exercices de mathématiques

oraux x-ens

algèbre 1

Serge Francinou
Hervé Gianella
Serge Nicolas

CASSINI

EXERCICES DE MATHÉMATIQUES
ORAUX X-ENS

Enseignement des mathématiques

1. J.-Y. Ouvrard, *Probabilités I*
2. J. Hubbard, B. West, *Équations différentielles et systèmes dynamiques*
3. M. Cottrell, V. Genon-Catalot, Ch. Duhamel, Th. Meyre, *Exercices de probabilités*
4. F. Rouvière, *Petit guide de calcul différentiel à l'usage de la licence et de l'agrégation*
5. J.-Y. Ouvrard, *Probabilités II*
6. G. Zémor, *Cours de cryptographie*
7. A. Szpirglas, *Exercices d'algèbre*
8. B. Perrin-Riou, *Algèbre, arithmétique et Maple*
10. S. Francinou, H. Gianella, S. Nicolas, *Exercices des oraux X-ENS, Algèbre 1*
11. S. Francinou, H. Gianella, S. Nicolas, *Exercices des oraux X-ENS, Analyse 1*
12. S. Francinou, H. Gianella, S. Nicolas, *Exercices des oraux X-ENS, Algèbre 2*
13. S. Francinou, H. Gianella, S. Nicolas, *Exercices des oraux X-ENS, Analyse 2*
14. S. Francinou, H. Gianella, S. Nicolas, *Exercices des oraux X-ENS, Algèbre 3*
15. H. Krivine, *Exercices de mathématiques pour physiciens*
16. J. Jacod, Ph. Protter, *L'essentiel en théorie des probabilités*
17. M. Willem, *Analyse fonctionnelle élémentaire*
18. É. Amar, É. Matheron, *Analyse complexe*
19. B. Randé, *Problèmes corrigés. Concours 2002 et 2003 (MP)*
20. D. Perrin, *Mathématiques d'école*
21. B. Randé, *Problèmes corrigés. Concours 2004 (MP)*
22. P. Bourgade, *Olympiades internationales de mathématiques 1976-2005*
23. V. Prasolov, *Problèmes et théorèmes d'algèbre linéaire*

SERGE FRANCINOU
HERVÉ GIANELLA
SERGE NICOLAS

Exercices de mathématiques des oraux de l'École polytechnique et des Écoles normales supérieures

Algèbre. Tome I

Deuxième édition, revue et augmentée

CASSINI

SERGE FRANCINOU, ancien élève de l'École normale supérieure et agrégé de Mathématiques est actuellement professeur en classe préparatoire au lycée Henri IV.

HERVÉ GIANELLA, ancien élève de l'École normale supérieure et agrégé de Mathématiques est actuellement professeur en classe préparatoire au lycée Saint-Louis.

SERGE NICOLAS, ancien élève de l'École normale supérieure et agrégé de Mathématiques est actuellement professeur en classe préparatoire au lycée Henri IV.

ISBN 978-2-84225-132-1
(1ere édition, 2001, ISBN-10 : 2-84225-030-3, ISBN-13 : 978-2-84225-030-0)

© Cassini, Paris, 2007.

Table des matières

Introduction 1

Chapitre 1. Combinatoire 5

1.1. Nombres de Fibonacci 6
1.2. Nombre de dérangements (1) 7
1.3. Nombre de dérangements (2) 9
1.4. Nombre de dérangements (3) 10
1.5. Nombres de Catalan 12
1.6. Nombres de Bell 14
1.7. Cardinal d'une relation d'équivalence 16
1.8. Cardinal de $\mathrm{GL}_n(\mathrm{K})$ et $\mathrm{SL}_n(\mathrm{K})$ 17
1.9. Cardinal de $\mathrm{SO}_2(\mathbb{Z}/p\mathbb{Z})$ 17
1.10. Nombre d'involutions 19
1.11. Partitions d'un entier 20
1.12. Un problème de théorie extrémale des ensembles 24
1.13. Ensembles définis par récurrence 25
1.14. Théorème de Howie 27
1.15. Distribution du premier chiffre des puissances de 2 29
1.16. Un théorème de Gauss 31
1.17. Théorème de Beatty (1926) 33
1.18. Un exercice d'Olympiades 34

Chapitre 2. Théorie des groupes 37

2.1. Existence d'un idempotent 37
2.2. Groupes dont l'ensemble des sous-groupes est fini 38
2.3. Morphismes de $\mathbb{Q}$ dans $\mathbb{Z}$ 38
2.4. Équivalence $\operatorname{Ker} f = \operatorname{Ker} f^2 \iff \operatorname{Im} f = \operatorname{Im} f^2$ 39
2.5. Sous-groupes finis de $\mathbb{Q}/\mathbb{Z}$ 40
2.6. Groupes abéliens de cardinal pq 41
2.7. Un cas particulier du lemme de Cauchy 41
2.8. Exposant d'un groupe abélien fini 43
2.9. Puissances dans un groupe abélien d'exposant fini 44
2.10. Lemme de Cauchy 46
2.11. Centre d'un p-groupe 47
2.12. Nombre de classes de conjugaison 49
2.13. Sous-groupe d'indice infini 50
2.14. Un théorème de Frobenius (1895) 52
2.15. Classes de conjugaison 53

2.16. Sous-groupes finis de $SO_3(\mathbb{R})$ 54
2.17. Groupe dérivé 57
2.18. Groupes quasi-cycliques de Prüfer 59
2.19. Le groupe modulaire 60
2.20. Unicité dans le théorème de structure des groupes abéliens finis 64
2.21. Génération du groupe symétrique 67
2.22. Plongement de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$ 68
2.23. Morphismes d'un sous-groupe de $\mathcal{S}_p$ dans $\mathbb{Z}/p\mathbb{Z}$ 69
2.24. Morphismes de $\mathcal{S}_4$ dans $\mathcal{S}_3$ 70
2.25. Automorphismes de $\mathcal{S}_n$ 74
2.26. Structure de groupe ordonné sur $\mathbb{Z}^2$ 78

Chapitre 3. Anneaux et corps **81**

3.1. Inversibilité à droite 82
3.2. Calcul d'inverse 83
3.3. Anneaux tels que $x^3 = x$ 84
3.4. Commutativité ou anti-commutativité 84
3.5. Anneaux réguliers 85
3.6. Idéaux principaux 87
3.7. Idéaux maximaux 88
3.8. Anneau des nombres décimaux 90
3.9. Anneau $\mathbb{Z}[X]$ 90
3.10. Anneaux factoriels 91
3.11. Anneaux euclidiens 94
3.12. Anneau des entiers de Gauss (1) 98
3.13. Anneau des entiers de Gauss (2) 100
3.14. Une extension quadratique de $\mathbb{C}[X]$ 104
3.15. Anneau sans idéal non premier 106
3.16. Automorphismes de $\mathbb{Q}(\sqrt{2})$ 106
3.17. Nombres algébriques 107
3.18. Valuations sur $\mathbb{Q}$ 110
3.19. Valeurs absolues non-archimédiennes sur $\mathbb{C}(X)$ 112
3.20. Indépendance des valeurs absolues sur $\mathbb{Q}$ 114

Chapitre 4. Arithmétique **117**

4.1. Étude de l'irréductibilité d'une fraction 118
4.2. Équation $a^b = b^a$ dans $\mathbb{N}$ 119
4.3. Divisibilité 120
4.4. Points du réseau $\mathbb{Z}^n$ visibles de l'origine 122
4.5. Produits d'entiers consécutifs 123
4.6. Parties de $\mathbb{N}$ additivement stables 124
4.7. Un exercice pour les années impaires 125

4.8. Équation du second degré dans $\mathbb{Z}/p\mathbb{Z}$ 126
4.9. Un problème de congruence 127
4.10. Un multiple de 1996 qui ne s'écrit qu'avec des 4 127
4.11. Somme des puissances k-ièmes dans $\mathbb{Z}/p\mathbb{Z}$ 127
4.12. Théorème de Wilson (1759) 128
4.13. Cyclicité du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ 129
4.14. Critères de primalité 130
4.15. Diviseurs premiers communs aux termes d'une suite arithmétique 131
4.16. Nombres de Fermat 132
4.17. Infinité des nombres premiers congrus à 3 modulo 4 134
4.18. Version faible du théorème de la progression arithmétique de Dirichlet (1837) 135
4.19. Plus petit nombre premier ne divisant pas n 137
4.20. Théorème de Kurschak (1918) 138
4.21. Théorème de Legendre (1808) 139
4.22. Un produit de trois entiers consécutifs n'est jamais une puissance k-ième 139
4.23. Théorème de Palfy-Erdös 140
4.24. Valuation p-adique de $C_{p^n}^k$ 143
4.25. Congruences de Lucas (1878) 144
4.26. Un problème de congruence 145
4.27. Le problème de Ducci 147
4.28. Expression de $\sum_{k=1}^{n} \tau(k)$ 150
4.29. Une majoration de σ 151
4.30. Équation faisant intervenir σ 151
4.31. Sur la fonction σ 152
4.32. Un théorème d'Erdös (1946) 153
4.33. Probabilité pour que deux entiers soient premiers entre eux 156
4.34. Écriture d'un nombre premier comme somme de deux carrés 158
4.35. Théorème des deux carrés, preuve combinatoire 160
4.36. Théorème des quatre carrés de Lagrange (1770) 162
4.37. Lemme de Davenport-Cassels 164
4.38. Une équation diophantienne 165
4.39. Théorème de Sophie Germain (1823) 167

Chapitre 5. Polynômes **171**

5.1. Égalité polynomiale 172
5.2. Une sous-algèbre de $\mathbb{R}[X]$ 173
5.3. Condition de divisibilité (1) 174
5.4. Condition de divisibilité (2) 174
5.5. Condition pour que $(P')^p$ divise P^q 175

5.6. Une équation fonctionnelle (1) 176
5.7. Une équation fonctionnelle (2) 177
5.8. Un théorème de Liouville (1879) 179
5.9. Théorème de Mason (1984) 180
5.10. Résultant de deux polynômes 182
5.11. Caractérisation d'un polynôme par les antécédents de deux points distincts 184
5.12. Image réciproque d'une partie finie par un polynôme 185
5.13. Sur le nombre d'antécédents d'un point par un polynôme . 186
5.14. Polynôme rationnel inséparable de degré 5 187
5.15. Un polynôme irréductible de $\mathbb{Z}[X]$ 188
5.16. Critère d'Eisenstein 188
5.17. Irréductibilité de Φ_p dans $\mathbb{Q}[X]$ 190
5.18. Décomposition de $1 + X + X^2 + \cdots + X^{n-1}$ 192
5.19. Polynômes complexes d'image réelle 193
5.20. Sommes de deux carrés dans $\mathbb{R}[X]$ 194
5.21. Polynômes positifs sur $[-1, 1]$ 195
5.22. Polynôme positif 197
5.23. Diviseurs d'un polynôme de $\mathbb{Z}[X]$ 197
5.24. Polynômes de Hilbert 198
5.25. Interpolation de Lagrange 199
5.26. Polynômes complexes envoyant surjectivement $\mathbb{Q}$ sur $\mathbb{Q}$ . . 200
5.27. Caractérisation des polygones réguliers 201
5.28. Polynômes entiers et fonctions polynomiales induites sur $\mathbb{Z}/p^i\mathbb{Z}$ 202
5.29. Images des racines d'un polynôme 206
5.30. Un calcul de $\zeta(2)$ 207
5.31. Formules de Newton (1707) 209
5.32. Polynômes réels scindés 211
5.33. Un théorème de Kronecker 213
5.34. Racines réelles de $nX^n - X^{n-1} - \cdots - X - 1$ 214
5.35. Un polynôme scindé sur $\mathbb{R}$ 215
5.36. Dénombrement de racines réelles 216
5.37. Dérivation et polynômes réels scindés 216
5.38. Un théorème de Laguerre 217
5.39. Plans vectoriels de polynômes scindés 219
5.40. L'ouvert des polynômes scindés à racines simples sur $\mathbb{R}$ dans l'ensemble des polynômes unitaires de degré n 221
5.41. Polynômes de Tchebychev 222
5.42. Inégalités de Bernstein et de Markov 225
5.43. Théorème de Gauss-Lucas 229
5.44. Polynôme à racines réelles 231
5.45. Théorème d'Eneström-Kakeya 233

5.46. Construction d'un polynôme satisfaisant des conditions sur le module de ses valeurs 234
5.47. Inégalité de Landau 234
5.48. Critère de Routh-Hurwitz pour le degré 3 235
5.49. Règle de Descartes 237
5.50. Théorème de Sturm 238
5.51. Décomposition en éléments simples 240
5.52. Inégalité de Bernstein 241
5.53. Inversion de la matrice de Hilbert 242
5.54. Automorphismes de K(X) 244
5.55. Approximation d'un irrationnel algébrique par des rationnels 247
5.56. Transcendance de e 249
5.57. Polynômes à plusieurs variables à valeurs entières 252
5.58. Applications de $\mathbb{R}^2$ dans $\mathbb{R}$ polynomiales par rapport à chaque variable 254
5.59. Un théorème de Bezout 255

Chapitre 6. Espaces vectoriels. Algèbres **259**

6.1. Intersection de sous-espaces 259
6.2. Supplémentaire commun 261
6.3. Drapeaux 263
6.4. Lemmes de factorisation 266
6.5. Condition pour que $\operatorname{rg} g \leqslant \operatorname{rg} f$ 267
6.6. Endomorphismes stabilisant les sous-espaces de dimension k 269
6.7. Exemple d'utilisation des espaces quotients 269
6.8. Majoration de l'indice de nilpotence 270
6.9. Produit commutatif d'endomorphismes nilpotents 271
6.10. Inégalité de Sylvester 272
6.11. Pseudo-inverse 274
6.12. Endomorphismes u tels que $\operatorname{Ker} u = \operatorname{Im} u$ 275
6.13. Endomorphismes u tels que $\operatorname{Ker} u \oplus \operatorname{Im} u = \mathrm{E}$ 276
6.14. Décomposition de Fitting 277
6.15. Endomorphismes tels que $\mathrm{E} = \operatorname{Ker} u \oplus \operatorname{Im} u$ 279
6.16. Endomorphisme annulé par un polynôme de degré 2 à racines simples 280
6.17. Équation linéaire dans $\mathcal{L}(\mathrm{E})$ 282
6.18. Projecteurs 284
6.19. Une somme de projecteurs 285
6.20. Endomorphismes de $\mathbb{C}[\mathrm{X}]$ 286
6.21. Formule de Burnside 289
6.22. Théorème de Maschke 292
6.23. Automorphismes de la K-algèbre $\mathcal{L}(\mathrm{E})$ 293
6.24. Simplicité de $\mathcal{L}(\mathrm{E})$ 295

