JEAN-ÉTIENNE ROMBALDI

Leçons d'oral pour l'agrégation de mathématiques

Première épreuve : les exposés

AGRÉGATION INTERNE
MATHÉMATIQUES

- Algèbre, géométrie, analyse et probabilités
- Les 48 leçons incontournables
- Des questions type de jury

deboeck SUPÉRIEUR

JEAN-ÉTIENNE ROMBALDI

Leçons d'oral pour l'agrégation de mathématiques

Première épreuve : les exposés

deboeck SUPÉRIEUR

Ouvrage complémentaire (épreuve orale)
Rombaldi J.-É., *Leçons d'oral pour l'agrégation de mathématiques. Seconde épreuve : les exercices*

Ouvrages complémentaires (épreuve écrite)
Dantzer J.-F., *Mathématiques pour l'agrégation. Analyse et probabilités*
Rombaldi J.-É., *Mathématiques pour l'agrégation. Algèbre et géométrie*
Rombaldi J.-É., *Exercices et problèmes corrigés pour l'agrégation de mathématiques*

Chez le même éditeur (extrait du catalogue)
Aebischer B., *Introduction à l'analyse*
Aebischer B., *Analyse. Fonctions à plusieurs variables et géométrie analytique*
Aebischer B., *Géométrie. Géométrie affine, géométrie euclidienne et introduction à la géométrie projective*
Aslangul C., *Des mathématiques pour les sciences. Corrigés détaillés et commentés des exercices et problèmes*
Belhaj S., *Mathématiques pour l'économie et la gestion*
Belhaj S., Ben Aissa A., *Mathématiques pour l'informatique*
Briane M., Pagès G., *Analyse. Théorie de l'intégration* – 7e édition
Burg P., Mathématiques. *Les fondamentaux en Licence 1*
Canon É., *Analyse numérique*
Carassus L., Pagès G., *Finance de marché. Modèles mathématiques à temps discret*
Carton O., *Langages formels. Calculabilité et complexité*
Choulli M., *Analyse fonctionnelle. Équations aux dérivées partielles*
Commenges D., Jacqmin-Gadda H., *Modèles bio statistiques pour l'épidémiologie*
Cortella A., *Algèbre. Théorie des groupes*
Cottet-Emard F., *36 problèmes corrigés pour le CAPES de mathématiques*
Cottet-Emard F., *Probabilités et tests d'hypothèses*
Cottet-Emard F., *Algèbre linéaire et bilinéaire*
Cottet-Emard F., *Analyse*
Depauw J., *Statistiques*
Mansuy R., Mneimné R., *Algèbre linéaire. Réduction des endomorphismes*
Pagès G., *101 quizz qui banquent. Mathématiques et finances sont-elles indépendantes ?*
Stoltz G., Rivoirard V., *Statistique mathématique en action*
Wassef P., *Algèbre. Arithmétique pour l'informatique*

Pour toute information sur notre fonds et les nouveautés dans votre domaine de spécialisation, consultez notre site web :
www.deboecksuperieur.com

En couverture : Coupe d'un nautile © AdrianHancu/Getty Images
Maquette & mise en pages de l'auteur
Maquette de couverture : Primo&Primo
Couverture : SCM, Toulouse

Dépôt légal :
Bibliothèque royale de Belgique : 2019/13647/069
Bibliothèque nationale, Paris : juin 2019
ISBN : 978-2-8073-2153-3

Tous droits réservés pour tous pays.
Il est interdit, sauf accord préalable et écrit de l'éditeur, de reproduire (notamment par photocopie) partiellement ou totalement le présent ouvrage, de le stocker dans une banque de données ou de le communiquer au public, sous quelque forme ou de quelque manière que ce soit.

© De Boeck Supérieur SA, 2018 - Rue du Bosquet 7, B1348 Louvain-la-Neuve
De Boeck Supérieur - 5 allée de la 2e DB, 75015 Paris

