

# Table des matières

[\*] : exercice très difficile, ne pas hésiter à consulter le corrigé.

[\*\*] : exercice utilisant des notions hors programme, plutôt destiné aux candidats à l'agrégation.

**Introduction** **5**

**Plan de la collection** **9**

**1. Théorie des groupes** **11**

1.1. Existence d'un idempotent . . . . .	11
1.2. Axiomes faibles de groupe . . . . .	12
1.3. Sous-groupe du groupe affine de $\mathbb{R}$ . . . . .	12
1.4. Groupes dont l'ensemble des sous-groupes est fini . . . . .	13
* 1.5. Sous-groupe et combinatoire . . . . .	13
* 1.6. Parties de $A$ sans somme dans $A$ . . . . .	14
1.7. Noyau et image de $f$ et $f^2$ . . . . .	16
1.8. Morphismes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$ . . . . .	17
1.9. Morphismes de $(\mathbb{Q}, +)$ dans $(\mathbb{Q}_+^*, \times)$ . . . . .	17
1.10. Involution sans point fixe non trivial . . . . .	17
1.11. Groupes finis sans automorphisme non trivial . . . . .	18
* 1.12. Morphismes de $(\mathbb{Z}^{\mathbb{N}}, +)$ dans $(\mathbb{Z}, +)$ . . . . .	19
1.13. Partie génératrice de $(\mathbb{Q}, +)$ . . . . .	21
1.14. Éléments non générateurs, sous-groupe de Frattini . . . . .	21
1.15. Groupe dérivé . . . . .	23
1.16. Groupe résoluble . . . . .	24
1.17. Un sous-groupe du groupe circulaire droit . . . . .	26
1.18. Fonction de croissance d'un groupe (1) . . . . .	27
1.19. Fonction de croissance d'un groupe (2) . . . . .	28
1.20. Famille minimale engendrant $G$ par produit . . . . .	29
1.21. Sous-groupes finis de $\mathbb{Q}/\mathbb{Z}$ . . . . .	31
1.22. Groupes de cardinal 8 . . . . .	32
1.23. Preuve de MacKay du lemme de Cauchy (1959) . . . . .	33
* 1.24. Théorème de Sylow . . . . .	35
1.25. Exposant d'un groupe abélien fini . . . . .	36
* 1.26. Groupes abéliens finis (1) . . . . .	38
* 1.27. Groupes abéliens finis (2) . . . . .	40
1.28. Puissances dans un groupe abélien d'exposant fini . . . . .	42
1.29. Involutions dans un groupe . . . . .	44
1.30. Classes de conjugaison . . . . .	45
1.31. Centre d'un $p$ -groupe . . . . .	45
1.32. Nombre de classes de conjugaison . . . . .	47
* 1.33. Sous-groupe d'indice infini . . . . .	48