6.25. Idéaux à gauche de $\mathcal{L}(E)$ 295
6.26. Idéaux à droite de $\mathcal{L}(E)$ 297
6.27. Orthogonalité duale en dimension quelconque 299
6.28. Familles libres d'applications 300
6.29. Familles positivement génératrices 302
6.30. Familles positivement génératrices de E^* 304
6.31. Caractérisation de $\mathbb{C}$ 307
6.32. Théorème de Frobenius 308
6.33. Sous-algèbres de dimension finie de $\mathcal{C}^0(\mathbb{R},\mathbb{R})$ 310
6.34. Racine carrée de la dérivation 311
6.35. Φ-dérivation (1) 311
6.36. Φ-dérivation (2) 312
6.37. Φ-dérivation (3) 314
6.38. Étude d'une algèbre 315

Chapitre 7. Matrices **319**

7.1. Condition pour que $\operatorname{rg} g \leqslant \operatorname{rg} f$ 320
7.2. Factorisation bilatère 321
7.3. Fonctions multiplicatives et inversibilité 322
7.4. Degré et valuation du polynôme $\det(XA + B)$ 322
7.5. Endomorphismes de $\mathcal{M}_n(\mathbb{C})$ stabilisant le groupe linéaire . . 323
7.6. Endomorphismes de $\mathcal{M}_n(\mathbb{C})$ conservant le rang 325
7.7. Équation matricielle $X + {}^tX = (\operatorname{Tr} X)A$ 328
7.8. Dual de $\mathcal{M}_n(K)$ 329
7.9. Tout hyperplan de $\mathcal{M}_n(K)$ coupe $GL_n(K)$ 331
7.10. Dimension maximale de sous-espaces de matrices de rang $\leqslant p$ 331
7.11. Orthogonalité duale 335
7.12. Crochets de Lie de $\mathcal{M}_n(K)$ 336
7.13. Diagonales possibles dans une classe de similitude 337
7.14. Traces modulo p 339
7.15. Matrices monotones 341
7.16. Puissances d'une matrice strictement stochastique 343
7.17. Théorème de Frobenius-König (1912-1916) 345
7.18. Décomposition de Bruhat et drapeaux 347
7.19. Bases d'un groupe abélien 350
7.20. Première colonne d'une matrice inversible de $\mathcal{M}_n(\mathbb{Z})$ 352
7.21. Matrices équivalentes dans $\mathcal{M}_n(\mathbb{Z})$ 354
7.22. Structure des groupes abéliens finis 358
7.23. Lemme de Siegel 360

Index **369**

Introduction

Cet ouvrage est le premier des six tomes d'un recueil d'exercices de mathématiques destiné à la préparation des oraux des concours d'entrée aux Écoles normales supérieures et à l'École polytechnique. Trois volumes seront consacrés à l'algèbre et trois à l'analyse.

La vocation première des Écoles normales est de former des chercheurs ou des enseignants-chercheurs. Le concours d'entrée vise donc à détecter les qualités scientifiques du candidat, son aptitude à la recherche. À l'oral, on jugera avant tout la capacité de prendre des initiatives, d'utiliser une indication, de mener à bien une démarche. On ne sera pas surpris que les exercices posés aient un contenu mathématique riche, qu'ils soient très éloignés du simple exercice technique, d'application du cours, qu'ils soient souvent difficiles. Ils visent la plupart du temps à la démonstration d'un résultat mathématique significatif. Ils pourraient apparaître excessivement difficiles, si on perdait de vue le déroulement concret de l'épreuve. L'oral des ENS est un long dialogue (l'épreuve dure environ cinquante minutes, comme d'ailleurs à l'École polytechnique) entre le candidat et l'examinateur, qui tout au long de l'épreuve fournit des indications, quand c'est nécessaire, pour relancer la réflexion du candidat et tester ses réactions. Il est d'ailleurs impossible de rendre pleinement compte dans un recueil d'exercices du caractère oral de l'épreuve.

L'École polytechnique, quant à elle, est plus généraliste. Les exercices posés au concours sont de facture plus classique et, en règle générale, l'examinateur intervient moins. C'est au candidat de montrer sa maîtrise du programme dans la résolution d'un exercice dont la difficulté est cependant très variable. Certains sont proches des exercices d'ENS. Les énoncés circulent d'ailleurs d'un concours à l'autre, ou peuvent même être repris d'exercices d'Olympiades.

Les énoncés qui figurent dans ce recueil, ont été donnés entre 1994 et 2006. Ils sont extraits pour l'essentiel des listes publiées chaque année par la RMS (*Revue des mathématiques de l'enseignement supérieur* aux éditions Vuibert jusqu'en 2003 et désormais *Revue de la filière Mathématiques* aux éditions e.net) dont nous remercions les auteurs pour l'aide précieuse qu'ils apportent ainsi aux élèves et aux professeurs des classes préparatoires. Il s'agit de versions communiquées par les étudiants, reflétant la compréhension que ceux-ci ont eue de l'exercice et le déroulement conjoncturel de leur oral, comme le montrent les variations d'une année à l'autre pour un même exercice. Nous n'avons pas hésité à les modifier, pour rectifier des erreurs, compléter un énoncé

quand manifestement l'exercice s'est arrêté avant que le résultat que l'examinateur avait en vue ne soit atteint, ou ajouter des indications.

Nous avons choisi de laisser quelques énoncés «bruts», ceux pour lesquels nous estimons qu'une démarche naturelle (qui peut être longue et ardue) permet de conduire à la solution. Pour d'autres exercices, nous avons pris la liberté de rajouter des questions intermédiaires, qui auraient pu être celles posées par l'examinateur. Quitte à perdre en concision, nous avons tenu à rédiger les solutions les plus pédagogiques possible, essayant d'exposer clairement les idées et démarches de raisonnement, sans escamoter les détails ou calculs qui peuvent paraître évidents. On évite autant que possible l'introduction d'une astuce ou d'un objet *ad hoc* permettant d'atteindre rapidement la solution. S'il n'y a pas moyen d'expliquer l'origine de cette astuce, c'est que l'exercice est peu intéressant et que l'étudiant en tirera peu de profit.

À l'intérieur de chaque chapitre, les exercices ont été regroupés thématiquement et à l'intérieur de chaque thème, souvent par ordre de difficulté croissante. Ainsi regroupés, ils apparaîtront plus accessibles, car plongés dans leur contexte mathématique, éclairés par d'autres exercices voisins. Les introductions historiques qui ouvrent chaque chapitre, outre leur intérêt propre, visent au même but. Enfin, nous avons agrémenté les énoncés de quelques remarques préliminaires. Sans faire de rappels de cours systématiques, nous avons énoncé, voire redémontré, certains résultats : lemmes classiques, intervenant dans la résolution d'un grand nombre d'exercices, ou résultats au contraire à la lisière du programme, mais utiles, pour lesquels des éclaircissements étaient nécessaires. On trouvera aussi des remarques de synthèse ou des généralisations qui, nous l'espérons, pourront amener le candidat curieux à approfondir ses connaissances. Les quelques indications bibliographiques ont le même objectif.

Le lecteur ne tirera profit de ce livre que s'il cherche des solutions personnelles des exercices avant d'en étudier les corrigés. Une bonne connaissance du cours est indispensable. En effet, les théorèmes du programme fournissent bon nombre de schémas de démonstration. Rappelons aussi quelques démarches générales qui peuvent faciliter l'appréhension des exercices difficiles :

▷ l'étude de cas particuliers permet souvent d'entrevoir les idées qu'il faudra mettre en œuvre dans la résolution du cas général. Ce peut être l'étude du problème pour les petites dimensions, dans un exercice d'algèbre linéaire, l'étude du problème dans $\mathbb{Z}$ pour un exercice où il est question d'un anneau quelconque... ;

▷ le renforcement des hypothèses peut aboutir à un problème plus simple : cas où le corps est algébriquement clos, s'il est question d'un corps K ou d'un K-espace vectoriel ; cas où les matrices sont diagonali-

sables dans un exercice d'algèbre linéaire ; étude du cas où la fonction f est supposée dérivable au lieu d'être seulement continue en analyse... ;

▷ parfois, l'étude de certains cas particuliers permet d'atteindre le cas général : problème linéaire qu'il suffit de traiter sur une base ; passage au cas général par des arguments de densité...

Au-delà des étudiants en classe préparatoire, ces ouvrages intéresseront aussi les candidats au CAPES et à l'Agrégation, qui y trouveront matière à réviser les principales notions du programme, ainsi que des exemples pour nourrir un développement pour leur oral.

Ce premier tome est consacré à l'algèbre générale (combinatoire, groupe, anneaux, corps, arithmétique, polynômes) et aux éléments de base de l'algèbre linéaire (espaces vectoriels, matrices). Il couvre de manière assez complète le programme d'algèbre des classes préparatoires scientifiques et pourra déjà être utilisé par des élèves de première année. La matière des différents chapitres est assez classique, sauf peut-être le premier qui fait appel à des techniques assez diverses. Le second tome d'algèbre contiendra la réduction, l'algèbre bilinéaire et multilinéaire et la géométrie. Enfin le troisième et dernier tome d'algèbre portera sur les espaces euclidiens, les espaces hermitiens, les formes quadratiques et la géométrie.

Nous remercions André Bellaïche, René Cori et Rached Mneimné, ainsi que nos élèves, pour leur relecture approfondie de l'ouvrage et leurs nombreuses suggestions, tant sur le fond que sur la forme.

Outre les notations habituelles, indiquons que $\mathrm{E}(x)$ désigne la partie entière du réel x et que le cardinal d'un ensemble fini X est noté indifféremment $\mathrm{Card}\,\mathrm{X}$ ou $|\mathrm{X}|$. Nous avons choisi de conserver la notation de Pascal C_n^k pour désigner les coefficients binomiaux plutôt que la notation anglo-saxonne $\binom{n}{k}$.

Enfin, si vous souhaitez nous contacter pour nous faire part de vos remarques, vous pouvez envoyer un courriel à l'adresse *fgn.cassini@free.fr*.

Chapitre 1
Combinatoire

L'Analyse combinatoire (ou plus brièvement la combinatoire) est la partie des Mathématiques qui s'occupe des configurations finies. Par nature, elle intervient dans de nombreuses branches des Mathématiques : arithmétique, théorie des graphes, théorie des groupes... Les techniques utilisées sont très variées : séries génératrices, analyse asymptotique...

Les exercices qui suivent traitent essentiellement du dénombrement, qui consiste à déterminer le nombre de configurations possibles d'un certain type : nombre de bijections sans point fixe d'un ensemble de cardinal n, nombre de matrices inversibles de taille n sur un corps fini... À la base du dénombrement se trouve l'étude de structures élémentaires : nombre d'éléments d'un produit cartésien, d'une réunion, nombre d'arrangements, de combinaisons – qui ont donné leur nom à la combinatoire.

La méthode la plus naturelle pour dénombrer un ensemble de configurations consiste à établir une bijection entre cet ensemble et un ensemble dont le nombre d'éléments est déjà connu. Mais ce n'est pas toujours la plus facile. Donnons un exemple où il s'agit non pas d'effectuer un dénombrement, mais d'établir une identité. Pour montrer que dans un ensemble E, *il y a autant de sous-ensembles de cardinal pair que de sous-ensembles de cardinal impair, on peut utiliser la formule du binôme de Newton :*

$$0 = (1-1)^n = \sum_{k=0}^{n} (-1)^k \mathrm{C}_n^k = \sum_{k \text{ pair}} \mathrm{C}_n^k - \sum_{k \text{ impair}} \mathrm{C}_n^k.$$

On peut aussi établir une bijection entre l'ensemble des sous-ensembles de E *de cardinal pair et celui des sous-ensembles de cardinal impair, par exemple comme ceci : on fixe $a \in \mathrm{E}$; à* A *on associe $\mathrm{A} \setminus \{a\}$ si* A *contient a, $\mathrm{A} \cup \{a\}$ sinon. De telles démonstrations où les égalités d'entiers traduisent des bijections entre ensembles finis sont appelées «démonstrations combinatoires».*

Dans les cas où un dénombrement exact est impossible, on s'intéressera à une évaluation asymptotique du nombre de structures.

Les exercices proposés dans ce chapitre concernent des sujets très variés et illustrent plusieurs techniques combinatoires importantes. Ils sont en général assez difficiles.

Le premier exercice voit apparaître la célèbre suite de Fibonacci.

Léonard de Pise, plus connu sous le nom de Leonardo Fibonacci est un des rares mathématiciens du Moyen Âge qui soit passé à la postérité. C'est dans le Liber Abacci. *écrit en 1202, qu'apparaît la suite qui porte son nom. Cet ouvrage remarquable, qui a introduit l'usage des chiffres arabes en Europe, réunissait presque toutes les connaissances en arithmétique et en algèbre de l'époque. La suite de Fibonacci a révélé par la suite de multiples propriétés extraordinaires. On la rencontre aussi bien en botanique en comptant les pétales des fleurs ou les écailles des ananas (c'est la phyllotaxie), que sur les marchés financiers où les analystes graphiques essaient de s'en servir pour prévoir l'amplitude des mouvements de hausse ou de baisse d'une action (ratio de Fibonacci). Elle apparaît dans l'exercice suivant, qui fournit un premier exemple de situation combinatoire où l'on utilise un raisonnement par récurrence. De telles situations se rencontrent chaque fois qu'il est possible de construire les configurations de rang n à partir de configurations de rang inférieur, ce qui est fréquent en combinatoire. Historiquement, c'est d'ailleurs pour donner une preuve solide de la formule des combinaisons (donnant la valeur de C_n^k) que Pascal a formulé pour la première fois de façon claire le principe de la démonstration par récurrence.*

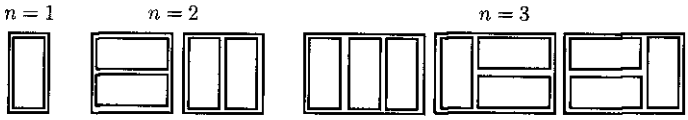
1.1. Nombres de Fibonacci

Déterminer le nombre a_n de manières de recouvrir un damier de dimension $2 \times n$ avec des pièces de dimension 1×2. Montrer que si n est assez grand, a_n est la partie entière de $\frac{1}{2} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$.

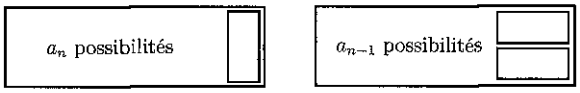
(École polytechnique)

▷ **Solution.**

On va effectuer ce dénombrement en établissant une relation de récurrence. Les configurations ci-dessous montrent que $a_1 = 1$, $a_2 = 2$ et $a_3 = 3$.