Sommaire

Avant-propos **xv**

I Leçons d'algèbre et de géométrie **1**

1 Groupes monogènes, groupes cycliques. Exemples **3**

2 Groupe opérant sur un ensemble. Exemples et applications **9**

3 Permutations d'un ensemble fini, groupe symétrique. Applications **19**

4 Nombres complexes de module 1. Racines de l'unité **29**

5 Utilisation de groupes en géométrie **39**

6 Idéaux d'un anneau commutatif. Exemples **49**

7 Anneaux $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Applications **59**

8 Nombres premiers **69**

9 pgcd dans $\mathbb{Z}$ et $\mathbb{K}[X]$ **79**

10 Polynômes à une indéterminée à coefficients réels ou complexes **91**

11 Polynômes d'endomorphismes en dimension finie. Applications **101**

12 Réduction d'un endomorphisme en dimension finie **113**

13 Endomorphismes symétriques d'un espace vectoriel euclidien. Applications **121**

14 Matrices symétriques réelles **127**

15 Groupe orthogonal d'un espace euclidien de dimension 2, ou 3 **133**

16 Notion de rang en algèbre linéaire et bilinéaire. Applications **143**

17 Formes linéaires, hyperplans, dualité **153**

18 Opérations élémentaires sur les lignes ou les colonnes d'une matrice **161**

19 Valeurs propres. Recherche et utilisation **173**

20 Formes quadratiques sur un espace vectoriel réel de dimension finie **183**

21 Utilisation des nombres complexes en géométrie **193**

22 Barycentres. Applications **207**

23 Coniques **215**

24 Droites et cercles dans le plan affine euclidien **227**

II Leçons d'analyse et de probabilité 241

25 Espaces vectoriels normés de dimension finie 243

26 Suites dans un espace vectoriel normé de dimension finie 251

27 Diverses notions de convergence en analyse et en probabilités. Exemples 261

28 Séries à termes réels positifs. Applications 273

29 Séries à termes réels ou complexes. Convergence absolue, semi-convergence 281

30 Comparaison d'une série et d'une intégrale. Applications 293

31 Séries de fonctions. Propriétés de la somme, exemples 303

32 Séries entières. Rayon de convergence. Propriétés de la somme. Exemples 313

33 Série de Fourier d'une fonction périodique ; propriétés. Exemples 321

34 Exponentielle complexe 331

35 Exponentielles de matrices. Applications 339

36 Intégrale d'une fonction dépendant d'un paramètre 349

37 La fonction gamma 359

38 Théorème des valeurs intermédiaires. Applications 369

39 Théorèmes des accroissements finis 377

40 Formules de Taylor pour une fonction d'une variable réelle 387

41 Fonctions convexes d'une variable réelle. Applications 395

42 Fonctions de plusieurs variables : dérivées partielles, différentiabilité 405

43 Méthodes de calcul approché d'une intégrale 421

44 Espaces préhilbertiens 433

45 Équations différentielles linéaires d'ordre deux 447

46 Systèmes différentiels linéaires à coefficients constants 459

47 Inégalités en analyse et en probabilités 467

48 Étude métrique des courbes planes 477

Bibliographie 489

Index 491

Table des matières

Avant-propos ..... **xv**

I Leçons d'algèbre et de géométrie **1**

1 Groupes monogènes, groupes cycliques. Exemples **3**
1.1 Groupes monogènes, groupes cycliques 3
1.2 Sous-groupes d'un groupe monogène 5
1.3 Théorème de structure des groupes abéliens finis 6
1.4 Questions possibles 7

2 Groupe opérant sur un ensemble. Exemples et applications **9**
2.1 Actions de groupes, orbites et stabilisateurs 9
2.2 L'équation des classes 11
2.3 Exemples d'utilisations des actions de groupes 12
2.4 Questions possibles 16

3 Permutations d'un ensemble fini, groupe symétrique. Applications **19**
3.1 Permutations d'un ensemble fini 19
3.2 Décomposition d'une permutation en produits de cycles 20
3.3 Signature d'une permutation 21
3.4 Le groupe alterné 22
3.5 Utilisations du groupe symétrique 23
3.6 Questions possibles 25

4 Nombres complexes de module 1. Racines de l'unité **29**
4.1 Racines n-èmes d'un nombre complexe 29
4.2 Les polynômes cyclotomiques 30
4.3 Le nombre π 32
4.4 Les fonctions argument principal et logarithme 33
4.5 Le théorème de relèvement 34
4.6 Mesure des angles 35
4.7 Questions possibles 35

5 Utilisation de groupes en géométrie **39**
5.1 Espace affine associé à un espace vectoriel réel 39

5.2 Le groupe affine $GA(\mathcal{E})$ en dimension finie 41
5.3 Orientation d'un espace affine réel 43
5.4 Groupes de bijections affines conservant un ensemble 43
5.5 Isométries affines d'un espace euclidien 44
5.6 Groupe des angles orientés dans le plan euclidien 44
5.7 Le groupe des isométries du cube 45
5.8 Sous groupes finis de $Is^+(\mathcal{E})$ pour $\mathcal{E}$ de dimension 2 ou 3 46
5.9 Questions possibles 47

6 Idéaux d'un anneau commutatif. Exemples 49
6.1 Généralités sur le idéaux de $\mathbb{A}$ 49
6.2 Congruences, anneaux quotients, idéaux premiers, maximaux 50
6.3 Anneaux principaux 51
6.4 pgcd dans un anneau principal 52
6.5 Éléments premiers entre eux dans un anneau principal 52
6.6 Idéal annulateur et polynôme minimal 53
6.7 Questions possibles 56

7 Anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$. Applications 59
7.1 Congruences dans $\mathbb{Z}$, anneaux $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ 59
7.2 Le groupe multiplicatif $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right)^{\times}$, fonction indicatrice d'Euler 60
7.3 Le théorème chinois 61
7.4 Systèmes d'équations diophantiennes 63
7.5 $\left(\dfrac{\mathbb{Z}}{p^{\alpha}\mathbb{Z}}\right)^{\times}$ est cyclique pour $p \geq 3$ premier 64
7.6 Questions possibles 65

8 Nombres premiers 69
8.1 L'ensemble $\mathcal{P}$ des nombres premiers 69
8.2 Décomposition en produit de facteurs premiers 70
8.3 Théorèmes de Legendre et de Bertrand 71
8.4 Quelques tests de primalité 72
8.5 Nombres de Carmichaël 73
8.6 La fonction de Möbius 73
8.7 Un théorème de Cesàro 74
8.8 Questions possibles 75

9 pgcd dans $\mathbb{Z}$ et $\mathbb{K}[X]$ 79
9.1 pgcd dans un anneau euclidien 79
9.2 Éléments premiers entre eux. Les théorèmes de Bézout et de Gauss 81
9.3 Le théorème chinois 82
9.4 Applications 83
9.5 Questions possibles 86

10 Polynômes à une indéterminée à coefficients réels ou complexes **91**
10.1 Le théorème de d'Alembert-Gauss 91
10.2 Racines n-èmes d'un nombre complexe 92
10.3 Localisation des racines d'un polynôme complexe 93
10.4 Décomposition en éléments simples des fractions rationnelles 94
10.5 Nombres algébriques 95
10.6 Polynômes d'interpolation de Lagrange et méthodes de Newton-Cotes 96
10.7 Questions possibles 98

