espaces ou sur lui-même. C'est le principe à l'origine de la théorie des actions de groupes, qui permet de réaliser un groupe comme un ensemble de mouvements, autrement dit (dans le cas des actions linéaires en dimension finie) comme un groupe de matrices. La théorie des représentations (Dév. 10, 11) est donc un moyen de donner corps à des groupes abstraits dans le cadre de l'algèbre linéaire, plus concrète et familière, et d'en tirer de nombreux résultats sur les groupes. De manière analogue, laisser un groupe connu agir sur un ensemble permet souvent d'obtenir des informations sur ce dernier.

Développement 1 (Incertitude de Heisenberg pour les groupes ★)

a) Soit G un groupe abélien fini d'ordre n, et $\widehat{G}$ son groupe dual. Soit f une fonction dans $\mathcal{F}(G, \mathbb{C})$. On introduit sa transformée de Fourier définie par

$$\forall \chi \in \widehat{G}, \qquad \widehat{f}(\chi) = \frac{1}{n} \sum_{a \in G} f(a)\overline{\chi}(a).$$

(*i*) Pour $a \in G$, notons δ_a la fonction sur G valant 1 en a et 0 ailleurs. Montrer que

$$\forall a \in G, \qquad \sum_{\chi \in \widehat{G}} \chi(a) = n\delta_a.$$

(*ii*) Montrer la relation d'orthogonalité des caractères,

$$\forall a, b \in G, \qquad \sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi}(b) = n\delta_{a,b}.$$

(*iii*) En déduire la formule d'inversion de Fourier,

$$\forall a \in G, \qquad f(a) = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(a).$$

b) (*i*) Montrer la majoration

$$\forall a \in G, \qquad |f(a)| \leqslant \sum_{\chi \in \widehat{G}} \left|\widehat{f}(\chi)\right|.$$

(*ii*) Notons $\operatorname{supp} f$ le support de f, c'est-à-dire l'ensemble des $a \in G$ tels que $f(a) \neq 0$. Montrer qu'il existe un $M > 0$ tel que

$$\forall \chi \in \widehat{G}, \qquad \left|\widehat{f}(\chi)\right| \leqslant \frac{M}{n} |\operatorname{supp} f|.$$

(*iii*) En déduire le principe d'incertitude de Heisenberg pour les groupes :

$$|\operatorname{supp} f| \cdot |\operatorname{supp} \widehat{f}| \geqslant n.$$

Leçons concernées : 104, 107, 246

Ce développement est un résultat important sur les groupes abéliens finis (104), exploitant fortement la dualité dans les groupes abéliens pour décomposer toute fonction dans la base formée des caractères additifs (107) du groupe. Les idées maîtresses sont celles de l'analyse harmonique abélienne, qui en cela est parallèle à celle des séries de Fourier (246) et peut être utilisée pour illustrer une généralisation de la leçon concernée si une partie du plan est dédiée à l'analyse harmonique abélienne au-delà de $\mathbb{R}/\mathbb{Z}$, comme expliqué dans les commentaires.

Correction.

a) (*i*) Soit $a \in G$. Si $a = 0$, on a bien

$$\sum_{\chi \in \widehat{G}} \chi(a) = \sum_{\chi \in \widehat{G}} 1 = n.$$

Si $a \neq 0$, alors il existe $\chi' \in \widehat{G}$ tel que $\chi'(a) \neq 1$. Or l'application $\chi \mapsto \chi'\chi$ est une bijection de $\widehat{G}$ dans lui-même, elle peut donc servir de changement de variable. On obtient dans ce cas

$$\sum_{\chi \in \widehat{G}} \chi(a) = \sum_{\chi \in \widehat{G}} (\chi'\chi)(a) = \chi'(a) \sum_{\chi \in \widehat{G}} \chi(a).$$