On partitionne l'ensemble des dispositions dans un échiquier de taille $n+1$ selon que la case $(1, n+1)$ est recouverte par un domino vertical ou horizontal. Dans le premier cas il reste à recouvrir un échiquier de taille $2 \times n$ ce qu'on peut faire de a_n manières. Dans le second cas, le domino qui recouvre la case $(2, n+1)$ est lui aussi horizontal et on a a_{n-1} possibilités de recouvrir l'échiquier $2 \times (n-1)$ restant.



La suite (a_n) vérifie donc la relation de récurrence $a_{n+1} = a_n + a_{n-1}$. On peut poser $a_0 = 1$ et on reconnaît alors, à un décalage d'indice près, la suite de Fibonacci. L'équation caractéristique associée à cette suite récurrente linéaire est $x^2 - x - 1 = 0$ et ses racines sont $\Phi = \dfrac{1+\sqrt{5}}{2}$, le nombre d'or[1] et $-\dfrac{1}{\Phi}$. On obtient alors, en tenant compte des conditions initiales, la formule[2]

$$\begin{aligned} a_n &= \frac{1}{\sqrt{5}}\left(\Phi^{n+1} - \left(-\frac{1}{\Phi}\right)^{n+1}\right) \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right). \end{aligned}$$

Comme $u_n = \dfrac{1}{2} + \dfrac{1}{\sqrt{5}}\left(\dfrac{1+\sqrt{5}}{2}\right)^{n+1} - a_n$ tend vers $\dfrac{1}{2}$, la partie entière de u_n est nulle pour n assez grand. Or celle-ci vérifie l'égalité

$$\mathrm{E}(u_n) = \mathrm{E}\left(\frac{1}{2} + \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}\right) - a_n.$$

D'où le résultat de la seconde question. ◁

Nous abordons maintenant le classique problème des dérangements posé pour la première fois en 1708 par Pierre Rémond de Montmort dans son livre Essai d'analyse sur les jeux de hasard *: si n personnes quittant une réunion, prennent au vestiaire un parapluie au hasard, quelle est la probabilité pour que personne n'ait son propre parapluie ? Nous allons aborder ce problème de plusieurs manières différentes. Le premier énoncé en propose une résolution élémentaire.*

1.2. Nombre de dérangements (1)

1. Calculer $\displaystyle\sum_{k=0}^{p} (-1)^k \mathrm{C}_n^k \mathrm{C}_{n-k}^{p-k}$ pour $0 \leqslant p \leqslant n$.

1. Ainsi noté en l'honneur du grec Phidias (Ve siècle avant notre ère) qui décora notamment le Parthénon.
2. Dite formule de Binet (1843) mais injustement dénommée puisque Euler l'avait déjà découverte en 1765.

2. Soit D_n le nombre de permutations de $\mathcal{S}_n$ n'ayant pas de point fixe. Montrer que $\sum_{k=0}^{n} C_n^k D_{n-k} = n!$ (on pose $D_0 = 1$).

3. Montrer que $D_n = n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right)$.

(**École polytechnique**)

▷ **Solution.**

1. On a

$$\begin{aligned}\sum_{k=0}^{p}(-1)^k C_n^k C_{n-k}^{p-k} &= \sum_{k=0}^{p}(-1)^k \frac{n!(n-k)!}{k!(n-k)!(p-k)!(n-p)!}\\ &= \sum_{k=0}^{p}(-1)^k C_n^p C_p^k\\ &= C_n^p(1-1)^p = \begin{cases} 0 \text{ si } p \geqslant 1\\ 1 \text{ si } p = 0\end{cases}\end{aligned}$$

2. Soit $n \geqslant 1$. Notons P_k l'ensemble des permutations de $\mathcal{S}_n$ ayant exactement k points fixes. Il est clair que $\{P_0, P_1, \ldots, P_n\}$ est une partition de $\mathcal{S}_n$. En particulier $n! = \sum_{k=0}^{n} \mathrm{Card}(P_k)$. Nous allons montrer que $\mathrm{Card}(P_k) = C_n^k D_{n-k}$ pour tout k. On a par définition $\mathrm{Card}(P_0) = D_n$ et $\mathrm{Card}(P_n) = 1 = C_n^n D_0$, car seule l'identité possède n points fixes. Pour $k \geqslant 1$, un élément de P_k est parfaitement déterminé par le choix de ses points fixes (C_n^k possibilités) et par le choix de la permutation induite sur les $n-k$ éléments restants (D_{n-k} possibilités puisque cette permutation est un dérangement d'un ensemble à $n-k$ éléments). Remarquons en passant que $D_1 = 0$ et que effectivement P_{n-1} est vide : une permutation ne peut avoir exactement $n-1$ points fixes ! On a donc

$$\boxed{n! = \sum_{k=0}^{n} C_n^k D_{n-k} = \sum_{k=0}^{n} C_n^k D_k}.$$

3. On part du membre de droite de l'égalité demandée. On a

$$n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) = \sum_{k=0}^{n}(-1)^k C_n^k (n-k)! = \sum_{k=0}^{n}(-1)^k C_n^k \sum_{p=0}^{n-k} C_{n-k}^p D_p$$

en remplaçant le terme $(n-k)!$ par la formule obtenue dans la question 2. En échangeant l'ordre de sommation, on obtient grâce à la question 1,

$$n!\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right)=\sum_{p=0}^{n}\left(\sum_{k=0}^{n-p}(-1)^k\mathrm{C}_n^k\mathrm{C}_{n-k}^p\right)\mathrm{D}_p=\mathrm{D}_n.\ \lhd$$

Une seconde possibilité, pour aboutir directement à cette dernière relation, consiste à utiliser la formule du crible (celle-ci est rappelée dans la solution de l'exercice 4.33). En effet, si on note U_i *l'ensemble des permutations de* $\mathcal{S}_n$ *fixant l'entier* i*, pour* $1 \leqslant i \leqslant n$*, on obtient* $\mathrm{D}_n = n! - \mathrm{Card}\left(\bigcup_{i=1}^{n}\mathrm{U}_i\right)$*. Le cardinal de la réunion s'évalue alors facilement à l'aide de la formule du crible. Nous invitons le lecteur à achever ce calcul.*

Dans l'exercice suivant, l'utilisation des séries entières fournit une troisième voie pour inverser le système linéaire donné par les relations de la question 2 ci-dessus et obtenir la formule de la question 3.

1.3. Nombre de dérangements (2)

On note toujours D_n le nombre de permutations d'un ensemble à n éléments n'ayant pas de point fixe.

1. Calculer $\sum_{k=0}^{n}\mathrm{C}_n^k\mathrm{D}_k$.

2. On considère la série entière $\sum_{k=0}^{+\infty}\frac{\mathrm{D}_k z^k}{k!}$, (on l'appelle série *génératrice exponentielle* de la suite $(\mathrm{D}_n)_{n\in\mathbb{N}}$). On note D sa somme. Minorer son rayon de convergence R. Calculer $\mathrm{D}(z)$ pour $|z| < \mathrm{R}$.

3. En déduire que D_k est la partie entière de $\frac{k!}{e}+\frac{1}{2}$.

(**École polytechnique**)

▷ **Solution.**

1. Voir la solution dans l'exercice précédent : $\sum_{k=0}^{n}\mathrm{C}_n^k\mathrm{D}_k = n!$.

2. On a évidemment $0 \leqslant \frac{\mathrm{D}_k}{k!} \leqslant 1$, donc le rayon de la série entière définissant $\mathrm{D}(z)$ est supérieur ou égal à 1.

Pour calculer $\mathrm{D}(z)$ on utilise la relation précédente. Elle peut s'écrire, pour tout $n \in \mathbb{N}$, $n! = \sum_{k=0}^{n}\frac{n!}{k!(n-k)!}\mathrm{D}_k$, ou encore $1 = \sum_{k=0}^{n}\frac{\mathrm{D}_k}{k!}\frac{1}{(n-k)!}$. On reconnaît le coefficient d'ordre n du produit de Cauchy des séries entières $\sum\frac{\mathrm{D}_k}{k!}z^k$ et $\sum\frac{1}{k!}z^k$. On en déduit que pour $|z| < 1$,

$$\mathrm{D}(z)e^z = \sum_{n=0}^{+\infty} z^n = \frac{1}{1-z}$$

d'où l'on tire, $D(z) = \dfrac{e^{-z}}{1-z}$ (c'est ici que s'effectue l'inversion). Il ne reste plus qu'à développer en série entière pour obtenir D_k. On a, pour tout $z \in \mathbb{C}$, $e^{-z} = \sum\limits_{k=0}^{+\infty} \dfrac{(-1)^k}{k!} z^k$. Il en résulte que pour tout $k \in \mathbb{N}$, $\dfrac{D_k}{k!} = \sum\limits_{p=0}^{k} \dfrac{(-1)^p}{p!}$. C'est bien le résultat obtenu dans l'exercice précédent.

3. On a, d'après ce qui précède, $\dfrac{1}{e} = \sum\limits_{p=0}^{+\infty} \dfrac{(-1)^p}{p!} = \dfrac{D_k}{k!} + R_k$, où $R_k = \sum\limits_{p=k+1}^{+\infty} \dfrac{(-1)^p}{p!}$. Ainsi, $\dfrac{k!}{e} + \dfrac{1}{2} = D_k + \dfrac{1}{2} + k!R_k$. La série $\sum \dfrac{(-1)^p}{p!}$ vérifiant le critère des séries alternées, on sait que $|R_k| \leqslant \dfrac{1}{(k+1)!}$. Pour $k \geqslant 1$, on a donc $|k!R_k| < \dfrac{1}{k+1} \leqslant \dfrac{1}{2}$ et donc

$$\boxed{D_k = E\left(\frac{k!}{e} + \frac{1}{2}\right)}.$$

La formule est par ailleurs aussi vérifiée au rang $k = 0$. $\lhd$

Remarquons que la proportion de dérangements $\dfrac{D_n}{n!}$ *tend vers le nombre* $\dfrac{1}{e} = 0{,}368...$ *lorsque* n *tend vers l'infini. En particulier le rayon de convergence de la série entière* D *ci-dessus est* e.

Dans l'exercice suivant on établit de manière combinatoire, une autre relation de récurrence qui permet le calcul de D_n.

1.4. Nombre de dérangements (3)

Les notations sont les mêmes que dans les deux exercices précédents.

1. Établir, par une preuve combinatoire, que pour tout $n \geqslant 2$,

$$D_{n+1} = n(D_n + D_{n-1}).$$

2. En déduire que pour tout $n \geqslant 2$, $D_n = nD_{n-1} + (-1)^n$.

3. Retrouver la valeur de D_n.

(École polytechnique)

$\rhd$ **Solution.**

1. Soit $\mathcal{D}_n$ l'ensemble des dérangements de $[\![1, n]\!]$. Si $\sigma \in \mathcal{D}_{n+1}$, l'image de $n+1$ par σ est dans $[\![1, n]\!]$. Pour tout $k \in [\![1, n]\!]$, on note

F_k l'ensemble des éléments σ de $\mathcal{D}_{n+1}$ tels que $\sigma(n+1) = k$. Les F_k partitionnent $\mathcal{D}_{n+1}$.

Nous allons prouver que le cardinal de F_k est égal à $D_n + D_{n-1}$ quel que soit l'entier k. On fixe donc k et on partitionne F_k en deux : G_k désigne l'ensemble des $\sigma \in F_k$ tels que $\sigma(k) = n+1$ et H_k désigne le complémentaire de G_k dans F_k. Il est clair qu'un élément de G_k est parfaitement déterminé par sa restriction à l'ensemble $\{1, \ldots, k-1, k+1, \ldots, n\}$, cette restriction devant être un dérangement. Il en résulte que $\mathrm{Card}(G_k) = D_{n-1}$. Cherchons maintenant le cardinal de H_k. Soit $\sigma \in H_k$. Alors $\sigma^{-1}(n+1) \neq k$. Considérons le dérangement $\tilde{\sigma}$ de $[\![1, n]\!]$ défini par $\tilde{\sigma}(i) = \sigma(i)$ pour $i \neq \sigma^{-1}(n+1)$, et $\tilde{\sigma}(\sigma^{-1}(n+1)) = k$ (on a simplement «court-circuité» $n+1$). Il est clair que l'application de H_k dans $\mathcal{D}_n$ qui à σ associe $\tilde{\sigma}$ est bijective de sorte que $\mathrm{Card}(H_k) = D_n$. On obtient donc $\mathrm{Card}(F_k) = D_{n-1} + D_n$, pour tout k, ce qui donne la relation de récurrence $D_{n+1} = n(D_n + D_{n-1})$.

2. On effectue une récurrence sur n, le résultat étant vrai pour $n = 2$ puisque $D_2 = 1$ et $D_1 = 0$. Supposons la formule vraie au rang n. On a alors

$$\begin{aligned} D_{n+1} &= n(D_n + D_{n-1}) = nD_n + nD_{n-1} \\ &= nD_n + D_n - (-1)^n = (n+1)D_n + (-1)^{n+1}, \end{aligned}$$

ce qui est la formule au rang $n+1$.

3. En divisant la relation précédente par $n!$ il vient, pour tout $n \geqslant 2$, $\dfrac{D_n}{n!} = \dfrac{D_{n-1}}{(n-1)!} + \dfrac{(-1)^n}{n!}$. En sommant cette relation pour les indices $2, 3, \ldots, n$, on retrouve la formule

$$D_n = n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right). \quad \lhd$$

Notons que les relations des questions 1 et 2 s'obtiennent facilement à partir de la série entière D *de l'exercice précédent. Il suffit pour cela de dériver la relation* $(1-z)D(z) = e^{-z}$. *Dans son ouvrage de combinatoire*[3], *Comtet suggère l'existence d'une preuve combinatoire directe de la relation de la question 2. Cela ne semble toutefois pas très facile...*

Dans l'exercice suivant, on rencontre les célèbres nombres de Catalan à travers le problème des parenthésages. C'est un exemple où l'emploi des séries génératrices se révèle incontournable.

3. COMTET (L.), *Analyse combinatoire*, tome 2. PUF, 1970, p. 11.

1.5. Nombres de Catalan

On considère un ensemble muni d'une loi de composition interne non associative et n éléments $a_1, \ldots, a_n$ de cet ensemble. Combien de valeurs différentes peut prendre le produit $a_1 a_2 \ldots a_n$?
(École Polytechnique)

▷ **Solution.**

Commençons par préciser l'énoncé. Pour calculer un produit de n éléments $a_1, \ldots, a_n$ on doit indiquer l'ordre dans lequel faire les opérations à l'aide d'un parenthésage, comme par exemple $((a_1(a_2a_3))a_4)$ pour $n = 4$. Bien entendu, pour des éléments donnés, il se peut que deux parenthésages distincts conduisent au même résultat : ainsi pour une loi associative, comme l'addition sur $\mathbb{R}$, tous les parenthésages donnent la même valeur ! L'énoncé demande en fait de calculer le nombre total de parenthésages du produit $a_1 a_2 \ldots a_n$. Il est en effet facile de construire une loi de composition interne pour laquelle deux parenthésages distincts conduisent toujours à deux produits distincts.