11 Polynômes d'endomorphismes en dimension finie. Applications **101**
11.1 L'algèbre commutative $\mathbb{K}[u]$ 101
11.2 Polynômes annulateurs, polynôme minimal 101
11.3 Le théorème de Cayley-Hamilton 102
11.4 Le théorème de décomposition des noyaux 103
11.5 La décomposition de Dunford 104
11.6 Un algorithme pour obtenir la décomposition de Dunford 106
11.7 Endomorphismes semi-simples 106
11.8 Applications 107
11.9 Questions possibles 109

12 Réduction d'un endomorphisme en dimension finie **113**
12.1 Diagonalisation 113
12.2 Trigonalisation 114
12.3 Réduction de Jordan 114
12.4 Réduction des matrices symétriques réelle 115
12.5 Réduction des matrices orthogonales réelle 115
12.6 Réduction des matrices normales 116
12.7 Propriétés topologiques de l'ensemble des matrices diagonalisables de $\mathcal{M}_n(\mathbb{C})$ 117
12.8 Questions possibles 118

13 Endomorphismes symétriques d'un espace vectoriel euclidien. Applications **121**
13.1 Endomorphismes symétriques 121
13.2 Réduction des endomorphismes symétriques 122
13.3 Endomorphismes symétriques positifs ou définis positifs 122
13.4 Réduction des endomorphismes symétriques et des formes quadratiques sur $\mathbb{R}^n$ 123
13.5 Quelques applications du théorème spectral 123
13.6 Questions possibles 124

14 Matrices symétriques réelles **127**
14.1 Réduction des matrices symétriques réelles 127
14.2 Rayon spectral 128
14.3 Formes quadratiques 128
14.4 Questions possibles 130

15 Groupe orthogonal d'un espace euclidien de dimension 2, ou 3 133
15.1 Isométries en dimension 2 ... 133
15.2 Isométries en dimension 3 ... 136
15.3 Questions possibles ... 139

16 Notion de rang en algèbre linéaire et bilinéaire. Applications . 143
16.1 Rang d'un système de vecteurs ou d'une application linéaire ... 143
16.2 Rang d'une matrice ... 145
16.3 Rang et systèmes linéaires ... 146
16.4 Rang et dualité ... 148
16.5 Rang d'une forme quadratique ... 149
16.6 Questions possibles ... 150

17 Formes linéaires, hyperplans, dualité ... 153
17.1 L'espace dual E^* ... 153
17.2 Exemples dans $\mathbb{K}_n[X]$ ... 154
17.3 Exemples dans $\mathcal{M}_n(\mathbb{K})$ ... 154
17.4 Hyperplans ... 155
17.5 Orthogonalité ... 155
17.6 Transposition ... 157
17.7 Questions possibles ... 159

18 Opérations élémentaires sur les lignes ou les colonnes d'une matrice ... 161
18.1 Matrices de dilatation et de transvection ... 161
18.2 Méthode des pivots de Gauss ... 163
18.3 Décomposition LR (méthode de Crout) ... 165
18.4 Décomposition $LD\,^tL$ ... 167
18.5 Décomposition de Cholesky des matrices symétriques réelles définies positives ... 167
18.6 Méthode d'élimination de Gauss-Jordan ... 168
18.7 Résolution des systèmes de Cramer à coefficients entiers ... 169
18.8 Questions possibles ... 170

19 Valeurs propres. Recherche et utilisation ... 173
19.1 Définitions et premières propriétés ... 173
19.2 Valeurs propres des endomorphismes nilpotents ... 174
19.3 Localisation des valeurs propres dans le cas réel ou complexe ... 175
19.4 Rayon spectral des matrices complexes ... 176
19.5 Calcul approché des valeurs propres ... 177
19.6 Polynômes orthogonaux ... 178
19.7 Questions possibles ... 179

20 Formes quadratiques sur un espace vectoriel réel de dimension finie ... 183
20.1 Théorème de réduction de Gauss ... 184
20.2 Orthogonalité, noyau et rang ... 185
20.3 Signature d'une forme quadratique réelle en dimension finie ... 186

20.4 Quadriques dans $\mathbb{R}^n$ ... 187
20.5 Orthogonalisation simultanée de deux formes quadratiques ... 189
20.6 Questions possibles ... 189

21 Utilisation des nombres complexes en géométrie ... 193
21.1 Le plan affine euclidien et le plan d'Argand-Cauchy ... 193
21.2 Utilisation du module et des arguments d'un nombre complexe ... 194
21.3 Le triangle dans le plan complexe ... 196
21.4 Centre de gravité, orthocentre, cercles inscrit et circonscrit ... 199
21.5 Droites, cercles, coniques dans le plan complexe ... 201
21.6 Inversions ... 204
21.7 Quelques questions possibles ... 205

22 Barycentres. Applications ... 207
22.1 Généralités ... 207
22.2 Coordonnées barycentriques ... 208
22.3 Ensembles convexes ... 209
22.4 Le théorème de Krein-Milman ... 211
22.5 Matrices bistochastiques ... 212
22.6 Questions possibles ... 212

23 Coniques ... 215
23.1 Définition algébrique des coniques ... 215
23.2 Définition par directrice, foyer et excentricité des coniques ... 217
23.3 Définition bifocale des coniques à centre ... 219
23.4 Définition par foyers et cercle directeur des coniques à centre ... 220
23.5 Lieu orthoptique d'une conique ... 220
23.6 Cocyclicité de 4 points sur une conique ... 222
23.7 Questions possibles ... 222