Puisque $\chi'(a)$ est non trivial, cela implique que

$$\sum_{\chi \in \widehat{G}} \chi(a) = 0.$$

(*ii*) Soit $\chi \in \widehat{G}$. Puisque les caractères sont unitaires, $\overline{\chi}$ est l'inverse de χ, et en particulier par multiplicativité on a $\chi(a)\overline{\chi}(b) = \chi(a-b)$ pour tous $a, b \in G$. Il vient donc par ce qui précède, en remplaçant a par $a - b$,

$$\sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi}(b) = n\delta_{a,b}.$$

(*iii*) La formule d'inversion de Fourier découle de l'orthogonalité des caractères, montrée à la question précédente, qui s'écrit pour tous a et b dans G,

$$\frac{1}{n} \sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi}(b) = \delta_{a,b}.$$

On calcule alors, pour tout $x \in G$,

$$\begin{aligned}
\sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi(x) &= \sum_{\chi \in \widehat{G}} \left(\frac{1}{n} \sum_{a \in G} f(a)\overline{\chi}(a) \right) \chi(x) \\
&= \frac{1}{n} \sum_{a \in G} f(a) \sum_{\chi \in \widehat{G}} \overline{\chi}(a)\chi(x) \\
&= \sum_{a \in G} f(a) \left(\frac{1}{n} \sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi}(a) \right) \\
&= \sum_{a \in G} f(a)\delta_{a,x} \\
&= f(x).
\end{aligned}$$

b) (*i*) Par la formule d'inversion de Fourier obtenue à la question **a)**(*iii*) et le fait que les caractères sont unitaires, on a

$$|f(a)| \leqslant \sum_{\chi \in \widehat{G}} \left|\widehat{f}(\chi)\right| \tag{1}$$

(*ii*) En remplaçant $\widehat{f}(\chi)$ par sa définition, il vient

$$\left|\widehat{f}(\chi)\right| \leqslant \frac{1}{n} \sum_{a \in G} |f(a)\overline{\chi}(a)| = \frac{1}{n} \sum_{a \in G} |f(a)|.$$

En majorant brutalement chaque terme de la somme par le maximum M de f, qui est bien défini car G est fini, on en déduit que pour tout $\chi \in \widehat{G}$,

$$\left|\widehat{f}(\chi)\right| \leqslant \frac{M}{n} |\text{supp } f|.$$

(*iii*) En introduisant la majoration précédente dans (1), il vient

$$|f(a)| \leqslant \sum_{\substack{\chi \in \widehat{G} \\ \widehat{f}(\chi) \neq 0}} \frac{M}{n} |\text{supp } f| = \frac{M}{n} |\text{supp } \widehat{f}| \cdot |\text{supp } f|.$$

En particulier, puisque le groupe est fini, il existe un certain $a_0 \in G$ pour lequel on a $|f(a_0)| = M$, on tire alors de l'inégalité précédente que

$$M = |f(a_0)| \leqslant \frac{M}{n} |\text{supp } \widehat{f}| \cdot |\text{supp } f|,$$

et $M \geqslant f(0) = 1$ est non nul. On en déduit le principe d'incertitude de Heisenberg

$$|\text{supp } f| \cdot |\text{supp } \widehat{f}| \geqslant n.$$

Commentaires.

♦ Ce développement propose de prouver le principe d'incertitude de Heisenberg pour les groupes abéliens finis. Il s'agit de la généralisation du principe analogue pour les fonctions périodiques, et un principe général en analyse de Fourier : plus on souhaite localiser une fonction, plus il faut être prêt à concéder de pertes sur la localisation de sa transformée de Fourier. Il s'agit bien du principe d'incertitude de la physique quantique, qui énonce qu'il n'est pas possible de connaître simultanément la position et le moment d'une particule avec une précision arbitraire. La transformation de Fourier fournit un moyen de passer du formalisme des positions au formalisme des moments, et le principe d'incertitude formulé dans ce développement souligne qu'il n'est pas possible de sélectionner très précisément les deux informations.