Nous noterons $\mathcal{C}_n$ ce nombre de parenthésages. On a clairement $\mathcal{C}_1 = \mathcal{C}_2 = 1$ et pour $n = 3$, on peut écrire $(a_1a_2)a_3$ ou $a_1(a_2a_3)$, donc $\mathcal{C}_3 = 2$. Pour $n \geqslant 2$, tout produit des a_i s'écrit d'une manière et d'une seule $(a_1 \ldots a_k)(a_{k+1} \ldots a_n)$ avec $1 \leqslant k \leqslant n-1$. En effet, il suffit de considérer le dernier produit effectué. Les deux termes qui forment ce dernier produit sont bien définis. Puisqu'il y a respectivement $\mathcal{C}_k$ parenthésages possibles pour le premier facteur $a_1 \ldots a_k$ et $\mathcal{C}_{n-k}$ pour le second facteur $a_{k+1} \ldots a_n$, il y a $\mathcal{C}_k\mathcal{C}_{n-k}$ parenthésages possibles où le premier facteur dans le dernier produit effectué contient k termes. On obtient donc

$$\mathcal{C}_n = \sum_{k=1}^{n-1} \mathcal{C}_k \mathcal{C}_{n-k}.$$

Cette relation fait penser à un produit de Cauchy. Il convient d'observer tout de même que la relation n'est pas valable pour $n = 1$. Considérons $f(x) = \sum_{n=1}^{+\infty} \mathcal{C}_n x^n$ la série entière génératrice des $\mathcal{C}_n$.

Analyse. Supposons que son rayon de convergence R soit différent de 0. Dans ces conditions, pour $x \in \mathbb{R}$, $|x| < \mathrm{R}$ on a

$$f(x)^2 = \sum_{n=2}^{+\infty} \left(\sum_{k=1}^{n-1} \mathcal{C}_k \mathcal{C}_{n-k} \right) x^n = \sum_{n=2}^{+\infty} \mathcal{C}_n x^n = f(x) - x.$$

Cette équation $f(x)^2 - f(x) + x = 0$ du second degré en $f(x)$ a un discriminant $\Delta = 1 - 4x$ et pour $x \leqslant \frac{1}{4}$, on aura donc $f(x) = \dfrac{1 + \varepsilon(x)\sqrt{1-4x}}{2}$.

avec $\varepsilon(x) = \pm 1$. Comme f est continue sur son intervalle ouvert de définition, il en est de même de ε qui est donc constante. Comme $f(0) = 0$, on a $\varepsilon(0) = -1$ et donc

$$f(x) = \frac{1 - \sqrt{1 - 4x}}{2}.$$

Synthèse. Considérons la fonction $f : x \longmapsto \dfrac{1 - \sqrt{1 - 4x}}{2}$ qui est développable en série entière en 0 avec un rayon de convergence égal à $\frac{1}{4}$. Elle vérifie $f(x)^2 - f(x) + x = 0$. Si on écrit $f(x) = \sum\limits_{n=1}^{+\infty} \mathrm{C}_n x^n$ son développement en série entière, la relation $f(x)^2 = f(x) - x$ donne, par unicité des coefficients, pour $n \geqslant 2$

$$\mathrm{C}_n = \sum_{k=1}^{n-1} \mathrm{C}_k \mathrm{C}_{n-k}.$$

Comme $f(x) = x + o(x)$ en 0, on en déduit que $\mathrm{C}_1 = 1 = \mathcal{C}_1$ et finalement par récurrence que $\mathrm{C}_n = \mathcal{C}_n$ pour tout $n \in \mathbb{N}^*$ et $\mathrm{R} = \dfrac{1}{4}$.

Pour l'expression de $\mathcal{C}_n$, dérivons f. Pour $|x| < \dfrac{1}{4}$, on a

$$f'(x) = \frac{1}{\sqrt{1 - 4x}} = (1 - 4x)^{-1/2}.$$

Le développement classique de $(1 - u)^\alpha$ donne en l'occurrence

$$\begin{aligned} f'(x) &= \sum_{n=0}^{+\infty} \left(-\frac{1}{2}\right)\left(-\frac{3}{2}\right)\cdots\left(-\frac{2n-1}{2}\right)\frac{(-4x)^n}{n!} \\ &= \sum_{n=0}^{+\infty} \frac{1}{2^n}\frac{(2n)!}{2.4\cdots(2n-2).(2n)}\frac{4^n x^n}{n!} = \sum_{n=0}^{+\infty} \frac{(2n)!}{4^n (n!)^2} 4^n x^n \\ &= \sum_{n=0}^{+\infty} \mathrm{C}_{2n}^n x^n. \end{aligned}$$

Comme $f(0) = 0$, on en déduit que $f(x) = \sum\limits_{n=0}^{+\infty} \dfrac{\mathrm{C}_{2n}^n}{n+1} x^{n+1}$. On aboutit à

$$\boxed{\mathcal{C}_n = \frac{\mathrm{C}_{2n-2}^{n-1}}{n}}. \quad \triangleleft$$

Les nombres de Catalan se rencontrent dans de nombreux problèmes de combinatoire. Par exemple, $\mathcal{C}_n$ est aussi le nombre de manières de

trianguler un polygone régulier à $n+1$ côtés ou encore le nombre d'arbres binaires à $n-1$ sommets.

L'exercice suivant s'intéresse au nombre de partitions d'un ensemble fini. C'est aussi le nombre de relations d'équivalence sur cet ensemble. On y fait encore usage de séries génératrices.

1.6. Nombres de Bell

Pour tout $n \in \mathbb{N}^*$, on note B_n le nombre de partitions de l'ensemble $[\![1, n]\!]$, avec par convention, $B_0 = 1$.

1. Calculer B_1, B_2, B_3.

Démontrer que, pour tout $n \in \mathbb{N}$, on a $B_{n+1} = \sum_{k=0}^{n} C_n^k B_k$.

2. On pose $f(z) = \sum_{n=0}^{+\infty} \frac{B_n}{n!} z^n$ (série génératrice exponentielle de la suite $(B_n)_{n \geqslant 0}$). Montrer que le rayon de convergence R de cette série entière n'est pas nul. Calculer $f(z)$ pour $z \in]-R, R[$.

3. Exprimer B_n comme somme d'une série.

(École polytechnique)

▷ **Solution.**

1. On obtient $B_1 = 1$, $B_2 = 2$, $B_3 = 5$. Pour $k \in [\![0, n]\!]$, considérons l'ensemble E_k des partitions de $[\![1, n+1]\!]$ pour lesquelles la partie de $[\![1, n+1[\![$ contenant $n+1$ est de cardinal $k+1$. On a $\operatorname{Card} E_k = C_n^k B_{n-k}$. En effet, pour constituer la partie contenant $n+1$, il faut choisir k élément dans $[\![1, n]\!]$, puis il faut réaliser une partition des $n-k$ éléments restants. Comme $E_0, E_1, \ldots, E_n$ forment une partition de l'ensemble des partitions de $[\![1, n+1]\!]$, on obtient

$$B_{n+1} = \sum_{k=0}^{n} C_n^k B_{n-k} = \sum_{j=0}^{n} C_n^j B_j,$$

en faisant le changement d'indice $j = n - k$ dans la seconde égalité.

2. Pour minorer le rayon de convergence de la série $\sum_{n \geqslant 0} \frac{B_n}{n!} z^n$ il faut majorer B_n. Montrons donc, par récurrence sur $n \in \mathbb{N}$, que $B_n \leqslant n!$. C'est vrai pour $n \leqslant 3$ et si la propriété est vérifiée jusqu'au rang n, alors

$$B_{n+1} \leqslant \sum_{k=0}^{n} C_n^k k! = n! \sum_{k=0}^{n} \frac{1}{(n-k)!} \leqslant (n+1)!.$$

On a donc, pour $n \in \mathbb{N}^*$, $\frac{B_n}{n!} \leqslant 1$ et le rayon de convergence R de la série entière est supérieur ou égal à 1.

Calculons $f(z)$, pour $z \in]-\mathrm{R}, \mathrm{R}[$ en utilisant la relation de récurrence démontrée dans 1. On a, pour $z \in]-\mathrm{R}, \mathrm{R}[$, $f(z) = 1 + \sum_{k=0}^{+\infty} \frac{\mathrm{B}_{n+1}}{(n+1)!} z^{n+1}$. La fonction f est dérivable sur $]-\mathrm{R}, \mathrm{R}[$ et $f'(z) = \sum_{n=0}^{+\infty} \frac{\mathrm{B}_{n+1}}{n!} z^n$. On en déduit que, pour $z \in]-\mathrm{R}, \mathrm{R}[$, on a

$$f'(z) = \sum_{n=0}^{+\infty} \frac{1}{n!} \left(\sum_{k=0}^{n} \mathrm{C}_n^k \mathrm{B}_k \right) z^n = \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{n} \frac{\mathrm{B}_k}{k!} \frac{1}{(n-k)!} \right) z^n.$$

On reconnaît dans le terme de droite un produit de Cauchy, celui des séries $\sum \frac{\mathrm{B}_n}{n!} z^n$ et $\sum \frac{z^n}{n!}$. La première a pour somme $f(z)$ et la seconde e^z. Elles ont toutes deux un rayon de convergence supérieur ou égal à R. On a donc, pour $z \in]-\mathrm{R}, \mathrm{R}[$, $f'(z) = f(z)e^z$. On en déduit qu'il existe $\mathrm{C} \in \mathbb{R}$ tel que, pour $z \in]-\mathrm{R}, \mathrm{R}[$, $f(z) = \mathrm{C}e^{e^z}$. Sachant que $f(0) = \mathrm{B}_0 = 1$, on en déduit que $\mathrm{C} = \frac{1}{e}$. Finalement, on obtient pour $z \in]-\mathrm{R}, \mathrm{R}[$,

$$\boxed{f(z) = \frac{1}{e} e^{e^z} = e^{e^z - 1}}.$$

3. La série entière définissant la fonction exponentielle ayant un rayon de convergence infini, on a, pour tout $z \in \mathbb{C}$,

$$e^{e^z} = \sum_{n=0}^{+\infty} \frac{e^{nz}}{n!} = \sum_{n=0}^{+\infty} \frac{1}{n!} \sum_{k=0}^{+\infty} \frac{(nz)^k}{k!}.$$

Considérons la série double $(u_{n,k})_{(n,k)\in\mathbb{N}^2}$ définie par $u_{n,k} = \frac{(nz)^k}{n!k!}$. On a, pour $n \in \mathbb{N}$,

$$\sum_{k=0}^{+\infty} |u_{n,k}| = \sum_{k=0}^{+\infty} \frac{|nz|^k}{n!k!} = \frac{e^{|nz|}}{n!},$$

puis

$$\sum_{n=0}^{+\infty} \frac{e^{|nz|}}{n!} = \sum_{n=0}^{+\infty} \frac{\left(e^{|z|}\right)^n}{n!} = e^{e^{|z|}}.$$

La série double est donc sommable, pour tout $z \in \mathbb{C}$. On peut donc échanger l'ordre des sommations et en déduire que, pour tout z de $]-\mathrm{R}, \mathrm{R}[$,

$$f(z) = \frac{1}{e} \sum_{n=0}^{+\infty} \left(\sum_{k=0}^{+\infty} u_{n,k} \right) = \frac{1}{e} \sum_{k=0}^{+\infty} \left(\sum_{n=0}^{+\infty} u_{n,k} \right) = \sum_{k=0}^{+\infty} \left(\sum_{n=0}^{+\infty} \frac{n^k}{n!} \right) \frac{z^k}{k!}.$$

D'après l'unicité du développement en série entière de f, on obtient, pour tout $k \in \mathbb{N}$,

$$\boxed{\mathrm{B}_k = \frac{1}{e}\sum_{n=0}^{+\infty} \frac{n^k}{n!}}. \lhd$$

Il résulte des calculs précédents que le rayon de convergence de la série entière définissant f est en fait infini. Cette formule peut servir de point de départ à l'étude asymptotique de la suite B_n. Le lecteur intéressé pourra par exemple étudier la première épreuve du concours Mines-Ponts de 2002 qui se propose d'obtenir un équivalent de B_n.

Voici maintenant un petit exercice facile qui concerne les relations d'équivalence.

1.7. Cardinal d'une relation d'équivalence

Soit A un ensemble de cardinal n, $\mathcal{R}$ une relation d'équivalence sur A avec k classes. Soit m le cardinal du graphe de $\mathcal{R}$. Montrer que $n^2 \leqslant km$.

(École polytechnique)

$\rhd$ **Solution.**

Notons $\mathrm{A}_1, \ldots, \mathrm{A}_k$ les différentes classes d'équivalence. On va commencer par expliciter les quantités n et m. Comme les classes d'équivalence partitionnent A on a déjà

$$n = \operatorname{Card} \mathrm{A} = \sum_{i=1}^{k} \operatorname{Card} \mathrm{A}_i.$$

D'autre part, si $\overline{x}$ désigne la classe d'équivalence d'un élément x de A, on a

$$\begin{aligned} m &= \operatorname{Card}\{(x,y) \in \mathrm{A}^2,\ (x,y) \in \mathcal{R}\} = \sum_{x \in \mathrm{A}} \operatorname{Card} \overline{x} \\ &= \sum_{i=1}^{k} \sum_{x \in \mathrm{A}_i} \operatorname{Card} \mathrm{A}_i = \sum_{i=1}^{k} (\operatorname{Card} \mathrm{A}_i)^2. \end{aligned}$$

L'inégalité demandée résulte alors de l'inégalité de Cauchy-Schwarz. $\lhd$

Le thème commun aux exercices qui suivent est l'algèbre linéaire sur des corps finis.

1.8. Cardinal de $GL_n(K)$ et $SL_n(K)$

Soit K un corps commutatif fini de cardinal q. Déterminer le cardinal de $GL_n(K)$ et celui de $SL_n(K)$.