24 Droites et cercles dans le plan affine euclidien ... 227
24.1 Droites. Définitions et propriétés ... 227
24.2 Cercles. Définitions et propriétés ... 229
24.3 Droites et cercles dans le plan complexe ... 231
24.4 Puissance d'un point par rapport à un cercle ... 233
24.5 Inversions ... 235
24.6 Questions possibles ... 236

II Leçons d'analyse et de probabilité 241

25 Espaces vectoriels normés de dimension finie ... 243
25.1 Applications linéaires continues, normes équivalentes ... 243
25.2 Espaces vectoriels normés de dimension finie ... 244
25.3 Quelques applications ... 246
25.4 Questions possibles ... 247

26 Suites dans un espace vectoriel normé de dimension finie 251
26.1 Suites dans un espace vectoriel normé 251
26.2 Suites numériques convergentes 253
26.3 Suites réelles monotones, adjacentes 255
26.4 Suites de matrices et rayon spectral 256
26.5 Sous-groupes additifs de $\mathbb{R}$ 257
26.6 Sous-groupes additifs de $\mathbb{R}^n$ 258
26.7 Questions possibles 258

27 Diverses notions de convergence en analyse et en probabilités. Exemples 261
27.1 Suites et séries dans un espace normé 261
27.2 Convergence au sens de Cesàro 263
27.3 Suite et séries de fonctions 263
27.4 Fonction génératrice d'une variable aléatoire discrète 265
27.5 Convergence de variables aléatoires 266
27.6 Questions possibles 268

28 Séries à termes réels positifs. Applications 273
28.1 Séries convergentes ou divergentes 273
28.2 Cas des séries à termes positifs 274
28.3 Comparaison des séries à termes positifs 275
28.4 Produit de Cauchy de deux séries 278
28.5 Questions possibles 279

29 Séries à termes réels ou complexes. Convergence absolue, semi-convergence 281
29.1 Séries convergentes ou divergentes 281
29.2 Séries alternées 283
29.3 Séries absolument convergentes 283
29.4 Produit de deux séries 284
29.5 Séries doubles 285
29.6 La transformation d'Abel 286
29.7 Questions possibles 287

30 Comparaison d'une série et d'une intégrale. Applications 293
30.1 Comparaison de $\sum f(n)$ et $\int_0^{+\infty} f(t)\,dt$ 293
30.2 Comparaison de $\sum \int_{x_n}^{x_{n+1}} f(t)\,dt$ et $\int_a^b f(t)\,dt$ 297
30.3 Utilisation des permutations de $\sum$ et $\int$ 298
30.4 Questions possibles 299

31 Séries de fonctions. Propriétés de la somme, exemples 303
31.1 Convergence simple, uniforme et normale 303
31.2 Propriétés de la somme d'une séries de fonctions convergente 305
31.3 Permutation des signes $\sum$ et $\int$ 307
31.4 Questions possibles. 308

32 Séries entières. Rayon de convergence. Propriétés de la somme. Exemples **313**
32.1 Rayon de convergence d'une série entière 313
32.2 Opérations sur les séries entières 315
32.3 Fonctions développables en série entière 316
32.4 Séries entières et équations différentielles 318
32.5 Questions possibles 319

33 Série de Fourier d'une fonction périodique ; propriétés. Exemples **321**
33.1 L'espace préhilbertien $\mathcal{D}$ de Dirichlet 321
33.2 Polynômes trigonométriques et séries de Fourier sur $\mathcal{D}$ 321
33.3 L'inégalité de Bessel et l'égalité de Parseval 323
33.4 Convergence ponctuelle des séries de Fourier sur $\mathcal{D}$ 324
33.5 Questions possibles 326

34 Exponentielle complexe **331**
34.1 La fonction exponentielle complexe 331
34.2 Les fonctions trigonométriques et hyperboliques 332
34.3 Le nombre π 333
34.4 Les fonction tan et arctan 334
34.5 Fonctions argument principal et logarithme 335
34.6 Mesure des angles 336
34.7 Questions possibles 336

35 Exponentielles de matrices. Applications **339**
35.1 Séries matricielles 339
35.2 L'exponentielle matricielle. Propriétés 340
35.3 Utilisation de la décomposition de Dunford 342
35.4 Surjectivité et injectivité de l'exponentielle matricielle 342
35.5 Questions possibles 344

36 Intégrale d'une fonction dépendant d'un paramètre **349**
36.1 Intégrale fonction de ses bornes 349
36.2 Théorèmes élémentaires 350
36.3 Théorèmes de convergence dominée 351
36.4 Produit de convolution 352
36.5 Questions possibles 353

37 La fonction gamma **359**
37.1 Généralités sur la fonction gamma 359
37.2 Formules d'Euler, de Wallis, de Legendre et de Stirling 359
37.3 Continuité et dérivabilité de gamma 360
37.4 Prolongement de la fonction gamma 361
37.5 La formule des compléments 361
37.6 Fonction Béta 362
37.7 Calcul de certaines intégrales à l'aide de Γ 362
37.8 Loi Gamma 363
37.9 Questions possibles 365

38 Théorème des valeurs intermédiaires. Applications **369**
38.1 Le théorème des valeurs intermédiaires 369
38.2 Réciproque du théorème des valeurs intermédiaires 371
38.3 Fonctions réciproques 372
38.4 Applications du théorème des valeurs intermédiaires 372
38.5 Questions possibles 373