♦ On se réfère parfois aux « carrés de Heisenberg » pour parler de ce principe d'incertitude. Géométriquement, en se plaçant dans l'espace des phases $G \times \widehat{G}$, le résultat obtenu stipule que le produit des supports recouvre un rectangle d'aire au moins n.

♦ Une situation élémentaire à garder en tête est celle des gaussiennes. Sans donner de normalisation précise pour la transformée de Fourier d'une fonction sur $\mathbb{R}$ et en ignorant les constantes, on a la dualité

$$f(x) \simeq e^{-\alpha^2 x^2} \quad \text{et} \quad \widehat{f}(x) \simeq e^{-x^2/\alpha^2},$$

de sorte que si le support (essentiel) de f est de mesure $1/\alpha$, alors le support (essentiel) de f est de mesure α. L'heuristique demeure ainsi plus généralement : une fonction et sa transformée de Fourier ne peuvent être toutes deux arbitrairement concentrées autour d'un point. Pour des versions quantitatives de tels résultats, on pourra se référer au Développement 85 sur les théorèmes de Paley-Wiener.

♦ Les arguments utilisés ici sont ceux de l'analyse harmonique sur les groupes. L'idée principale est que l'analyse de Fourier, qui n'est qu'une décomposition suivant les caractères du groupe $\mathbb{R}/\mathbb{Z}$, se généralise à bien des groupes abéliens, notamment les groupes finis et les groupes topologiques compacts. Les fruits de l'analyse harmonique en découlent alors de la même manière. Les idées ne sont en rien plus difficiles que l'analyse de Fourier classique, une fois que les caractères additifs $\exp(2i\pi n\cdot)$ du tore $\mathbb{R}/\mathbb{Z}$ sont remplacés par ceux de G.

♦ Explicitons la formule de Poisson pour illustrer le commentaire précédent. Soit f une fonction sur G à valeurs complexes. Pour un sous-groupe H de G, on définit

$$H^\perp = \left\{\chi \in \widehat{G} \ : \ \chi_{|H} = 1\right\}.$$

On a alors la formule

$$\sum_{h\in H} f(h) = \frac{1}{|G/H|} \sum_{\chi\in H^\perp} \widehat{f}(\chi). \tag{2}$$

À condition de remplacer les sommes par des intégrales contre une bonne mesure de Haar et les cardinaux par des volumes, on arrive à une formule similaire pour tout groupe abélien topologique. Dans le cas de $G = \mathbb{R}$ et $H = \mathbb{Z}$, on retrouve la forme de Poisson classique. En effet, le tore $\mathbb{R}/\mathbb{Z}$ est alors de volume 1 et les caractères de $\mathbb{R}$ (qui sont les exponentielles $x \mapsto \exp(\lambda x)$ avec $\lambda \in \mathbb{C}$) qui sont triviaux sur $\mathbb{Z}$ sont les $x \mapsto \exp(2i\pi nx)$. La formule précédente s'écrit alors

$$\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \int_{\mathbb{R}} f(\lambda) e^{2i\pi nx} \mathrm{d}x = \sum_{n\in\mathbb{Z}} \widehat{f}(n).$$

♦ La formule de Poisson est parfois considérée à tort comme une curiosité à l'utilité douteuse. La formulation (2) montre qu'elle entrelace les propriétés de f sur H et de $\widehat{f}$ sur $H^\perp$, montrant qu'il s'agit essentiellement du même phénomène que le principe d'incertitude. La relation qu'elle tisse entre différents mondes « duaux » en fait l'un des outils les plus puissants en analyse harmonique et en théorie des nombres. Elle contient en essence le théorème de Riemann-Roch en géométrie algébrique, l'équation fonctionnelle de la fonction ζ de Riemann en théorie des nombres, ou encore de nombreux liens insoupçonnés entre géométrie d'une surface et théorie spectrale des opérateurs associés. On pourra se référer au Développement 89 pour en voir une belle application géométrique.