(École normale supérieure)

▷ **Solution.**

Choisir une matrice inversible de taille n revient à choisir la famille $(C_1, \ldots, C_n)$ de ses n colonnes, famille qui constitue une base de K^n. Pour le choix de C_1, on a donc $q^n - 1$ possibilités : elle doit simplement être non nulle. Pour chacun de ces choix, on a $q^n - q$ possibilités pour la colonne C_2 (elle ne doit pas appartenir à la droite engendrée par C_1). Puis on a $q^n - q^2$ possibilités pour C_3 (elle ne doit pas être dans le plan $KC_1 \oplus KC_2$). Plus généralement, si $C_1, C_2, \ldots, C_{k-1}$ sont fixées, on a $q^n - q^{k-1}$ choix possibles pour C_k. En effet, il doit simplement être en dehors de l'espace $KC_1 \oplus \cdots \oplus KC_{k-1}$ et cet espace de dimension $k-1$ est de cardinal q^{k-1}. Finalement, on obtient

$$\boxed{|GL_n(K)| = (q^n - 1)(q^n - q)(q^n - q^2)\ldots(q^n - q^{n-1})}.$$

L'application det : $GL_n(K) \to K^*$ est un morphisme surjectif de groupes de noyau $SL_n(K)$. Nous savons alors (cela est redémontré dans l'exercice 2.4) que $|\operatorname{Im}\det| \times |\operatorname{Ker}\det| = |GL_n(K)|$, de sorte que

$$\boxed{|SL_n(K)| = \frac{(q^n - 1)(q^n - q)(q^n - q^2)\ldots(q^n - q^{n-1})}{q-1}}. \triangleleft$$

Dans l'exercice suivant on s'intéresse à l'analogue du groupe spécial orthogonal sur le corps $\mathbb{Z}/p\mathbb{Z}$.

1.9. Cardinal de $SO_2(\mathbb{Z}/p\mathbb{Z})$

Soit p un nombre premier. On note $SO_2(\mathbb{Z}/p\mathbb{Z})$ l'ensemble des matrices M de $\mathcal{M}_2(\mathbb{Z}/p\mathbb{Z})$ telles que ${}^tMM = I_2$ et $\det M = 1$. Soit u_p le cardinal de $SO_2(\mathbb{Z}/p\mathbb{Z})$. Montrer que $u_2 = 2$, que $u_p = p - 1$ si $p \equiv 1$ [4] et enfin que $u_p = p + 1$ si $p \equiv 3$ [4].

(École normale supérieure)

▷ **Solution.**

Soit $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(\mathbb{Z}/p\mathbb{Z})$. Alors $M \in SO_2(\mathbb{Z}/p\mathbb{Z})$ si et

seulement si $\det M = 1$ et $M^{-1} = {}^tM$. Or, si $\det M = 1$, M^{-1} est égale à la transposée de la comatrice de M, c'est-à-dire à la matrice $M' = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Ainsi, $M' = {}^tM$ équivaut à $a = d$ et $b = -c$. Finalement, M appartient à $SO_2(\mathbb{Z}/p\mathbb{Z})$ si et seulement si (a, b, c, d) vérifient le système

$$\begin{cases} a = d \\ b = c \\ ad - bc = 1, \end{cases} \quad \text{qui équivaut au système} \quad \begin{cases} a = d \\ b = c \\ a^2 + b^2 = 1. \end{cases}$$

On a donc une bijection entre $SO_2(\mathbb{Z}/p\mathbb{Z})$ et l'ensemble (qu'on a envie d'appeler «cercle») $S = \{(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2,\ a^2 + b^2 = 1\}$. Dans le cas réel, S est le cercle unité de $\mathbb{R}^2$ et en le paramétrant par $(\cos\theta, \sin\theta)$, $\theta \in \mathbb{R}$, on obtient l'écriture classique des matrices de rotation de taille $(2, 2)$. Évidemment ce paramétrage ne va pas nous servir ici. Cependant, le cercle admet un paramétrage rationnel très important qu'on retrouve à partir du précédent grâce aux formules trigonométriques donnant $\cos\theta$ et $\sin\theta$ en fonction de $t = \tan\dfrac{\theta}{2}$:

$$\cos\theta = \frac{1 - t^2}{1 + t^2} \text{ et } \sin\theta = \frac{2t}{1 + t^2}.$$

Plus précisément, lorsque t décrit $\mathbb{R}$, le point $M(t)$ de coordonnées $\left(\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2}\right)$ décrit bijectivement le cercle S privé du point $(-1, 0)$ (car $\theta = 2\arctan t$ décrit bijectivement l'intervalle $]-\pi, \pi[$).

On va examiner si on a encore cette bijection dans le cas du corps $\mathbb{Z}/p\mathbb{Z}$. Un problème survient du fait que la quantité $1 + t^2$ peut s'annuler (si -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$). Laissons de côté le cas $p = 2$ qui se traite directement : on a aisément dans ce cas $S = \{(0, 1); (1, 0)\}$ et donc $u_2 = 2$. On suppose dans la suite que p est un nombre premier impair et on distingue deux cas.

• Supposons que -1 n'est pas un carré dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire que $p \equiv 3\ [4]$ (voir exercice 4.34). Pour tout élément t de $\mathbb{Z}/p\mathbb{Z}$ on peut considérer le point $A(t) = \left(\dfrac{1 - t^2}{1 + t^2}, \dfrac{2t}{1 + t^2}\right)$. Il est aisé de vérifier que $A(t) \in S$ et que $A(t) \neq (-1, 0)$. Montrons que A est injective. Soit t, t' tels que $A(t) = A(t')$. On a $\dfrac{1 - t^2}{1 + t^2} = \dfrac{1 - t'^2}{1 + t'^2}$, ce qui conduit à $2t^2 = 2t'^2$. Comme 2 est inversible dans $\mathbb{Z}/p\mathbb{Z}$, on a $t^2 = t'^2$. En regardant les secondes coordonnées des points $A(t)$ et $A(t')$, on obtient alors $2t = 2t'$ soit $t = t'$. Donc A est une application injective. Soit $(x, y) \in S$ un point distinct de $(-1, 0)$. On cherche t tel que $A(t) = (x, y)$. L'équation

$\frac{1-t^2}{1+t^2} = x$ conduit à $t^2 = \frac{1-x}{1+x}$, ce qui est possible puisque $x \neq -1$. En substituant dans l'égalité $\frac{2t}{1+t^2} = y$, on obtient $t = \frac{y}{1+x}$. On vérifie réciproquement, que pour cette valeur de t on a $A(t) = (x, y)$. On en déduit que

$$u_p = |\mathbb{Z}/p\mathbb{Z}| + 1 = p + 1.$$

• Supposons maintenant que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire que $p \equiv 3\ [4]$ et notons $\pm\varepsilon$ ses deux racines carrées. L'application A restreinte à $\mathbb{Z}/p\mathbb{Z} \setminus \{\pm\varepsilon\}$ reste bien entendu injective et à valeurs dans $S \setminus \{(-1, 0)\}$. Elle reste en fait surjective, car si $(x, y) \in S \setminus \{(-1, 0)\}$, le réel $t = \frac{y}{1+x}$ obtenu précédemment vérifie $t^2 = \frac{1-x}{1+x} \neq -1$ de sorte que $t \notin \{\pm\varepsilon\}$. On a donc dans ce cas,

$$u_p = |\mathbb{Z}/p\mathbb{Z} \setminus \{\pm\varepsilon\}| + 1 = p - 1.$$

D'où le résultat. ◁

L'exercice suivant montre un exemple d'utilisation des opérations de groupes dans un problème combinatoire.

1.10. Nombre d'involutions

Soit K un corps fini de caractéristique différente de 2. Déterminer le nombre de matrices $A \in GL_n(K)$ telles que $A^2 = I_n$.

(École normale supérieure)

1. **Solution.**

• Soit $A \in GL_n(K)$ telle que $A^2 = I_n$. Comme la caractéristique de K est différente de 2, le polynôme $X^2 - 1$ est scindé à racines simples sur K. Il en résulte que A est diagonalisable avec $K^n = \mathrm{Ker}(A - I_n) \oplus \mathrm{Ker}(A + I_n)$. Autrement dit, A est la matrice de la symétrie par rapport au sous-espace $F = \mathrm{Ker}(A - I_n)$ parallèlement au sous-espace $G = \mathrm{Ker}(A + I_n)$. Soit alors f l'application qui à cette matrice A associe le couple des sous-espaces supplémentaires (F, G). Il est clair que f est injective (A est parfaitement déterminée par la connaissance des sous-espaces F et G) et que son image est exactement l'ensemble des couples de sous-espaces supplémentaires. L'exercice revient donc à dénombrer ces couples.

• Pour $p \in [\![0, n]\!]$ on note E_p l'ensemble des couples (F, G) où $\dim F = p$ et $F \oplus G = K^n$. Le groupe $GL_n(K)$ opère naturellement sur E_p et cette opération est clairement transitive. Notons $(e_1, \ldots, e_n)$ la base canonique de K^n, $F_p = \mathrm{Vect}(e_1, \ldots, e_p)$ et $G_p = \mathrm{Vect}(e_{p+1}, \ldots, e_n)$. On a $(F_p, G_p) \in E_p$. Le cardinal de E_p est égal à l'indice du stabilisateur

de l'élément (F_p, G_p) dans $GL_n(K)$. Or, une matrice de $GL_n(K)$ stabilise (F_p, G_p) si et seulement si elle est de la forme

$$\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$$

où $X \in GL_p(K)$ et où $Y \in GL_{n-p}(K)$ (évidemment, si $p = 0$ ou $p = n$, l'un des deux éléments disparaît). On a donc

$$\boxed{\mathrm{Card}\{A \in GL_n(K), A^2 = I\} = \sum_{p=0}^{n} \frac{|GL_n(K)|}{|GL_p(K)|\,|GL_{n-p}(K)|}},$$

où par convention $|GL_0(K)| = 1$. On peut conclure en remplaçant les cardinaux des groupes linéaires par la valeur déterminée dans l'exercice 1.8. $\lhd$

L'exercice qui suit concerne un sujet qui forme un pan entier de la combinatoire : la théorie des partitions. On appelle partition d'un entier naturel n toute décomposition de n sous la forme $n = a_1 + a_2 + \cdots + a_k$ où $0 < a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k$. Les a_i sont appelés les parts de la partition. L'entier 5 admet ainsi 7 partitions qui sont $5 = 1+4 = 2+3 = 1+1+3 = 1+2+2 = 1+1+1+2 = 1+1+1+1+1$. Cette notion est étudiée depuis Euler à qui l'on doit déjà de très beaux résultats, par exemple le fait qu'un entier admet autant de partitions en parts distinctes que de partitions en parts impaires. Ce résultat peut s'établir à l'aide de la série génératrice $\sum p(n)z^n$ où on note usuellement $p(n)$ le nombre de partitions de n. A l'aide de l'analyse complexe, on peut démontrer la formule de Ramanujan (1887-1920)

$$\ln p(n) \sim \pi\sqrt{\frac{2n}{3}}.$$

L'exercice qui suit est un joli problème extrémal sur les partitions.

1.11. Partitions d'un entier

1. Pour quelles partitions de n sous la forme $n = a_1 + \cdots + a_k$ (où les a_i sont dans $\mathbb{N}^*$), le produit $\prod_{i=1}^{k} a_i$ est-il maximal ?

2. Résoudre le même problème si on considère seulement les partitions constituées d'entiers 2 à 2 distincts.

(École normale supérieure)

Solution.

1. Voici pour les premiers entiers les partitions réalisant le produit maximal :

$2 = 2$; $3 = 3$; $4 = 2+2 = 4$; $5 = 2+3$; $6 = 3+3$; $7 = 2+2+3 = 3+4$; $8 = 2+3+3$; $9 = 3+3+3+$; ...

Soit n un entier que l'on suppose supérieur à 5. L'ensemble des partitions de n étant fini, on est certain d'en trouver au moins une donnant un produit maximal : $n = a_1 + a_2 + \cdots + a_k$ avec $a_1 \leqslant a_2 \leqslant \cdots \leqslant a_k$. Étudions les propriétés que doit avoir une telle partition.

• Les a_i sont inférieurs ou égaux à 4. En effet, si $a_k \geqslant 5$ on peut le remplacer par $(a_k - 3) + 3$ et comme $3(a_k - 3) > a_k$ (car $2a_k > 9$), on a une partition de n donnant un produit strictement plus grand. C'est absurde.

• On peut remplacer les coefficients égaux à 4 par $2+2$ sans changer le produit. On peut donc supposer $a_k \leqslant 3$.

• On a $a_1 \geqslant 2$. En effet, si $a_1 = 1$, la partition $(1+a_2) + a_3 + \cdots + a_k$ donne un produit strictement plus grand.

• Il y a au plus deux a_i égaux à 2. En effet, s'il y en a trois, le terme $2+2+2$ peut être remplacé par $3+3$ qui donne encore un produit supérieur.

Conclusion.

⋆ si $n \equiv 0$ [3], $n = 3k$ ($k \geqslant 1$), l'unique partition de produit maximal est $n = 3 + 3 + \cdots + 3$ avec k fois le terme 3.

⋆ si $n \equiv 1$ [3], $n = 3k + 1$ ($k \geqslant 1$), les partitions de produit maximal sont $n = 2+2+3+3+\cdots+3 = 4+3+3+\cdots+3$ avec $(k-1)$ fois le terme 3.

⋆ si $n \equiv 2$ [3], $n = 3k + 2$ ($k \geqslant 0$), l'unique partition de produit maximal est $n = 2 + 3 + 3 + \cdots + 3$ avec k fois le terme 3.

2. Le problème est plus difficile mais la démarche est la même. L'existence est claire pour les mêmes raisons que ci-dessus. On commence par regarder les premiers entiers. On donne toutes les partitions en entiers distincts, celle(s) de produit maximal étant en gras.

$2 = \mathbf{2}$

$3 = 1 + 2 = \mathbf{3}$

$4 = 1 + 3 = \mathbf{4}$

$5 = 1 + 4 = \mathbf{2} + \mathbf{3} = 5$

$6 = 1 + 2 + 3 = 1 + 5 = \mathbf{2} + \mathbf{4} = 6$

$7 = 1 + 2 + 4 = 2 + 5 = \mathbf{3} + \mathbf{4} = 7$

$8 = 1 + 2 + 5 = 1 + 3 + 4 = 2 + 6 = \mathbf{3} + \mathbf{5} = 8$

$9 = 1 + 2 + 6 = 1 + 3 + 5 = \mathbf{2} + \mathbf{3} + \mathbf{4} = 3 + 6 = 4 + 5 = 9$

$10 = 1 + 2 + 3 + 4 = 1 + 2 + 7 = 1 + 3 + 6 = 1 + 4 + 5 = \mathbf{2} + \mathbf{3} + \mathbf{5} = 3 + 7 = 4 + 6 = 10$ ...