39 Théorèmes des accroissements finis **377**
39.1 Le théorème de Rolle sur un espace vectoriel normé 377
39.2 Théorème et inégalité des accroissements finis 378
39.3 Quelques applications du théorème des accroissements finis 379
39.4 Questions possibles 384

40 Formules de Taylor pour une fonction d'une variable réelle **387**
40.1 La formule de Taylor-Lagrange 387
40.2 Le théorème de Taylor-Young 387
40.3 Formule de Taylor avec reste intégral 388
40.4 Applications de la formule de Taylor-Lagrange 389
40.5 Applications de la formule de Taylor avec reste intégral 392
40.6 Questions possibles 392

41 Fonctions convexes d'une variable réelle. Applications **395**
41.1 Fonctions convexes 395
41.2 Régularité des fonctions convexes 397
41.3 Inégalités de convexité 400
41.4 Questions possibles 403

42 Fonctions de plusieurs variables : dérivées partielles, différentiabilité **405**
42.1 Fonctions différentiables 405
42.2 Dérivée suivant un vecteur, dérivées partielles 407
42.3 Théorème et inégalité des accroissements finis 409
42.4 Différentielles d'ordre supérieur 410
42.5 Formule de Taylor-Lagrange 412
42.6 Différentiabilité et problèmes d'extremum 413
42.7 Questions possibles 414

43 Méthodes de calcul approché d'une intégrale **421**
43.1 Formules de quadrature 421
43.2 Méthodes des rectangles et des points milieux 422
43.3 Les méthodes de Newton-Cotes 423
43.4 La méthode des trapèzes et de Simpson 425
43.5 La formule d'Euler-Maclaurin 427
43.6 Méthode de Gauss 429
43.7 Questions possibles 431

44 Espaces préhilbertiens **433**
44.1 Espaces préhilbertiens 433

44.2 Orthogonalisation de Gram-Schmidt 435
44.3 Meilleure approximation dans un espace préhilbertien 436
44.4 Inégalité de Bessel et égalité de Parseval 437
44.5 Déterminants de Gram 439
44.6 Les théorèmes de Müntz 441
44.7 Questions possibles 443

45 Équations différentielles linéaires d'ordre deux 447
45.1 Le théorème de Cauchy-Lipschitz linéaire 447
45.2 Méthode de Lagrange 449
45.3 Équations différentielles linéaires d'ordre 2 450
45.4 Équations différentielles linéaires à coefficients développables en série entière 452
45.5 Racines des solutions d'une équation différentielle linéaire d'ordre 2 454
45.6 Problèmes aux limites 455
45.7 Questions possibles 456

46 Systèmes différentiels linéaires à coefficients constants 459
46.1 Systèmes différentiels linéaires à coefficients constants 459
46.2 L'exponentielle d'une matrice 461
46.3 Un algorithme de calcul de l'exponentielle d'une matrice 463
46.4 Equations différentielles linéaires d'ordre n 463
46.5 Questions possibles 464

47 Inégalités en analyse et en probabilités 467
47.1 Inégalités de Cauchy-Schwarz et Minkowski 467
47.2 Inégalité des accroissements finis 468
47.3 Inégalités de convexité 469
47.4 L'inégalité de Bessel 472
47.5 Inégalités de Bienaymé-Tchebychev 472
47.6 Questions possibles 473

48 Étude métrique des courbes planes 477
48.1 Arcs paramétrés, arcs géométriques dans $\mathbb{R}^2$ 477
48.2 Tangente à un arc paramétré 478
48.3 Longueur d'un arc paramétré 480
48.4 Vecteur unitaire tangent, normal. Courbure 481
48.5 L'inégalité isopérimétrique 483
48.6 Questions possibles 484

Bibliographie 489

Index 491

Première partie

Leçons d'algèbre et de géométrie

Leçon 1

Groupes monogènes, groupes cycliques. Exemples

1.1 Groupes monogènes, groupes cycliques

Définition 1.1 *Un groupe $(G, \cdot)$ est dit monogène s'il existe un élément $g \in G$ tel que $G = \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Si de plus G est fini, on dit alors qu'il est cyclique.*

Pour un groupe additif, on a $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$.

Un groupe cyclique est nécessairement commutatif et s'il est engendré par un élément $g \neq 1$, il a alors au moins deux élément.

Exemples 1.1

1. *Le groupe additif $(\mathbb{Z}, +)$ est monogène engendré par 1 et ses sous-groupes qui sont tous de la forme $n\mathbb{Z}$ avec $n \geq 0$ sont monogènes.*
2. *Pour tout $n \in \mathbb{N}^*$, le groupe quotient $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ est cyclique d'ordre n engendré par $\overline{1}$.*
3. *Le groupe multiplicatif $\mathbb{U}_n$ des racines n-ème de l'unité est cyclique d'ordre n isomorphe à $\dfrac{\mathbb{Z}}{n\mathbb{Z}}$ par l'application $\overline{k} \mapsto e^{\frac{2ik\pi}{n}}$.*
4. *Tout sous-groupe d'ordre $n \geq 1$ du groupe $O_2^+(\mathbb{R})$ des matrices de rotations du plan vectoriel euclidien $\mathbb{R}^2$ est cyclique engendré par la rotation $R\left(\dfrac{2\pi}{n}\right)$ d'angle $\dfrac{2\pi}{n}$.*
5. *Tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ d'un corps commutatif $\mathbb{K}$ est cyclique. En particulier, pour tout nombre premier $p \geq 2$, le groupe multiplicatif $\mathbb{F}_p^*$ et cyclique d'ordre $p-1$ (en notant $\mathbb{F}_p$ le corps $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$).*

Théorème 1.1.