** 1.34. Un théorème de Frobenius (1895) . . . . .	50
1.35. Le groupe diédral . . . . .	51
1.36. Sous-groupes finis de $SO_3(\mathbb{R})$ . . . . .	52
1.37. Groupes quasi-cycliques de Prüfer . . . . .	56
1.38. Le groupe modulaire . . . . .	57
* 1.39. Groupe libre . . . . .	61
* 1.40. Théorème de Frucht (1939) . . . . .	63
1.41. Un théorème de Cayley . . . . .	67
1.42. Sous-groupe commutatif transitif de $\mathfrak{S}_n$ . . . . .	68
1.43. Maximalité de $\mathfrak{S}_{n-1}$ dans $\mathfrak{S}_n$ . . . . .	68
1.44. Génération du groupe symétrique . . . . .	69
1.45. Carrés de $\mathfrak{S}_n$ . . . . .	70
1.46. Plongement de $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$ . . . . .	71
1.47. Un calcul de signature . . . . .	72
1.48. Morphismes d'un sous-groupe de $\mathfrak{S}_p$ dans $\mathbb{Z}/p\mathbb{Z}$ . . . . .	72
* 1.49. Morphismes de $\mathfrak{S}_4$ dans $\mathfrak{S}_3$ . . . . .	74
* 1.50. Automorphismes de $\mathfrak{S}_n$ . . . . .	78
1.51. Structure de groupe ordonné sur $\mathbb{Z}^2$ . . . . .	80
<b>2. Anneaux et corps</b> . . . . .	<b>83</b>
2.1. Inversibilité à droite . . . . .	84
2.2. Calcul d'inverse . . . . .	85
* 2.3. Cas particuliers d'un théorème de Jacobson . . . . .	86
2.4. Commutativité ou anti-commutativité . . . . .	87
2.5. Nilpotents de $\mathbb{Z}/n\mathbb{Z}$ . . . . .	88
2.6. Anneaux réguliers . . . . .	88
2.7. Groupe des inversibles de $\mathbb{Z}[\sqrt{7}]$ . . . . .	90
2.8. Sous-groupe du groupe des inversibles de $\mathbb{Z}[\sqrt{2}]$ . . . . .	91
2.9. Idéaux principaux . . . . .	93
2.10. Idéaux maximaux . . . . .	93
2.11. Exemple d'anneau local . . . . .	95
2.12. Anneau des nombres décimaux . . . . .	96
** 2.13. Anneau $\mathbb{Z}[X]$ . . . . .	97
** 2.14. Anneaux factoriels . . . . .	98
** 2.15. Anneaux euclidiens . . . . .	100
2.16. Anneau des entiers de Gauss (1) . . . . .	104
** 2.17. Anneau des entiers de Gauss (2) . . . . .	106
2.18. L'anneau euclidien $\mathbb{Z}[i\sqrt{2}]$ . . . . .	110
** 2.19. L'anneau $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ . . . . .	110
2.20. Une extension quadratique de $\mathbb{C}[X]$ . . . . .	113
2.21. Anneau sans idéal non premier . . . . .	115
* 2.22. Anneau produit fini de corps finis . . . . .	116
2.23. Racines carrées . . . . .	117
2.24. Nombres algébriques . . . . .	119

2.25. Automorphismes de  $\mathbb{Q}(\sqrt{2})$  . . . . . 122

2.26. Corps quadratiques . . . . . 123

2.27. Valuations sur  $\mathbb{Q}$  . . . . . 125

\*\* 2.28. Valeurs absolues non-archimédiennes sur  $\mathbb{C}(X)$  . . . . . 127

\*\* 2.29. Indépendance des valeurs absolues sur  $\mathbb{Q}$  . . . . . 129

**3. Arithmétique** **131**

3.1. Question de divisibilité (1) . . . . . 132

3.2. Question de divisibilité (2) . . . . . 133

3.3. Question de divisibilité (3) . . . . . 133

3.4. Question de divisibilité (4) . . . . . 134

3.5. Question de divisibilité (5) . . . . . 135

\* 3.6. Question de divisibilité (6) . . . . . 136

3.7. Produits d'entiers consécutifs . . . . . 138

3.8. Pgcd d'une famille de coefficients binomiaux . . . . . 138

3.9. Suite de Fibonacci . . . . . 139

3.10. Étude de l'irréductibilité d'une fraction . . . . . 140

3.11. Points du réseau  $\mathbb{Z}^n$  visibles de l'origine . . . . . 141

3.12. Une identité arithmétique . . . . . 142

3.13. Parties de  $\mathbb{N}$  additivement stables . . . . . 143

\* 3.14. Fonction  $f : \mathbb{N} \rightarrow \mathbb{Z}$  telle que  $m - n$  divise  $f(m) - f(n)$  . . . . . 144