Soit $n \geqslant 5$ que l'on écrit $n = a_1 + a_2 + \cdots + a_k$, avec $a_1 < a_2 < \cdots < a_k$, où le produit est maximal. On va ici encore étudier les propriétés que doit avoir cette partition. Sur les exemples ci-dessus, il semblerait qu'il faille prendre des entiers presque consécutifs. Précisons cela.

• Fait 1 : il y a au plus un entier de l'intervalle $[\![a_1, a_k]\!]$ qui n'apparaît pas dans la partition. En effet, dans le cas contraire, on peut trouver deux éléments $a < b$ de la partition tels que $a + 1$ et $b - 1$ ne soient pas dans la partition et $a < a + 1 < b - 1 < b$. Mais si on remplace alors $a + b$ par $(a + 1) + (b - 1)$, le produit obtenu est strictement plus grand en vertu de l'inégalité $(a + 1)(b - 1) > ab$ (car $b - a > 1$), ce qui est contradictoire.

La partition est donc formée d'entiers consécutifs avec au plus un «trou». Sur les exemples ci-dessus, il semblerait aussi qu'elle commence toujours par 2 ou 3.

• Fait 2 : on a $a_1 \in \{2, 3\}$ (on a supposé $n \geqslant 5$). En effet, si $a_1 \geqslant 7$ on le remplace par $3 + (a_1 - 3)$ et le produit est strictement plus grand. Si $a_1 = 6$ on le remplace par $2 + 4$ et si $a_1 = 5$ on le remplace par $2 + 3$. Supposons que $a_1 = 4$. Si $a_2 = 5$ on remplace $a_1 + a_2 = 4 + 5$ par $2 + 3 + 4$ avec $2 \times 3 \times 4 = 24 > 4 \times 5 = 20$ et si $a_2 = 6$ on remplace $a_1 + a_2 = 4 + 6$ par $2 + 3 + 5$ avec $2 \times 3 \times 5 = 30 > 4 \times 6 = 24$. Il reste enfin à voir que a_1 ne peut être égal à 1 ce qui est évident car si on le rajoute à a_2, le produit est plus grand.

Enfin, voici une dernière propriété qui n'est pas visible sur les exemples ci-dessus mais que l'on découvre par exemple en décomposant $14 = 3 + 5 + 6 = 2 + 3 + 4 + 5$. La partition maximale est la seconde : le 6 est avantageusement remplacé par $2 + 4$. Plus généralement,

• Fait 3 : si $a_1 = 3$ et si la partition admet un «trou», celui-ci est nécessairement entre a_{k-1} et a_k (c'est-à-dire en dernière position). En effet, dans le cas contraire, la partition s'écrit

$$n = 3 + 4 + \cdots + (m - 1) + (m + 1) + (m + 2) + \cdots + a_k,$$

où m est l'entier manquant. Mais la partition

$$n = 2 + 3 + \cdots + (m - 1) + m + (m + 1) + (m + 3) + \cdots + a_k$$

donne un produit strictement plus grand car $2m > m + 2$, ce qui est absurde.

• On peut maintenant effectuer la synthèse de ce travail. On fixe un entier $m \geqslant 3$ et on pose $\mathrm{S}_m = 2 + 3 + \cdots + m = \dfrac{m(m+1)}{2} - 1$. On note enfin E_m l'ensemble des suites finies strictement croissante d'entiers $s = (a_1, a_2, \ldots, a_k)$ ayant les propriétés suivantes :

(i) les a_i sont des entiers consécutifs avec éventuellement un «trou» ;

(ii) $a_1 = 2$ ou $a_1 = 3$;

(*iii*) lorsque $a_1 = 3$, s'il y a un «trou», il est entre a_{k-1} et a_k ;

(*iv*) la somme $a_1 + \cdots + a_k$ est inférieure ou égale à S_m.

L'application f qui à une suite s de E_m associe la somme de ses termes, a pour image l'intervalle $[\![2, S_m]\!]$ privé de l'entier 4 : c'est ce qui résulte de l'étude précédente.

On se propose de montrer que f est bijective, c'est-à-dire que la partition réalisant le produit maximal est unique, ce qu'on a pu observer sur les exemples ci-dessus. Pour cela il suffit de montrer que le cardinal de E_m est égal au cardinal de l'image de f à savoir $S_m - 2 = \dfrac{m^2+m-6}{2}$.

Comptons les éléments de E_m.

⋆ Il y a les suites commençant par 2. Il y a $m-1$ suites sans «trou» : (2) ; $(2,3)$; $(2,3.4)$; ... ; $(2,3,\ldots,m)$.

Dans chacune de ses suites (sauf les deux premières), on peut placer un «trou» dans n'importe quelle position, ce qui à partir de la suite $(2,3,\ldots,k)$, donne $k-3$ suites supplémentaires et donc $k-2$ suites en tout. On a au total $1+1+2+3+\cdots+(m-2) = 1 + \dfrac{(m-2)(m-1)}{2}$ telles suites.

⋆ Il y a les suites commençant par 3 sans «trou» : (3) ; $(3,4)$; ... ; $(3,4,\ldots,m)$. Cela fait $m-2$ suites.

⋆ Il y a enfin les suites commençant par 3 avec un «trou» en dernière place : $(3,5)$; $(3,4,6)$; ... ; $(3,4,5,\ldots,m-2,m)$; mais aussi (à ne pas oublier !) la suite $(3,4,5,\ldots,m-1,m+1)$ dont la somme est $S_m - 1$. On a donc $m-3$ telles suites.

Au total, on obtient

$$|E_m| = 1 + \frac{(m-2)(m-1)}{2} + (m-2) + (m-3) = \frac{m^2+m-6}{2},$$

ce qui est le résultat voulu.

Conclusion. Tout entier $n \geqslant 2$ admet une unique partition en entiers distincts de produit maximal, partition décrite ci-dessus. ◁

Remarquons qu'il est facile de trouver la partition optimale de proche en proche. Supposons celle de n connue, $n = a_1 + \cdots + a_k$, et voyons comment obtenir celle de $n+1$.

• *Si $a_1 = 3$ et s'il n'y a pas de trou, on remplace a_k par $a_k + 1$.*

• *Si $a_1 = 3$ et s'il y a un trou,* i.e. $n = 3+4+\cdots+(m-2)+m$, *la partition de $n+1$ est $n+1 = 2+3+4+\cdots+(m-2)+(m-1)$. C'est par exemple le cas pour $n = 13 = 3+4+6$; on obtient $14 = 2+3+4+5$.*

• *Si $a_1 = 2$ et s'il n'y a pas de trou, i.e. $n = 2+3+\cdots+m$, la partition de $n+1$ est $n+1 = 2+3+\cdots+(m-1)+(m+1)$, obtenu en remplaçant m par $m+1$. Pour obtenir $n+2$, on remplace $m-1$ par m, etc. Le trou se décale progressivement vers la gauche. Enfin si on a une décomposition de la forme $2+4+5+\cdots+m$ l'entier qui suit s'écrira $3+4+\cdots+m$ et on est ramené au premier point.*

L'étude de configurations d'ensembles finis obéissant à diverses contraintes forme ce qu'on appelle la théorie extrémale des ensembles. Cette définition étant assez vague, voici deux exemples simples de problèmes de ce type : quel est le nombre maximal de parties distinctes de $[\![1,n]\!]$ *dont deux quelconques ont toujours une intersection non vide*[4] *? Un autre exemple, moins simple, est le problème de Sperner : quel est le nombre maximal de parties distinctes de* $[\![1,n]\!]$ *telles qu'aucune des parties ne soit incluse dans une autre (on parle d'antichaîne pour la relation d'inclusion) ? Les problèmes posés sont souvent difficiles. En voici un exemple qui montre en outre comment un outil algébrique, ici les matrices d'incidence, permet de résoudre un problème combinatoire.*

1.12. Un problème de théorie extrémale des ensembles

Soit A un ensemble fini de cardinal $m \geqslant 2$ et $\mathrm{U}_1, \ldots, \mathrm{U}_n$ des parties non vides deux à deux distinctes de A. On suppose qu'il existe un entier $a \geqslant 0$ tel que si $i \neq j$, $\mathrm{Card}(\mathrm{U}_i \cap \mathrm{U}_j) = a$. Montrer que $n \leqslant m$.

(École normale supérieure)

▷ **Solution.**

• Notons $x_1, \ldots, x_m$ les éléments de A. On va traduire les relations d'appartenance des x_i aux ensembles U_j à l'aide d'une matrice, appelée matrice d'incidence. Soit $\mathrm{M} = (m_{ij}) \in \mathcal{M}_{m,n}(\mathbb{R})$ définie par $m_{ij} = 1$ si $x_i \in \mathrm{U}_j$ et $m_{ij} = 0$ sinon.

• Regardons comment se traduisent les hypothèses sur cette matrice M. Pour $i \neq j$ on a

$$\mathrm{Card}(\mathrm{U}_i \cap \mathrm{U}_j) = \sum_{k=1}^{m} m_{ki} m_{kj} = a$$

On reconnaît le terme (i,j) de la matrice ${}^t\mathrm{MM} \in \mathcal{M}_n(\mathbb{R})$. En notant d_i le cardinal de U_i, on a donc

$$\mathrm{H} = {}^t\mathrm{MM} = \begin{pmatrix} d_1 & a & \ldots & a \\ a & d_2 & \ldots & a \\ \vdots & & \ddots & \vdots \\ a & \ldots & a & d_n \end{pmatrix}$$

4. Réponse 2^{n-1}. Cette valeur est atteinte en prenant par exemple la famille des parties qui contiennent un élément fixé. Et si $\mathrm{A}_1, \ldots, \mathrm{A}_p$ sont des parties deux à deux distinctes qui ont la propriété mentionnée, alors les complémentaires des A_i sont deux à deux distincts et distincts des A_i, de sorte que $2p \leqslant 2^n$.

On va montrer que cette matrice H est inversible. Cela permettra de conclure puisqu'alors $n = \operatorname{rg} \mathrm{H} \leqslant \operatorname{rg}(\mathrm{M}) \leqslant m$ fournit l'inégalité souhaitée.

Pour cela on va simplement calculer le déterminant de H, connu sous le nom de déterminant de Hurwitz. Notons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$ et C la colonne dont tous les coefficients sont égaux à a. On a

$$\det \mathrm{H} = \det(\mathrm{C} + (d_1 - a)e_1, \ldots, \mathrm{C} + (d_n - a)e_n).$$

Si on développe $\det \mathrm{H}$ par multilinéarité, on obtient $\prod_{i=1}^{n}(d_i - a) + \sum_{k=1}^{n} \det((d_1 - a)e_1, \ldots, (d_{k-1} - a)e_{k-1}, \mathrm{C}, (d_{k+1} - a)e_{k+1}, \ldots, (d_n - a)e_n)$, puisque les déterminants où la colonne C intervient deux fois ou plus sont nuls. On a donc

$$\det \mathrm{H} = \prod_{i=1}^{n}(d_i - a) + a \sum_{i=1}^{n} \prod_{j \neq i}(d_j - a)$$

Or, pour tout i, on a $a \leqslant d_i$ (car $a = \operatorname{Card}(\mathrm{U}_i \cap \mathrm{U}_j)$, pour tout $j \neq i$), avec égalité pour au plus un indice i (car les égalités $a = d_i = d_j$ impliquent $\mathrm{U}_i = \mathrm{U}_i \cap \mathrm{U}_j = \mathrm{U}_j$ et les ensembles U_i sont deux à deux distincts). Il en résulte que $\det \mathrm{H} > 0$ et donc que H est inversible. $\lhd$

L'exercice suivant est un autre exemple où l'on utilise un outil algébrique, cette fois des polynômes, pour traduire une situation ensembliste.

1.13. Ensembles définis par récurrence

On définit des sous-ensembles de $\mathbb{N}$ par $\mathrm{A}_1 = \emptyset, \mathrm{B}_1 = \{0\}$ et pour n entier $\geqslant 1$,

$$\mathrm{A}_{n+1} = \mathrm{B}_n + 1 = \{x + 1,\ x \in \mathrm{B}_n\}$$
$$\mathrm{B}_{n+1} = \mathrm{A}_n \Delta \mathrm{B}_n = (\mathrm{A}_n \cup \mathrm{B}_n) \setminus (\mathrm{A}_n \cap \mathrm{B}_n).$$

Montrer que si p est une puissance de 2, alors $\mathrm{B}_p = \mathrm{B}_1$.

Indication : on pourra considérer les polynômes $\mathrm{P}_n = \sum_{k \in \mathrm{A}_n} \mathrm{X}^k$ et $\mathrm{Q}_n = \sum_{k \in \mathrm{B}_n} \mathrm{X}^k$ et raisonner modulo 2.

(École polytechnique)

Solution.

• L'ensemble B_{n+1} est la différence symétrique de A_n et B_n. Regardons les ensembles pour les premières valeurs de n. On a

$$\begin{array}{ll} A_2 = \{1\} & B_2 = \{0\} \\ A_3 = \{1\} & B_3 = \{0,1\} \\ A_4 = \{1,2\} & B_4 = \{0\} \\ A_5 = \{1\} & B_5 = \{0,1,2\} \\ A_6 = \{1,2,3\} & B_6 = \{0,2\} \\ A_7 = \{1,3\} & B_7 = \{0,1,3\} \\ A_8 = \{1,2,4\} & B_8 = \{0\}. \end{array}$$

Il apparaît effectivement que $B_2 = B_4 = B_8 = B_1$.

• Suivons l'indication et posons $P_n = \sum_{k \in A_n} X^k$ et $Q_n = \sum_{k \in B_n} X^k$, en regardant ces polynômes dans $\mathbb{Z}/2\mathbb{Z}[X]$. Ces polynômes caractérisent parfaitement les parties A_n et B_n. Les relations de définition se traduisent alors par les relations

$$P_{n+1} = XQ_n \quad \text{et} \quad Q_{n+1} = P_n + Q_n, \quad \text{pour tout } n \in \mathbb{N}^*.$$

En particulier, la suite (Q_n) vérifie la relation de récurrence linéaire à deux termes : pour tout $n \geqslant 2$, $Q_{n+1} = Q_n + XQ_{n-1}$, avec $Q_1 = Q_2 = 1$. Par convention on pose $Q_0 = 0$, ce qui rend la relation encore vraie pour $n = 1$.