Soit $(G, \cdot)$ un groupe monogène. S'il est infini, il est alors isomorphe à $(\mathbb{Z}, +)$, s'il est cyclique d'ordre n, il est alors isomorphe à $\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}, +\right)$.

Dire que G est cyclique d'ordre n, signifie que G est de cardinal égal à n et qu'il existe dans G au moins un élément g d'ordre n. Dans ce cas, on a :

$$G = \langle g \rangle = \left\{1, g, \cdots, g^{n-1}\right\}$$

Théorème 1.2.

Si $G = \langle g \rangle$ est un groupe cyclique d'ordre n, ses générateurs sont alors les g^k, où k est un entier compris entre 1 et $n-1$ premier avec n. Le nombre de ces générateurs est égal à $\varphi(n)$, où φ est la fonction indicatrice d'Euler.

Le théorème qui suit nous dit qu'à isomorphisme près, il y a un seul groupe d'ordre p premier, à savoir $\dfrac{\mathbb{Z}}{p\mathbb{Z}}$.

Théorème 1.3.

Un groupe de cardinal premier est cyclique.

Si p et q sont deux nombres premiers, un groupe d'ordre pq n'est pas nécessairement cyclique comme le montre l'exemple du groupe symétrique $\mathcal{S}_3$ qui est d'ordre 6 non commutatif et donc non cyclique. Mais pour G commutatif d'ordre pq avec $p \neq q$, on a le résultat suivant.

Théorème 1.4.

Un groupe commutatif d'ordre pq, où p et q sont deux nombres premiers distincts, est cyclique.

Pour $p = q$ premier, le théorème précédent est faux comme le montre l'exemple de $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ qui est d'ordre p^2 non cyclique puisque tous ses éléments distincts du neutre sont d'ordre p.

Théorème 1.5.

Un groupe d'ordre p^2 avec p premier est commutatif isomorphe au groupe cyclique $\dfrac{\mathbb{Z}}{p^2\mathbb{Z}}$ ou au groupe non cyclique $\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$.

Théorème 1.6.

Si $n \geq 2$ est un entier premier avec $\varphi(n)$, alors tout groupe commutatif d'ordre n est cyclique.

Plus généralement, on peut montrer qu'un entier $n \geq 2$ est premier avec $\varphi(n)$ si, et seulement si, tout groupe d'ordre n est cyclique (c'est plus délicat).

Théorème 1.7.

Si p est un nombre premier impair et α un entier supérieur ou égal à 2, le groupe multiplicatif $\left(\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}\right)^\times$ des éléments inversibles de $\dfrac{\mathbb{Z}}{p^\alpha\mathbb{Z}}$ est alors

cyclique. Pour $p = 2$, le groupe multiplicatif $\left(\dfrac{\mathbb{Z}}{2^\alpha\mathbb{Z}}\right)^\times$ est cyclique pour $\alpha = 1$, $\alpha = 2$ et non cyclique pour $\alpha \geq 3$.

1.2 Sous-groupes d'un groupe monogène

Théorème 1.8.

Soit $(G, \cdot)$ un groupe monogène infini. Tout sous-groupe de G est monogène isomorphe à $(n\mathbb{Z}, +)$ où $n \in \mathbb{N}^*$.

Théorème 1.9.

Soient $n \geq 2$ un entier et $G = \langle a \rangle$ un groupe cyclique d'ordre n.

1. *Les sous-groupes de $G = \langle a \rangle$ sont tous cycliques d'ordre divisant n.*
2. *Pour tout diviseur positif d de n, il existe un unique sous-groupe d'ordre d de G. Ce sous-groupe est le groupe cyclique $H = \left\langle a^{\frac{n}{d}} \right\rangle$. C'est également l'ensemble de tous les éléments de G d'ordre divisant d et les générateurs de H sont tous les éléments d'ordre d de G.*

Exemple 1.1 *Les sous-groupes de $\mathbb{U}_n = \{z \in C \mid z^n = 1\} = \left\langle e^{\frac{2i\pi}{n}} \right\rangle$ sont les $\left\langle \left(e^{\frac{2i\pi}{n}}\right)^{\frac{n}{d}} \right\rangle = \left\langle e^{\frac{2i\pi}{d}} \right\rangle = \mathbb{U}_d$ où d est un diviseur de n et il y en a autant que de diviseurs de n.*

Le résultat précédent est en fait caractéristique des groupes cycliques.

Théorème 1.10.

Un groupe commutatif fini d'ordre $n \geq 1$ est cyclique si, et seulement si, pour tout diviseur d de n, il existe un unique sous-groupe d'ordre d de G.

Si $G = \langle a \rangle$ est un groupe cyclique d'ordre $n \geq 1$, il y a autant de sous-groupes de G que de diviseurs de n puisque l'application $d \in \mathcal{D}_n \mapsto \left\langle a^{\frac{n}{d}} \right\rangle$ réalise une bijection de l'ensemble $\mathcal{D}_n$ des diviseurs positifs de n sur l'ensemble des sous-groupes de G.

Pour un groupe fini non commutatif d'ordre $n \geq 4$ et pour d divisant n, il n'existe pas nécessairement de sous-groupe d'ordre d. Par exemple dans le groupe alterné $\mathcal{A}_4$ qui est d'ordre 12, il n'y a pas de sous-groupes d'ordre 6. Mais pour tout diviseur premier p de n, il existe un sous-groupe de G d'ordre p (théorème de Cauchy).