3.15. Un exercice pour les années impaires . . . . . 147

3.16. Un problème de congruence . . . . . 147

3.17. Entiers qui ne s'écrivent qu'avec le chiffre 1 . . . . . 148

3.18. Somme des puissances  $k$ -ièmes dans  $\mathbb{Z}/p\mathbb{Z}$  . . . . . 148

3.19. Théorème de Wilson (1759) . . . . . 149

3.20. Théorème de Wolstenholme (1862) . . . . . 150

3.21. Cyclicité du groupe multiplicatif  $(\mathbb{Z}/p\mathbb{Z})^*$  . . . . . 150

3.22. Suite des ordres multiplicatifs d'un entier modulo  $p^n$  . . . . . 152

3.23. Critères de primalité . . . . . 153

3.24. Diviseurs premiers communs aux termes d'une suite arithmétique . . . . . 154

3.25. Nombres de Fermat . . . . . 154

3.26. Une caractérisation des nombres premiers impairs . . . . . 156

3.27. Infinité des nombres premiers congrus à 3 modulo 4 . . . . . 157

3.28. Version faible du théorème de Dirichlet (1) . . . . . 158

3.29. Version faible du théorème de Dirichlet (2) . . . . . 158

\* 3.30. Un théorème d'Erdős (1965) . . . . . 161

3.31. Plus petit nombre premier ne divisant pas  $n$  . . . . . 162

3.32. Théorème de Kurschak (1918) . . . . . 163

3.33. Diviseurs d'un entier congrus à 1 ou 2 modulo 3 . . . . . 163

3.34. Formule de Legendre (1808) . . . . . 165

3.35. Produit de trois entiers consécutifs . . . . . 167

\* 3.36. Théorème de Palfy-Erdős (1987) . . . . . 168

3.37. Divisibilité de coefficients binomiaux . . . . . 170

3.38. Congruences de Lucas (1878) . . . . . 171

3.39. Valuation  $p$ -adique d'un coefficient binomial . . . . . 173

3.40. Un problème de congruence . . . . . 173

3.41. Le problème de Ducci . . . . .	175
3.42. Nombre moyen de diviseurs . . . . .	178
3.43. Une majoration de $\sigma$ . . . . .	179
3.44. Équation faisant intervenir $\sigma$ . . . . .	180
* 3.45. Sur la fonction $\sigma$ . . . . .	180
3.46. Fonctions arithmétiques multiplicatives . . . . .	181
* 3.47. Un théorème d'Erdős (1946) . . . . .	184
3.48. Probabilité pour que deux entiers soient premiers entre eux . . . . .	186
* 3.49. Minoration de Tchebychev (1) . . . . .	189
3.50. Minoration de Tchebychev (2) . . . . .	191
3.51. Majoration de Tchebychev . . . . .	191
3.52. Triplets pythagoriciens . . . . .	192
3.53. Écriture d'un nombre premier comme somme de deux carrés . . . . .	194
3.54. Théorème des deux carrés, preuve combinatoire . . . . .	195
3.55. Cercle $x^2 + y^2 = 1$ dans $\mathbb{F}_p$ . . . . .	197
3.56. Théorème des quatre carrés de Lagrange (1770) . . . . .	198
* 3.57. Lemme de Davenport-Cassels . . . . .	200
3.58. Équation diophantienne $a^b = b^a$ . . . . .	201
3.59. Un cas particulier de l'équation de Catalan . . . . .	202
3.60. Une équation diophantienne . . . . .	203
3.61. Théorème de Sophie Germain (1823) . . . . .	204