• On va regarder (Q_n) comme une suite du corps $K = \mathbb{Z}/2\mathbb{Z}(X)$ des fractions rationnelles à coefficients dans $\mathbb{Z}/2\mathbb{Z}$. L'équation caractéristique est $r^2 + r + X = 0$ (ne pas oublier qu'on est en caractéristique 2 donc les moins peuvent être remplacés par des plus). La théorie habituelle de l'équation du second degré ne s'applique pas en caractéristique 2 : il est impossible de passer à la forme canonique car 2 n'est pas inversible. Cela dit, il existe un sur-corps K' de K dans lequel l'équation admet deux racines α_1 et α_2. On a

$$\alpha_1 + \alpha_2 = 1 \text{ et } \alpha_1\alpha_2 = X.$$

En particulier $\alpha_1 \neq \alpha_2$ car sinon $1 = 2\alpha_1 = 0$ ce qui est impossible. On sait alors qu'il existe deux éléments A, B de K' tels que, pour tout $n \in \mathbb{N}$,

$$Q_n = A\alpha_1^n + B\alpha_2^n.$$

On détermine A et B à l'aide de Q_0 et Q_1. Il vient $A + B = 0$, c'est-à-dire $A = B$ et $A(\alpha_1 + \alpha_2) = 1$, soit finalement $A = B = 1$. On a donc, pour tout $n \in \mathbb{N}$,

$$Q_n = \alpha_1^n + \alpha_2^n.$$

• Il ne reste plus qu'à calculer α_i^n lorsque n est une puissance de 2 (pour $i = 1$ et 2). On a $\alpha_i^2 = \alpha_i + X$. Comme on est en caractéristique deux, le carré d'une somme est la somme des carrés (les doubles produits

disparaissent). On a donc $\alpha_i^4 = (\alpha_i + X)^2 = \alpha_i^2 + X^2 = \alpha_i + X + X^2$. De même, on a facilement par récurrence sur p,

$$\alpha_i^{2^p} = \alpha_i + X + X^2 + X^4 + \cdots + X^{2^{p-1}} = \alpha_i + \sum_{k=0}^{p-1} X^{2^k}.$$

On en déduit que $Q_{2^p} = \alpha_1^{2^p} + \alpha_2^{2^p} = \alpha_1 + \alpha_2 = 1$. Donc $B_{2^p} = \{1\}$. $\lhd$

Dans l'énoncé suivant on s'intéresse aux applications d'un ensemble fini dans lui-même qui peuvent se décomposer en un produit d'applications idempotentes.

1.14. Théorème de Howie

Soit X un ensemble fini non vide et θ une application injective et non surjective d'une partie D de X dans X.

1. On suppose que $\theta(D) \subset D$. Montrer qu'il existe un nombre fini d'applications $p_1, \ldots, p_n$ de X dans X vérifiant $p_i \circ p_i = p_i$ pour tout i et telles que la restriction à D de $p_1 \circ \cdots \circ p_n$ coïncide avec θ.

2. Montrer que la conclusion de la question 1 reste vraie sans l'hypothèse $\theta(D) \subset D$.

3. Soit α une application non bijective de X dans X. Montrer qu'il existe un nombre fini d'applications $\pi_1, \ldots, \pi_n$ de X dans X vérifiant $\pi_i \circ \pi_i = \pi_i$ pour tout i et telles que $\alpha = \pi_1 \circ \cdots \circ \pi_n$. *C'est le théorème de Howie.*

(École normale supérieure)

Solution.

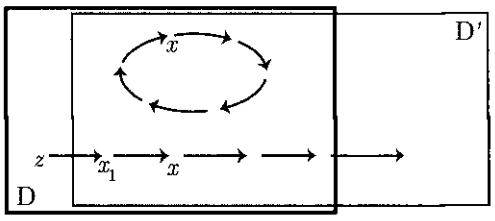
1. Comme θ est supposée injective et que $\theta(D) \subset D$, on a forcément $\theta(D) = D$ et θ établit une bijection de D sur D. Comme θ n'est pas surjective lorsqu'on la regarde comme une application de D dans X, on peut affirmer que D est une partie stricte de X. Observons qu'une application p de X dans X vérifie $p \circ p = p$ si et seulement si p fixe tous les points de son image. La question est triviale si D est vide et facile si D est un singleton $\{x\}$ (il suffit de prendre $n = 1$ et pour p_1 l'application constante égale à x). Nous supposerons que D contient au moins deux éléments. Nous savons que toute permutation de D peut se décomposer en un produit de transpositions. Il suffit donc de traiter le cas où θ est une transposition, disons $\theta = (b, c)$. Par hypothèse, il existe au moins un élément $a \in X \setminus D$. Notons p_1 l'application qui envoie b sur a et qui fixe tous les autres points de X, p_2 l'application qui envoie c sur b et qui fixe tous les autres points et enfin p_3 l'application qui envoie a sur c et qui fixe tout le reste. Il est clair que p_1, p_2, p_3 sont idempotentes (*i.e.* vérifient $p_i \circ p_i = p_i$). Et on a

$$\begin{array}{ccccccc} & p_1 & & p_2 & & p_3 & \\ b & \longrightarrow & a & \longrightarrow & a & \longrightarrow & c \\ c & \longrightarrow & c & \longrightarrow & b & \longrightarrow & b \end{array}$$

Comme par ailleurs $p_3 \circ p_2 \circ p_1$ fixe tout point de $\mathrm{D} \setminus \{b, c\}$ on a le résultat : la restriction de $p_3 \circ p_2 \circ p_1$ à D est égale à la transposition qui échange b et c.

Notons qu'on aurait aussi pu utiliser la décomposition de la permutation θ en produit de cycles à supports disjoints avec la même idée. Pour obtenir la décomposition d'un cycle $(b_1, \ldots, b_m)$ on choisit à nouveau a en dehors de D et on considère p_1 qui envoie b_m sur a en fixant tous les autres points, p_2 qui envoie b_{m-1} sur b_m en fixant tous les autres points, jusqu'à p_m qui envoie b_1 sur b_2 en fixant le reste, et enfin p_{m+1} qui envoie a sur b_1 en fixant le reste. On vérifie comme avant que les p_i sont idempotentes et que la restriction de $p_{m+1} \circ p_m \circ \cdots \circ p_1$ à D est égale au cycle $(b_1, \ldots, b_m)$.

2. On ne suppose plus maintenant que $\mathrm{D}' = \theta(\mathrm{D})$ est égal à D. On va utiliser une généralisation de la décomposition en cycles à support disjoints d'une permutation. Prolongeons momentanément θ à D' en disant que les points de $\mathrm{D}' \setminus \mathrm{D}$ sont fixes. On définit alors la relation binaire R sur $\mathrm{D} \cup \mathrm{D}'$ en disant que $x\mathrm{R}y$ s'il existe un entier naturel k tel que $y = \theta^k(x)$ ou $x = \theta^k(y)$. Il s'agit clairement d'une relation d'équivalence sur $\mathrm{D} \cup \mathrm{D}'$. Décrivons la classe d'un élément. Soit $x \in \mathrm{D}$. Si les images successives de x par θ restent toutes dans D alors, comme dans le cas des bijections, il existe nécessairement un plus petit entier k tel que $\theta^k(x) = x$ et la classe de x est égale à $\{x, \theta(x), \ldots, \theta^{k-1}(x)\}$. L'alternative est qu'il existe un entier k tel que $\theta^k(x)$ ne soit plus dans D. Les itérés de x par θ s'arrêtent alors à cet élément. On regarde alors si x est ou non dans D'. Si oui, il est l'image par θ d'un unique élément x_1 de D : la classe de x est la même que la classe de x_1. On regarde alors si x_1 est encore dans D' ou non. Bref, on peut trouver un élément z de $\mathrm{D} \setminus \mathrm{D}'$ tel que la classe de x soit celle de z, à savoir $\{z, \theta(z), \ldots, \theta^\ell(z) = x, \ldots, \theta^k(x) = \theta^{k+\ell}(z)\}$. La figure suivante résume ces possibilités :



Comme dans la question 1 il nous suffit de prouver le résultat pour la restriction de θ à une classe d'équivalence (intersectée avec D), restriction qui reste injective. C'est fait dans la question 1 pour les classes

circulaires. Il reste donc à traiter le cas d'une classe du second type. On suppose donc que $D = \{z, \theta(z), \ldots, \theta^{k-1}(z)\}$ avec $\theta^k(z) \notin D$ $(k \geqslant 2)$. Prenons alors l'application p_1 de X dans X qui envoie $\theta^{k-1}(z)$ sur $\theta^k(z)$ et qui fixe tous les autres points, p_2 qui envoie $\theta^{k-2}(z)$ sur $\theta^{k-1}(z)$ et qui fixe tous les autres points et ainsi de suite jusqu'à p_k qui envoie z sur $\theta(z)$ en fixant le reste. Il est clair que les p_i sont idempotentes et que la restriction de $p_k \circ \cdots \circ p_1$ à D est égale à θ.

3. Choisissons $D = \{x_1, \ldots, x_p\}$ un système de représentants des classes d'équivalence pour la relation d'équivalence canoniquement associée à α : la restriction θ de α à D établit une bijection entre D et l'image de α. Comme α n'est pas bijective, θ n'est pas surjective et on peut donc appliquer la question 2. Il existe des applications $\pi_1, \ldots, \pi_n$ de X dans X vérifiant $\pi_i \circ \pi_i = \pi_i$ pour tout i et telles que $\pi(x_k) = \pi_1 \circ \cdots \circ \pi_n(x_k)$ pour tout k. Notons alors π l'application qui à tout x de X associe l'unique x_k tel que $\alpha(x) = \alpha(x_k)$. Il est clair que π est idempotente et on a $\alpha = \pi_1 \circ \cdots \circ \pi_n \circ \pi$. Le théorème de Howie est prouvé. $\lhd$

Les deux exercices qui suivent concernent des évaluations asymptotiques.

1.15. Distribution du premier chiffre des puissances de 2

> Pour $i \in [\![1, 9]\!]$, et $n \in \mathbb{N}^*$, on note $N_i(n)$ le nombre d'éléments de l'ensemble $\{2, 2^2, \ldots, 2^n\}$ dont le premier chiffre de l'écriture décimale est i. Calculer $\lim\limits_{n \to +\infty} \dfrac{N_i(n)}{n}$.
>
> **(École normale supérieure)**

Solution.

Le but de l'exercice est de déterminer la fréquence d'apparition des chiffres $1, 2, \ldots, 9$ en première position dans la suite des puissances de 2. A priori on ne sait pas si tous les chiffres vont apparaître, et encore moins s'il vont apparaître une infinité de fois. Fixons i entre 1 et 9, et commençons par traduire le fait que i est le premier chiffre de 2^p.

• L'entier 2^p commence par i si et seulement s'il existe $k \in \mathbb{N}$ tel que $i.10^k \leqslant 2^p < (i+1).10^k$ c'est-à-dire, en prenant le logarithme, si et seulement s'il existe k tel que

$$\frac{\ln i}{\ln 10} + k \leqslant p\frac{\ln 2}{\ln 10} < k + \frac{\ln(i+1)}{\ln 10}.$$

Cela est encore équivalent à dire que le résidu modulo 1 de $p\theta$ est dans l'intervalle $\left[\dfrac{\ln i}{\ln 10}, \dfrac{\ln(i+1)}{\ln 10}\right[$, où $\theta = \dfrac{\ln 2}{\ln 10}$. Ainsi, $N_i(n)$ est exacte-

ment le nombre d'entiers $p \in [\![1, n]\!]$ tels que $p\theta$ modulo 1 appartienne à $\left[\frac{\ln i}{\ln 10}, \frac{\ln(i+1)}{\ln 10}\right[$.

• On est donc amené à étudier le comportement de la suite $(p\theta)_{p\geqslant 1}$ modulo 1. Il s'avère que θ est irrationnel. En effet, si $\frac{\ln 2}{\ln 10} = \frac{a}{b}$ avec $(a, b) \in (\mathbb{N}^*)^2$, il vient $2^b = 10^a$ ce qui est impossible puisque 2^b n'est pas divisible par 5. Montrons alors que la suite $(p\theta)$ mod 1 est dense dans l'intervalle $[0, 1]$. Cela prouvera déjà qu'il y a une infinité d'entiers p tels que 2^p commence par le chiffre i.

Il est bien entendu équivalent de montrer que l'ensemble $\mathbb{N}\theta + \mathbb{Z}$ est dense dans $\mathbb{R}$. On a presque un sous-groupe additif de $\mathbb{R}$. Or, nous savons qu'un sous-groupe additif de $\mathbb{R}$ est soit monogène, soit dense. Le sous-groupe $\mathbb{Z} + \theta\mathbb{Z}$ n'est pas monogène : si on avait $\mathbb{Z} + \theta\mathbb{Z} = a\mathbb{Z}$, il existerait des entiers α, β tels que $1 = \alpha a$ et $\theta = \beta a$. Mais en faisant le rapport des deux égalités, on aurait $\theta = \frac{\beta}{\alpha} \in \mathbb{Q}$ ce qui n'est pas. Ainsi, $\mathbb{Z} + \theta\mathbb{Z}$ est dense dans $\mathbb{R}$. Il est alors facile d'en déduire que $\mathbb{N}\theta + \mathbb{Z}$ reste encore dense dans $\mathbb{R}$. Soit $]a, b[\subset \mathbb{R}$. On peut trouver un élément z non nul de $\mathbb{Z} + \theta\mathbb{Z}$ tel que $|z| < b - a$. Quitte à prendre $-z$, on peut prendre z dans $\mathbb{N}\theta + \mathbb{Z}$. Supposons par exemple $z > 0$. Si $n_0 \in \mathbb{Z}$ est un entier inférieur à a, il est clair que l'un des éléments de la suite $(n_0 + kz)_{k\geqslant 0}$ va tomber dans l'intervalle $]a, b[$. Or, $n_0 + kz$ est dans $\mathbb{N}\theta + \mathbb{Z}$ pour tout $k \geqslant 0$. D'où le résultat. (Pour $z < 0$, on considère de même un entier $n_0 > b$.)

• La suite $(p\theta)$ (mod 1) est donc dense dans $[0, 1]$. Mais cela ne suffit pas pour déterminer un équivalent de $\mathrm{N}_i(n)$. Il nous faut étudier comment les résidus modulo 1 des termes $p\theta$ se répartissent dans l'intervalle $[0, 1[$ afin de déterminer la proportion de ceux qui vont tomber dans l'intervalle $\left[\frac{\ln i}{\ln 10}, \frac{\ln(i+1)}{\ln 10}\right[$ ou plus généralement dans un intervalle I fixé. Si la répartition est régulière, concept que nous allons préciser, il est légitime de penser que la proportion cherchée est exactement la longueur de l'intervalle I. Nous dirons qu'une suite (s_n) de réels de $[0, 1]$ est *équirépartie* si, pour tout intervalle $\mathrm{I} \subset [0, 1]$, la proportion

$$\frac{\mathrm{Card}\{k \in [\![1, n]\!], \quad s_k \in \mathrm{I}\}}{n}$$

tend vers la longueur de I lorsque n tend vers l'infini.