♦ Ce formalisme éclaire la transformée de Fourier rapide (voir Développement 106), qui est une illustration de l'analyse harmonique sur les groupes abéliens finis.

Questions.

1. Expliquer pourquoi les $\chi(a)$, pour $a \in G$, sont des racines de l'unité.
2. Soit $a \neq 0$ dans G. Montrer qu'il existe $\chi \in \widehat{G}$ tel que $\chi(a) \neq 1$.

Indication : penser à définir le caractère χ sur le groupe cyclique $\langle a \rangle$ (on pourra penser au cas des racines n-ièmes de l'unité), puis l'étendre trivialement à G.

3. Rappeler pourquoi G et $\widehat{G}$ ont le même cardinal.
4. Si $y \neq 1$, montrer que la translation $x \in G \mapsto xy$ est une bijection de G.
5. Définissons la convolution de deux fonctions f et g sur G par

$$\forall a \in G, \qquad (f \star g)(a) = \frac{1}{n} \sum_{b \in G} f(b) g(a-b).$$

Montrer que $\widehat{f \star g} = \widehat{f} \cdot \widehat{g}$.

6. Soient deux groupes abéliens finis G et H. Montrer que $\widehat{G \times H} = \widehat{G} \times \widehat{H}$.
7. Déduire des relations d'orthogonalité pour les caractères prouvées dans le développement le théorème de Plancherel pour les groupes abéliens finis :

$$\sum_{a \in G} |f(a)|^2 = \frac{1}{n} \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2.$$

8. Prouver la formule de Poisson (2) mentionnée en commentaires.

Indication : on peut commencer par s'inspirer de la preuve classique de la formule de Poisson pour $\mathbb{R}/\mathbb{Z}$, en introduisant la fonction moyennée sur H définie par, pour tout $x \in G$,

$$F(x) = \sum_{h \in H} f(xh).$$

Cette fonction est alors H-périodique et définit donc une fonction sur G/H. On peut alors obtenir la formule, pour tout $x \in G$,

$$\sum_{h \in H} f(xh) = \frac{1}{|G/H|} \sum_{\chi \in H^\perp} \widehat{f}(\chi) \chi(x),$$

et il suffit de prendre $x = 1$ pour obtenir la formule de Poisson. Il est aussi possible de vérifier directement la formule ci-avant en développant et en utilisant les relations d'orthogonalité, comme dans le développement.

Développement 2 (Théorème de Dixon ★)

Soit G un groupe fini non abélien.

a) Soit $Z(G)$ le centre de G. Montrer que $[G : Z(G)] \geqslant 4$.

b) Montrer que la probabilité $p(G)$ pour que deux éléments de G tirés uniformément et indépendamment commutent est majorée par $5/8$.

c) On note D_8 le groupe diédral à 8 éléments. Montrer que $p(D_8) = 5/8$.

Leçons concernées : 103, 104, 106, 160, 161, 190

*Le théorème de Dixon démontré dans cet exercice est un résultat surprenant de théorie des groupes finis, ce qui le rend tout à fait adapté à la leçon 104. Sa preuve consiste à établir une inégalité en apparence grossière en utilisant une minoration de l'indice du centre d'un groupe non abélien, qui s'avère optimale puisque l'égalité est réalisée dans le cas du groupe diédral D_8. L'étude précise de ce dernier justifie l'utilisation de ce développement comme une illustration (facile) des leçons sur les isométries (106, 160 et 161). On peut enfin envisager de présenter ce développement dans le cadre de la leçon sur les groupes quotient et les groupes distingués (103), en remplaçant la preuve de la question **a)** ci-après par celle donnée en commentaire. Enfin, le calcul de la probabilité recherchée passe par un dénombrement explicite des éléments commutant dans le groupe diédral, en faisant une bonne illustration pour la leçon de combinatoire (190).*