#### 4. Polynômes

207

4.1. Condition de divisibilité (1) . . . . .	208
4.2. Condition de divisibilité (2) . . . . .	209
* 4.3. Condition de divisibilité (3) . . . . .	209
4.4. Condition pour que $(P')^p$ divise $P^q$ . . . . .	211
4.5. Racine cubique de X modulo P . . . . .	211
4.6. Racine carrée de X modulo $X^n - 1$ . . . . .	212
4.7. Une suite de pgcd périodique . . . . .	213
4.8. Trinômes irréductibles de $\mathbb{Z}/p\mathbb{Z}[X]$ . . . . .	213
4.9. Une équation fonctionnelle (1) . . . . .	214
4.10. Une équation fonctionnelle (2) . . . . .	215
4.11. Un théorème de Liouville (1879) . . . . .	217
4.12. Théorème de Mason (1984) . . . . .	218
4.13. Résultant de deux polynômes . . . . .	219
4.14. Caractérisation d'un polynôme par les antécédents de deux points distincts . . . . .	222
4.15. Image réciproque d'une partie finie par un polynôme . . . . .	223
4.16. Sur le nombre d'antécédents d'un point par un polynôme . . . . .	223
4.17. Racines d'un polynôme de $(\mathbb{Z}/n\mathbb{Z})[X]$ avec $n$ non premier . . . . .	224
4.18. Polynôme rationnel inséparable de degré 5 . . . . .	225
4.19. Un polynôme irréductible de $\mathbb{Z}[X]$ . . . . .	225
4.20. Critère d'Eisenstein . . . . .	227
* 4.21. Irréductibilité de $\Phi_p$ dans $\mathbb{Q}[X]$ . . . . .	228
4.22. Polynômes complexes d'image réelle . . . . .	230
4.23. Polynômes de $\mathbb{Q}[X]$ envoyant $\mathbb{R} \setminus \mathbb{Q}$ dans $\mathbb{R} \setminus \mathbb{Q}$ . . . . .	231
4.24. Polynômes et fractions laissant invariant le cercle unité . . . . .	231

* 4.25. Famille de fonctions polynomiales . . . . .	232
4.26. Comparaison entre trinômes . . . . .	233
4.27. Étude locale d'une fonction polynomiale complexe . . . . .	235
* 4.28. Polynômes à coefficients dans $\{-1, 1\}$ . . . . .	236
4.29. Polynômes positifs . . . . .	238
4.30. Polynômes positifs sur $\mathbb{R}_+$ . . . . .	238
4.31. Polynômes positifs sur $[-1, 1]$ . . . . .	239
4.32. Polynômes strictement positifs sur $\mathbb{R}_+$ . . . . .	241
4.33. Un polynôme positif . . . . .	243
4.34. Diviseurs d'un polynôme de $\mathbb{Z}[X]$ . . . . .	244
4.35. Décomposition en base $-2$ . . . . .	244
4.36. Polynômes de Hilbert . . . . .	245
4.37. Polynômes laissant invariant un ensemble d'entiers . . . . .	246
4.38. Interpolation de Lagrange . . . . .	247
4.39. Majoration de la norme infinie . . . . .	248
4.40. Polynômes complexes envoyant surjectivement $\mathbb{Q}$ sur $\mathbb{Q}$ . . . . .	249
4.41. Nombre de solutions à $ P(x)  = 1$ pour $P \in \mathbb{Z}[X]$ . . . . .	250
4.42. Caractérisation des polygones réguliers . . . . .	251
4.43. Images des racines d'un polynôme . . . . .	252
4.44. Un calcul de $\zeta(2)$ . . . . .	253
4.45. Encadrement de racines réelles . . . . .	254
4.46. Polynômes réels scindés . . . . .	255
4.47. Un théorème de Kronecker . . . . .	257
* 4.48. Racine de $P'$ de plus petit module . . . . .	258
4.49. Formules de Newton (1707) . . . . .	259
** 4.50. Conjecture de Popoviciu . . . . .	262
4.51. Un polynôme scindé sur $\mathbb{R}$ . . . . .	264
4.52. Dénombrement de racines réelles . . . . .	265
4.53. Dérivation et polynômes réels scindés . . . . .	266
4.54. Comportement asymptotique des racines d'un polynôme . . . . .	267
* 4.55. Un théorème de Laguerre . . . . .	268
4.56. Plan vectoriel de polynômes scindés sur $\mathbb{R}$ (1) . . . . .	270
4.57. Plan vectoriel de polynômes scindés sur $\mathbb{R}$ (2) . . . . .	272
4.58. L'ouvert des polynômes scindés à racines simples sur $\mathbb{R}$ . . . . .	272
4.59. Condition nécessaire pour qu'un polynôme réel soit scindé à racines simples	273
* 4.60. Condition suffisante pour qu'un polynôme réel soit scindé à racines simples	274
4.61. Polynômes de Tchebychev . . . . .	277
* 4.62. Inégalités de Bernstein et de Markov . . . . .	280
4.63. Localisation des racines . . . . .	283
4.64. Théorème de Gauss-Lucas . . . . .	284
* 4.65. Application du théorème de Gauss-Lucas (1) . . . . .	286
4.66. Application du théorème de Gauss-Lucas (2) . . . . .	287
4.67. Application du théorème de Gauss-Lucas (3) . . . . .	288
4.68. Application du théorème de Gauss-Lucas (4) . . . . .	290
4.69. Construction d'un polynôme satisfaisant des conditions sur le module de ses valeurs . . . . .	291
4.70. Inégalité de Landau . . . . .	291