Pour $G = \dfrac{\mathbb{Z}}{n\mathbb{Z}}$ et tout diviseur d de n, l'unique sous-groupe d'ordre d de G est $\langle q\overline{1} \rangle = \dfrac{q\mathbb{Z}}{n\mathbb{Z}}$, où $q = \dfrac{n}{d}$ et ce sous-groupe est isomorphe à $\dfrac{\mathbb{Z}}{d\mathbb{Z}}$.

Corollaire 1.1. *Pour tout entier $n \geq 2$, on a* $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$.

Le théorème 1.10 nous permet de montrer le théorème de Cauchy dans le cas commutatif.

Théorème 1.11. (Cauchy).

Soit G un groupe commutatif fini d'ordre $n \geq 2$. Pour tout diviseur premier p de n il existe dans G un élément d'ordre p.

1.3 Théorème de structure des groupes abéliens finis

On note $\theta(g)$ l'ordre d'un élément g d'un groupe G. Pour un groupe abélien fini G, l'entier $e(G) = \max_{g \in G} \theta(g)$ est l'exposant du groupe. On rappelle qu'on a aussi $e(G) = \text{ppcm}\{\theta(g) \mid g \in G\}$.

Un caractère d'un groupe G est un morphisme de groupes de G dans $\mathbb{C}^*$.

Pour tout entier $m \geq 2$, on note $\mathbb{U}_m$ le groupe cyclique des racines m-èmes de l'unité dans $\mathbb{C}^*$.

Dans ce qui suit, on se donne un groupe commutatif G d'ordre $n \geq 2$.

Lemme 1.1 *Soit H un sous-groupe de G. Tout caractère $\varphi : H \to \mathbb{C}^*$ peut se prolonger en un caractère sur G.*

Lemme 1.2 *On se donne un élément g_0 de G d'ordre égal à l'exposant de G, soit :*

$$m = \theta(g_0) = \max_{g \in G} \theta(g) = \text{ppcm}\{\theta(g) \mid g \in G\}$$

et en supposant que $m \leq n-1$, on note $K = \langle g_0 \rangle$ le sous-groupe cyclique de G engendré par g_0.

— *Il existe un unique caractère $\varphi_0 : K \to \mathbb{C}^*$ tel que $\varphi_0(g_0) = \omega = e^{\frac{2i\pi}{m}}$.*

— *En prolongeant le caractère φ_0 en un caractère φ de G, l'application :*

$$\begin{array}{rccc} \theta : & \langle g_0 \rangle \times \ker(\varphi) & \to & G \\ & (g_0^k, h) & \mapsto & g_0^k h \end{array}$$

est un isomorphisme de groupes.

Théorème 1.12. (Kronecker).

Il existe une unique suite d'entiers $(n_k)_{1 \leq k \leq r}$ telle que $n_1 \geq 2$, n_2 est multiple de $n_1, \cdots, n_k$ est multiple de n_{k-1} et G est isomorphe au groupe produit $\prod_{k=1}^{r} \mathbb{U}_{n_k}$

1.4 Questions possibles

Question 1.1 *Soit $X = \{r_1, \cdots, r_n\}$ une partie finie de $\mathbb{Q}$ et $G = \langle X \rangle$ le sous-groupe de $(\mathbb{Q}, +)$ engendré par X. Montrer que G est monogène infini.*

Solution. En désignant par μ le ppcm des dénominateurs de $r_1, \cdots, r_n$, il existe des entiers relatifs $a_1, \cdots, a_n$ tels que $r_k = \dfrac{a_k}{\mu}$ pour tout k compris entre 1 et n et en désignant par δ le pgcd de $a_1, \cdots, a_n$, on a :

$$G = \left\{ \sum_{k=1}^{n} \alpha_k \frac{a_k}{\mu} \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\} = \left\{ \frac{\delta}{\mu} \sum_{k=1}^{n} \alpha_k b_k \mid (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n \right\}$$

où $b_1, \cdots, b_n$ sont des entiers relatifs premiers entre eux dans leur ensemble. On a donc $G = \dfrac{\delta}{\mu}\mathbb{Z}$, ce qui signifie que G est monogène engendré par $\dfrac{\delta}{\mu}$.

Question 1.2 *Montrer que, pour tout entier $n \geq 1$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n et que ce groupe est cyclique.*

Solution. Supposons que G soit un sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ d'ordre n. Tout $\overline{r} \in G$ a un ordre qui divise n (théorème de Lagrange), donc $n\overline{r} = \overline{0}$, c'est-à-dire qu'il existe $q \in \mathbb{Z}$ tel que $nr = q$ et $r = \dfrac{q}{n}$. On a donc $\overline{r} = \overline{\dfrac{q}{n}} = q\overline{\dfrac{1}{n}} \in \left\langle \overline{\dfrac{1}{n}} \right\rangle$ et $G \subset \left\langle \overline{\dfrac{1}{n}} \right\rangle$. Comme $\overline{\dfrac{1}{n}}$ est d'ordre n dans $\mathbb{Q}/\mathbb{Z}$ (on a $k\overline{\dfrac{1}{n}} = \overline{\dfrac{k}{n}} = \overline{0}$ si, et seulement si, $\dfrac{k}{n} \in \mathbb{Z}$, ce qui équivaut à dire que k est multiple de n), on a nécessairement $G = \left\langle \overline{\dfrac{1}{n}} \right\rangle$. D'où l'unicité d'un groupe d'ordre n et ce groupe existe (c'est $\left\langle \overline{\dfrac{1}{n}} \right\rangle$).