Correction.
On rappelle que pour tout $x \in G$, on note

$$C_x = \{g \in G : gx = xg\}$$

le centralisateur de x dans G.

a) Comme G n'est pas abélien, il existe un élément $x \in G$ dont le centralisateur C_x n'est pas égal à G tout entier, et donc tel que l'indice $[G : C_x]$ de C_x dans G est au moins égal à 2. Par ailleurs, le centre $Z(G)$ de G est un sous-groupe de C_x, qui n'est pas égal à C_x puisqu'il ne contient pas x. Par conséquent, $[C_x : Z(G)]$ est lui aussi au moins égal à 2, d'où, par multiplicativité des indices,

$$[G : Z(G)] = [G : C_x] \cdot [C_x : Z(G)] \geqslant 4.$$

b) Par définition de la probabilité $p(G)$, on a

$$\begin{aligned} p(G) &= \frac{1}{|G|^2} \left| \left\{ (x, y) \in G^2 : xy = yx \right\} \right| \\ &= \frac{1}{|G|^2} \sum_{x \in G} |\{y \in G : xy = yx\}| \\ &= \frac{1}{|G|^2} \sum_{x \in G} |C_x| \,. \end{aligned}$$

Notons que $x \in Z(G)$ si et seulement si $C_x = G$, de sorte que $x \notin Z(G)$ implique que $[G : C_x] \geqslant 2$, autrement dit $|C_x| \leqslant \frac{1}{2}|G|$. En séparant la somme ci-avant entre éléments du centre et éléments hors du centre, il vient

$$\begin{aligned} p(G) &= \frac{1}{|G|^2}\left(\sum_{x\in Z(G)} |C_x| + \sum_{x\in G\setminus Z(G)} |C_x|\right) \\ &= \frac{1}{|G|^2}\left(\sum_{x\in Z(G)} |G| + \sum_{x\in G\setminus Z(G)} |C_x|\right) \\ &\leqslant \frac{1}{|G|^2}\left(\sum_{x\in Z(G)} |G| + \sum_{x\in G\setminus Z(G)} \frac{|G|}{2}\right). \end{aligned}$$

De plus, la question **a)** garantit que $[G : Z(G)] \geqslant 4$, ce qui se traduit par le fait que $|Z(G)| \leqslant \frac{1}{4}|G|$. On obtient donc comme voulu

$$p(G) \leqslant \frac{1}{|G|^2}\left(\frac{|G|}{4}|G| + \left(|G| - \frac{|G|}{4}\right)\frac{|G|}{2}\right) = \frac{5}{8}.$$

c) Le groupe diédral D_8 est composé de quatre rotations (d'angles 0, $\pi/2$, π et $3\pi/2$) et de quatre réflexions. Déterminons les couples d'éléments de D_8 qui commutent :

- Une rotation de D_8 commute avec toute autre rotation de D_8.
- Si $s \in D_8$ est la réflexion d'axe Δ et si $s' \in D_8$ est la réflexion d'axe Δ', alors $s \circ s'$ est une isométrie directe de D_8 donc une rotation, et son angle est le double de l'angle orienté (Δ', Δ) modulo 2π. Comme $s' \circ s = (s \circ s')^{-1}$ (puisque s et s' sont des involutions), $s' \circ s$ est la rotation d'angle le double de l'angle orienté (Δ, Δ') modulo 2π. Ainsi, s' et s commutent si et seulement si