* 4.71. Inégalité de Mignotte . . . . .	292
4.72. Décomposition d'un polynôme en somme de polynômes de racines de module 1 . . . . .	294
4.73. Théorème d'Eneström-Kekeya . . . . .	295
4.74. Critère de Routh-Hurwitz pour le degré 3 . . . . .	296
4.75. Règle de Descartes . . . . .	297
4.76. Théorème de Sturm . . . . .	299
4.77. Irréductibilité dans $\mathbb{Z}[X]$ (1) . . . . .	300
4.78. Irréductibilité dans $\mathbb{Z}[X]$ (2) . . . . .	301
4.79. Irréductibilité dans $\mathbb{Z}[X]$ (3) . . . . .	302
4.80. Critère d'irréductibilité de Cohn . . . . .	303
4.81. Décomposition en éléments simples . . . . .	304
4.82. Une identité algébrique . . . . .	304
4.83. Inégalité de Bernstein . . . . .	306
4.84. Inversion de la matrice de Hilbert . . . . .	307
* 4.85. Fractions rationnelles prenant des valeurs entières sur $\mathbb{Z}$ . . . . .	309
4.86. Automorphismes de $K(X)$ . . . . .	311
4.87. Image de $\mathbb{R}$ ou $\mathbb{R}^2$ par un polynôme . . . . .	314
4.88. Ensemble des zéros d'un polynôme à plusieurs variables . . . . .	315
4.89. Réunion des zéros d'une famille dénombrable de polynômes . . . . .	315
* 4.90. Théorème de Cauchy-Davenport . . . . .	316
4.91. Polynômes à plusieurs variables à valeurs entières . . . . .	317
4.92. Somme de carrés dans $\mathbb{R}[X, Y]$ . . . . .	319
* 4.93. Polynômes strictement positifs sur $(\mathbb{R}_+)^3 \setminus \{0\}$ . . . . .	320
4.94. Applications de $\mathbb{R}^2$ dans $\mathbb{R}$ polynomiales par rapport à chaque variable . . . . .	322
* 4.95. Équations polynomiales dans $\mathbb{F}_p$ . . . . .	323
** 4.96. Polynômes harmoniques . . . . .	326
** 4.97. Irréductibilité dans $K[X_1, \dots, X_n]$ . . . . .	327
** 4.98. Un théorème de Bezout . . . . .	330
** 4.99. Équations homogènes dans $k$ et $k(X)$ . . . . .	332
** 4.100. Racines d'un polynôme dont les coefficients sont des séries formelles . . . . .	334