Question 1.3 *Montrer que pour tout corps commutatif $\mathbb{K}$ et tout entier $n \in \mathbb{N}^*$, le groupe $\mu_n(\mathbb{K}) = \{\lambda \in \mathbb{K} \mid \lambda^n = 1\}$ des racines n-èmes de l'unité dans $\mathbb{K}^*$ est cyclique d'ordre au plus égal à n. Préciser les cas de $\mathbb{C}$, $\mathbb{R}$, et $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ pour p premier.*

Solution. $\mu_n(\mathbb{K})$ est le noyau du morphisme de groupes $\lambda \in \mathbb{K}^* \mapsto \lambda^n$, c'est donc un sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ de cardinal au plus égal à n (racines dans $\mathbb{K}$ du polynôme de degré n, $X^n - 1$) et en conséquence il est cyclique. Pour $\mathbb{K} = \mathbb{C}$, $\mu_n(\mathbb{C}) = \mathbb{U}_n \left\{ e^{\frac{2ik\pi}{n}},\ 0 \leq k \leq n-1 \right\}$ est cyclique d'ordre n. Pour $\mathbb{K} = \mathbb{R}$, $\mu_{2p+1}(\mathbb{R}) = \{1\}$ est cyclique d'ordre 1 et $\mu_{2p}(\mathbb{R}) = \{-1, 1\}$ est cyclique d'ordre 2, pour $\mathbb{K} = \mathbb{F}_p$, $\mu_n(\mathbb{F}_p)$ qui est un sous-groupe du groupe cyclique $\mathbb{F}_p^*$ est cyclique d'ordre divisant $p - 1$.

Question 1.4 *Soit G un sous-groupe fini de $GL_2(\mathbb{R})$. Montrer que G est cyclique ou diédral.*

Solution. En munissant $\mathbb{R}^2$ de sa structure euclidienne canonique, l'application $\varphi : (x, y) \mapsto \sum_{u \in G} \langle u(x) \mid u(y) \rangle$ définit un produit scalaire sur E et pour $g \in G$, x, y dans $\mathbb{R}^2$, on a :

$$\begin{aligned}\varphi(g(x), y) &= \sum_{u \in G} \langle u(g(x)) \mid u(y) \rangle = \sum_{u \in G} \left\langle u \circ g(x) \mid u \circ g\left(g^{-1}(y)\right) \right\rangle \\ &= \sum_{v \in G} \left\langle v(x) \mid v\left(g^{-1}(y)\right) \right\rangle = \varphi\left(x, g^{-1}(y)\right)\end{aligned}$$

($u \mapsto u \circ g$ est une permutation de G), donc G est un sous-groupe de $\mathcal{O}(E, \varphi)$. Si G est contenu dans $\mathcal{O}^+(E, \varphi)$, il est isomorphe à un sous-groupe du groupe $\mathbb{U}$ des nombres complexes de module égal à 1 et on sait que l'unique sous-groupe d'ordre $n = \operatorname{card}(G)$ de $\mathbb{U}$ est le groupe $\mathbb{U}_n$ des racines n-èmes de l'unité. L'unique sous-groupe d'ordre n de $\mathcal{O}^+(E, \varphi)$ est donc le groupe cyclique $\left\{Id, \rho, \cdots, \rho^{n-1}\right\}$ d'ordre p engendré par la rotation ρ d'angle $\dfrac{2\pi}{n}$. Si G n'est pas contenu dans $\mathcal{O}^+(E, \varphi)$, pour toute réflexion $\sigma \in G \setminus \mathcal{O}^+(E, \varphi)$, on a $G = G^+ \cup \sigma \circ G^+$, en notant $G^+ = G \cap \mathcal{O}^+(E, \varphi)$. Comme $G^+ = \left\{Id, \rho, \cdots, \rho^{r-1}\right\}$ (sous-groupe fini de $\mathcal{O}^+(E, \varphi)$) où $r = \dfrac{n}{2}$ et ρ est une rotation d'angle $\dfrac{2\pi}{n}$ qui engendre G^+, on a :

$$G = \left\{Id, \rho, \cdots, \rho^{r-1}, \rho \circ \sigma, \cdots, \rho^{r-1} \circ \sigma\right\}$$

qui est diédral.

Leçons d'oral pour l'agrégation de mathématiques

Première épreuve : les exposés

Taillé sur mesure pour les candidats à l'agrégation de mathématiques, cet ouvrage est exclusivement consacré à la première épreuve orale d'exposés.

Il rassemble les 48 leçons incontournables en algèbre et géométrie, puis en analyse et probabilités, pour permettre au candidat d'élaborer dans le temps imparti, plan, théorèmes et définitions attendus.

Chaque leçon se termine par une série de questions que pourrait poser le jury afin de se mettre dans les conditions réelles de l'épreuve.

LES PLUS

- **24 leçons d'algèbre et de géométrie**
- **24 leçons d'analyse et de probabilités**
- **Plus de 230 questions type de jury et leurs solutions**

Agrégé de mathématiques, **Jean-Étienne Rombaldi** a enseigné à l'université Grenoble-Alpes, institut Fourier. Préparateur à l'agrégation interne de cette même université ainsi que pour le CNED, il a été membre du jury du CAPES externe et de l'agrégation interne de mathématiques et responsable de la préparation à l'agrégation interne de l'université de Grenoble.

Un ouvrage complémentaire du même auteur, consacré à la seconde épreuve d'exercices, est disponible chez le même éditeur.

Conception graphique : Primo&Primo®

ISBN : 978-2-8073-2153-3

9 782807 321533

deboeck SUPÉRIEUR

www.deboecksuperieur.com