  $$2(\Delta, \Delta') \equiv 2(\Delta', \Delta) \mod 2\pi,$$

  c'est-à-dire

  $$4(\Delta, \Delta') \equiv 0 \mod 2\pi,$$

  soit

  $$(\Delta, \Delta') \equiv 0 \mod \pi/2.$$

  Une réflexion $s \in D_8$ d'axe Δ commute donc avec elle-même et avec la réflexion dont l'axe est $\Delta^\perp$, mais pas avec les autres réflexions.
- Si s est une réflexion de D_8 d'axe Δ et r une rotation de D_8, voyons à quelle condition elles commutent. L'isométrie $r \circ s \circ r^{-1} \in D_8$ est de déterminant -1, donc c'est une réflexion. De plus, on voit facilement qu'elle préserve la droite $r(\Delta)$, et donc qu'elle est d'axe $r(\Delta)$. Si s et r commutent, alors $r \circ s \circ r^{-1} = s$, donc $r(\Delta) = \Delta$; r est donc l'identité ou la rotation d'angle π, c'est-à-dire $-\mathrm{Id}$. Réciproquement, il est clair que Id et $-\mathrm{Id}$ commutent avec toutes les réflexions de D_8.

Puisque D_8 est composé de 8 éléments, il y a 64 couples dans $(D_8)^2$. Décomptons ceux qui commutent en les distinguant selon leur premier élément, en utilisant la discussion précédente pour conclure dans chaque cas :

- Id et $-\mathrm{Id}$ commutent avec tous les éléments de D_8. Il y a donc $2 \times 8 = 16$ couples d'éléments commutants de D_8 dont le premier élément est Id et $-\mathrm{Id}$.
- Les deux rotations autres que Id et $-\mathrm{Id}$ commutent avec les rotations uniquement (donc avec quatre éléments), ce qui correspond à $2 \times 4 = 8$ couples.
- Les quatre réflexions commutent chacune avec deux réflexions et deux rotations (donc avec quatre éléments), ce qui correspond à $4 \times 4 = 16$ couples.

Il vient donc :

$$p(G) = \frac{16 + 8 + 16}{64} = \frac{40}{64} = \frac{5}{8},$$

ce qu'il fallait établir.

Commentaires.

♦ On peut proposer une autre preuve du résultat de la question **a)**. Puisque G n'est pas abélien, $Z(G)$ est d'indice au moins 2. Si cet indice était égal à 2 ou 3, alors $G/Z(G)$ serait cyclique en tant que groupe de cardinal 2 ou 3. Mais alors G serait abélien : en effet, en notant $aZ(G) \in G/Z(G)$ un générateur de $G/Z(G)$ on aurait pour tous x et y dans G l'existence de m et n entiers tels que $x \in a^n Z(G)$ et $y \in a^m Z(G)$, et donc de z_1 et z_2 dans $Z(G)$ tels que $x = a^n z_1$ et $y = a^m z_2$. On aurait alors

$$xy = a^n z_1 a^m z_2 = a^n a^m z_1 z_2 = a^m a^n z_2 z_1 = a^m z_2 a^n z_1 = yx$$

puisque $z_1, z_2 \in Z(G)$. Ainsi, l'indice de $Z(G)$ est nécessairement supérieur ou égal à 4.

♦ Le théorème de Dixon donne une majoration de la probabilité $p(G)$. On voit dans le Développement 7 qu'il est impossible de minorer $p(G)$ par un réel strictement positif indépendamment du cardinal de G puisque $\lim_{n\to+\infty} p(\mathfrak{S}_n) = 0$.

Questions.

1. Démontrer que le centralisateur d'un élément x de G ainsi que le centre $Z(G)$ de G sont des sous-groupes de G.
2. Montrer que si $G/Z(G)$ est abélien, alors G est abélien.
3. Montrer que si H est un sous-groupe de G et si K est un sous-groupe de H,

$$[G : K] = [G : H] \cdot [H : K].$$

4. Justifier la majoration

$$\sum_{x \in Z(G)} |G| + \sum_{x \in G \setminus Z(G)} \frac{|G|}{2} \leqslant \frac{|G|}{4}|G| + \left(|G| - \frac{|G|}{4}\right)\frac{|G|}{2}$$

dans le premier calcul de la question **b)**.

Indication : raisonner en termes de combinaisons convexes de $\frac{|G|}{2}$ et de $|G|$.