## 5. Espaces vectoriels. Algèbres

337

5.1. Liberté de familles de fonctions . . . . .	337
5.2. Liberté d'une famille d'exponentielles . . . . .	338
5.3. Liberté d'une famille de polynômes . . . . .	339
5.4. Indépendance des caractères d'un groupe fini . . . . .	340
5.5. Intersection de sous-espaces . . . . .	341
5.6. Supplémentaire commun . . . . .	342
5.7. Intersection d'un sous-espace et d'un hypercube . . . . .	344
** 5.8. Drapeaux . . . . .	345
5.9. Lemmes de factorisation . . . . .	348
5.10. Condition pour que $\text{rg } g \leq \text{rg } f$ . . . . .	349
5.11. Endomorphismes stabilisant les sous-espaces de dimension $k$ . . . . .	351
5.12. Endomorphismes tels que $(a, x, u(x))$ est liée pour tout $x$ . . . . .	351
5.13. Produit commutatif d'endomorphismes nilpotents . . . . .	352
5.14. Inégalité de Sylvester . . . . .	353

5.15. Pseudo-inverse . . . . .	355
5.16. Endomorphismes $u$ tels que $\text{Ker } u = \text{Im } u$ . . . . .	356
5.17. Endomorphismes $u$ tels que $\text{Ker } u \oplus \text{Im } u = E$ . . . . .	357
5.18. Décomposition de Fitting . . . . .	358
5.19. Endomorphismes tels que $E = \text{Ker } u \oplus \text{Im } u$ . . . . .	359
5.20. Images et noyaux de puissances . . . . .	360
* 5.21. Équivalence entre $\text{Ker } u \cap \text{Ker } v = \{0\}$ et $\text{Im } u + \text{Im } v = E$ . . . . .	361
5.22. Équation linéaire dans $\mathcal{L}(E)$ . . . . .	362
5.23. Somme et différence de deux projecteurs . . . . .	365
5.24. Projecteurs . . . . .	365
5.25. Combinaison linéaire de 3 projecteurs . . . . .	366
5.26. Une somme de projecteurs . . . . .	366
* 5.27. Endomorphismes de $\mathbb{C}[X]$ . . . . .	367
5.28. Commutant de la dérivation discrète dans $\mathbb{C}[X]$ . . . . .	370
5.29. Formule de Burnside . . . . .	371
* 5.30. Théorème de Maschke . . . . .	374
5.31. Groupes irréductibles . . . . .	375
* 5.32. Automorphismes de la $K$ -algèbre $\mathcal{L}(E)$ . . . . .	376
5.33. Simplicité de $\mathcal{L}(E)$ . . . . .	378
5.34. Idéaux à gauche de $\mathcal{L}(E)$ . . . . .	378
5.35. Idéaux à droite de $\mathcal{L}(E)$ . . . . .	380
5.36. Orthogonalité duale en dimension quelconque . . . . .	382
5.37. Cône positif . . . . .	383
5.38. Familles positivement génératrices . . . . .	384
5.39. Familles positivement génératrices de $E^*$ . . . . .	385
5.40. Caractérisation de $\mathbb{C}$ . . . . .	388
* 5.41. Théorème de Frobenius . . . . .	389
5.42. Sous-algèbres de dimension finie de $C^0(\mathbb{R}, \mathbb{R})$ . . . . .	391
5.43. Une sous-algèbre de $\mathbb{R}[X]$ . . . . .	392
5.44. Racine carrée de la dérivation . . . . .	393
5.45. Trace d'une algèbre . . . . .	393
5.46. $\Phi$ -dérivation (1) . . . . .	395
5.47. $\Phi$ -dérivation (2) . . . . .	396
5.48. $\Phi$ -dérivation (3) . . . . .	398
5.49. Étude d'une algèbre . . . . .	399
* 5.50. Théorème de Burnside sur les sous-algèbres irréductibles . . . . .	400
* 5.51. Paires de Weyl . . . . .	402