Topologiquement le quotient $\mathbb{R}/\mathbb{Z}$ est un cercle (c'est le segment $[0, 1]$ où on a identifié 0 et 1). En fait, l'application $\overline{x} \longmapsto e^{2i\pi x}$ établit une bijection (et même un homéomorphisme pour le lecteur connaissant la notion de topologie quotient) entre $\mathbb{R}/\mathbb{Z}$ et le cercle unité S^1 du plan complexe. La suite $(p\theta)$ modulo 1 devient la suite des puissances de $e^{2i\pi\theta}$. Cette suite tourne sur le cercle S^1, l'écart (angulaire) entre deux termes consécutifs étant constant. Il est alors assez naturel de penser que cette

suite est équirépartie et c'est effectivement le cas : c'est le théorème de Bohl-Sierpinski-Weyl[5] qui l'affirme. Pour notre problème on peut alors en déduire que

$$\boxed{\lim_{n\to+\infty} \frac{\mathrm{N}_i(n)}{n} = \frac{\ln(i+1)-\ln i}{\ln 10}}.$$

En particulier le chiffre i apparaît d'autant plus fréquemment qu'il est petit ! Pour $i = 1$ on a une fréquence de 30%, alors que pour $i = 9$, on obtient $4,5\%$.

• Évidemment il reste à prouver le théorème de Bohl-Sierpinski-Weyl. On peut en donner une preuve directe[6] mais c'est assez long. On renvoie le lecteur au tome 2 d'analyse (exercices 1.29 et 1.30) où figure un exercice qui démontre le critère d'équirépartition de Weyl qui implique facilement ce résultat. ◁

L'exercice suivant établit un résultat qui remonte à Gauss et qui donne une estimation du nombre de points à coordonnées entières dans un disque euclidien de rayon R.

1.16. Un théorème de Gauss

On munit $\mathbb{R}^n$, $n \geqslant 2$, de sa structure euclidienne canonique. Donner un équivalent lorsque r tend vers $+\infty$ du nombre $\mathrm{N}(r)$ de points de $\mathbb{Z}^n$ de norme inférieure ou égale à r.

(École polytechnique, École normale supérieure)

▷ **Solution.**

L'idée naturelle est la suivante. Le nombre de points entiers dans un domaine D de $\mathbb{R}^n$, suffisamment grand et assez régulier (par exemple convexe), est approximativement le volume de D. Dans le cas des boules fermées B_r de centre l'origine et de rayon $r > 0$ on va montrer rigoureusement que $\mathrm{N}(r)$ est effectivement équivalent au volume $\mathrm{V}(r)$ de cette boule.

À tout point $x = (x_1, \ldots, x_n)$ de $\mathbb{Z}^n$, on associe l'hypercube C_x de coté 1 centré en x défini par

$$\mathrm{C}_x = \left\{ t = (t_1, \ldots, t_n) \in \mathbb{R}^n, \quad \forall i \in [\![1, n]\!], \ |t_i - x_i| \leqslant \frac{1}{2} \right\}.$$

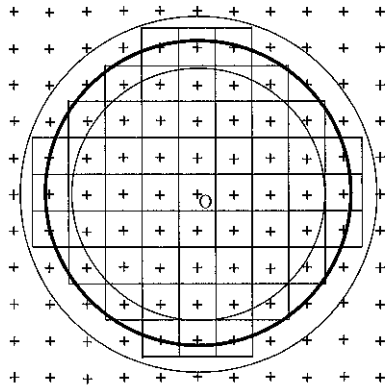
Ces hypercubes C_x sont de volume 1. Pour $r > 0$, considérons l'ensemble

5. Prouvé indépendamment par les trois mathématiciens vers 1910.

6. Le lecteur pourra trouver une preuve de ce type dans les deux ouvrages suivants : HAUZY (G.), *Propriétés statistiques de suites arithmétiques*, PUF, 1976 ; HARDY (G.H.) & WRIGHT (E.M), *An introduction to the theory of numbers*, Oxford University Press, 5éd., 1979.

des cubes C_x centrés aux points de $\mathbb{Z}^n$ qui sont dans la boule fermée B_r ; il y en a $N(r)$. Le volume de la réunion de ces hypercubes est donc $N(r)$.

• Voici une figure dans le plan :



Le réseau $\mathbb{Z}^2$ est représenté par des petites croix. En gras figure un cercle de rayon $r > 0$, les deux autres cercles ayant pour rayons respectifs $r + \frac{\sqrt{2}}{2}$ et $r - \frac{\sqrt{2}}{2}$. Commençons par expliquer l'idée dans le cas du plan. Il est clair que tout carré C_x centré en un point $x \in \mathbb{Z}^2 \cap B_r$ est inclus dans le disque de rayon $r + \frac{\sqrt{2}}{2}$. Cela provient de l'inégalité triangulaire et du fait qu'un point de C_x est à une distance inférieure à $\frac{\sqrt{2}}{2}$ de x. De même, on montre que le disque de rayon $r - \frac{\sqrt{2}}{2}$ est complètement inclus dans la réunion des petits carrés. Or, l'aire de la réunion des carrés est exactement $N(r)$, le nombre de carrés (car ils sont tous d'aire 1 et d'intérieurs disjoints). On a donc l'encadrement

$$\pi\left(r - \frac{\sqrt{2}}{2}\right)^2 \leqslant N(r) \leqslant \pi\left(r + \frac{\sqrt{2}}{2}\right)^2.$$

Cette double inégalité prouve que $N(r) \sim \pi r^2$.

• Passons au cas général. La démarche est la même. On fait intervenir le volume d'une boule de rayon r. A priori, on ne sait pas le calculer, mais si on note b_n le volume de la boule euclidienne fermée de rayon 1 (ainsi $b_2 = \pi$), par homogénéité une boule de rayon $r > 0$ a pour volume $V(r) = b_n r^n$. La distance maximale d'un point d'un de nos hypercubes à son centre est $\frac{\sqrt{n}}{2}$. L'inégalité précédente s'écrit alors

$$b_n\left(r - \frac{\sqrt{n}}{2}\right)^n \leqslant N(r) \leqslant b_n\left(r + \frac{\sqrt{n}}{2}\right)^n.$$

On en déduit que $N(r) \sim b_n r^n$ lorsque r tend vers $+\infty$. $\lhd$

Voici une autre manière de voir les choses. Au lieu de compter les points de $\mathbb{Z}^n$ dans B_r, il revient au même de compter les points du réseau $\frac{1}{r}\mathbb{Z}^n$ dans la boule unité B_1. Alors $\frac{\mathrm{N}(r)}{r^n}$ est le volume de la réunion des hypercubes de côté $\frac{1}{r}$ centrés aux points de $\frac{1}{r}\mathbb{Z}^n \cap \mathrm{B}_1$ et il semble clair que ce volume va tendre vers le volume de B_1 : c'est pratiquement le procédé d'approximation utilisé pour définir la notion de partie quarrable dans le cas du plan.

On trouvera dans le tome 2 d'analyse (exercice 3-23) une application du résultat de cet exercice à la recherche d'un équivalent pour une série entière. Signalons enfin qu'il est facile d'obtenir une relation de récurrence entre b_n et b_{n-1} conduisant à la formule suivante : $b_n = \dfrac{\pi^{n/2}}{\Gamma\left(\frac{n+2}{2}\right)}$, où Γ est la fonction d'Euler.

Nous allons terminer par deux exercices concernant les entiers naturels, exercices de nature moins combinatoire, mais qui s'inscrivent tout de même naturellement dans ce chapitre. Le premier étudie à quelle condition deux suites pseudo-arithmétiques permettent de partitionner $\mathbb{N}^*$ (une suite pseudo-arithmétique est une suite d'entiers de la forme $(\mathrm{E}(n\alpha))_{n\geqslant 1}$ avec $\alpha > 1$).

1.17. Théorème de Beatty (1926)

Soit $a, b > 1$, $\mathrm{E} = \{\mathrm{E}(na), n \in \mathbb{N}^*\}$ et $\mathrm{F} = \{\mathrm{E}(nb), n \in \mathbb{N}^*\}$. Montrer qu'il y a équivalence entre :

(*i*) E et F forment une partition de $\mathbb{N}^*$;

(*ii*) $\dfrac{1}{a} + \dfrac{1}{b} = 1$ et a et b sont irrationnels.

(École normale supérieure)

1. Solution.

• Le résultat est assez intuitif si l'on introduit la notion de *densité* d'une partie A de $\mathbb{N}^*$. Pour tout $n \geqslant 1$, on note a_n le cardinal de $\mathrm{A} \cap [\![1, n]\!]$. Si la suite $\left(\dfrac{a_n}{n}\right)$ converge on dira que A admet une densité égale par définition à la limite $d(\mathrm{A})$ de cette suite. Par exemple, l'ensemble des entiers pairs est de densité $\dfrac{1}{2}$, l'ensemble des carrés est de densité nulle.

• Montrons que pour $\alpha > 1$, l'ensemble $\{\mathrm{E}(n\alpha), n \in \mathbb{N}^*\}$ est de densité α^{-1}. En effet, les entiers $\mathrm{E}(k\alpha)$ sont deux à deux distincts et il y en a $\mathrm{E}\left(\dfrac{n}{\alpha}\right)$ dans l'intervalle $[\![1, n]\!]$. Le résultat annoncé provient de ce que $\lim\limits_{n\to+\infty} \dfrac{1}{n}\mathrm{E}\left(\dfrac{n}{\alpha}\right) = \dfrac{1}{\alpha}$.

• $(i) \Longrightarrow (ii)$. Il est clair que si A, B sont des parties disjointes de $\mathbb{N}^*$ admettant toutes deux une densité, alors $A \cup B$ admet une densité et $d(A \cup B) = d(A) + d(B)$. Comme $d(\mathbb{N}^*) = 1$, on a donc $a^{-1} + b^{-1} = 1$ d'après le point précédent. De plus, a et b ne peuvent pas être tous les deux rationnels car si $a = \frac{p}{q}$ et $b = \frac{p'}{q'}$, alors $E(p'qa) = E(pq'b) = pp'$ est dans $E \cap F$. L'un des deux est donc irrationnel. Mais la relation $\frac{1}{a} + \frac{1}{b} = 1$ impose alors l'irrationalité du second.

• $(ii) \Longrightarrow (i)$. Commençons par montrer que E et F sont disjoints. On raisonne par l'absurde. Soit $k \in E \cap F$, $n \geqslant 1$ et $m \geqslant 1$ tels que $k = E(na) = E(mb)$. Par définition de la partie entière, $k \leqslant na < k+1$ et $k \leqslant mb < k+1$. En divisant la première inégalité par a et la seconde par b on a $\frac{k}{a} \leqslant n < \frac{k}{a} + \frac{1}{a}$ et $\frac{k}{b} \leqslant m < \frac{k}{b} + \frac{1}{b}$. Compte tenu de la relation qui lie a et b, on obtient en additionnant les deux inégalités $k \leqslant n+m < k+1$. Comme k, n et m sont entiers cela impose $n+m = k$. On a alors nécessairement égalité dans les deux inégalités précédentes, c'est-à-dire $na = mb = k$. C'est absurde car a et b sont irrationnels. On a donc $E \cap F = \emptyset$.

Montrons maintenant que $E \cup F = \mathbb{N}^*$. Soit $n \geqslant 1$, $p = E(na)$ et m l'unique entier (éventuellement nul) tel que $E(mb) < p < E((m+1)b)$ (les inégalités sont strictes car $E \cap F = \emptyset$). L'entier $E(mb)$ (resp. $p = E(na)$) est le plus grand élément de F (resp. de E) appartenant à l'intervalle $[\![1, p]\!]$. Les applications $k \longmapsto E(ka)$ et $k \longmapsto E(kb)$ étant injectives (car $a, b > 1$), l'intervalle $[\![1, p]\!]$ contient donc $m+n$ éléments de $E \cup F$ (car ces deux ensembles sont disjoints). Or, on a $\frac{p}{a} \leqslant n < \frac{p+1}{a}$ et $\frac{p}{b} - 1 < m < \frac{p+1}{b}$. En additionnant il vient $p - 1 < n + m < p + 1$, donc $p = n + m$: tous les entiers de $[\![1, p]\!]$ sont dans $E \cup F$. Le résultat suit car n est arbitraire et p est donc arbitrairement grand. $\lhd$

Il a été démontré, dans les années 20, qu'il est impossible de partitionner $\mathbb{N}^*$ avec trois suites pseudo-arithmétiques ou plus.

Voici, pour finir, un exercice posé aux Olympiades Internationales en 1971 à Zilina (aujourd'hui en Slovaquie).

1.18. Un exercice d'Olympiades

Soit $A = (a_{ij})$ une matrice carrée de taille $n \geqslant 2$, à coefficients entiers naturels et telle que, pour $(k, l) \in [\![1, n]\!]^2$, si $a_{kl} = 0$ alors $\sum_{i=1}^{n} a_{il} + \sum_{j=1}^{n} a_{kj} \geqslant n$. Montrer que $\sum_{i,j} a_{ij} \geqslant \frac{n^2}{2}$. Donner un exemple où il y a égalité.

(École normale supérieure)

1. **Solution.**

On va essayer d'évaluer la somme des coefficients en utilisant une rangée (*i.e.* une ligne ou une colonne) où il y a beaucoup de zéros pour exploiter au mieux l'hypothèse. Cela invite à considérer une rangée dont la somme S des éléments est minimale. Quitte à prendre la transposée de A puis à permuter deux lignes on peut supposer que la rangée en question est la première ligne de A.

• Si $S \geqslant \frac{n}{2}$, le résultat est évident car la somme des coefficients de chacune des n lignes de A est minorée par $\frac{n}{2}$.

• Si $S < \frac{n}{2}$, il y a $\alpha \geqslant \frac{n}{2}$ zéros dans la première ligne de A. En notant $J = \{j \in [\![1, n]\!],\ a_{1j} = 0\}$, on a d'après l'hypothèse

$$\sum_{i,j} a_{ij} = \sum_{j \in J} \sum_{i=1}^{n} a_{ij} + \sum_{j \notin J} \sum_{i=1}^{n} a_{ij} \geqslant \alpha(n - S) + (n - \alpha)S.$$

En écrivant $\alpha(n - S) + (n - \alpha)S = \frac{n^2}{2} + (n - 2S)(\alpha - \frac{n}{2}) \geqslant \frac{n^2}{2}$, on obtient l'inégalité voulue.

Pour avoir égalité, il est bien entendu nécessaire de prendre n pair. La matrice «damier» définie par $a_{ij} = 1$ si $i \equiv j\ [2]$ et $a_{ij} = 0$ fournit alors un exemple où il y a égalité. ◁

Chapitre 2
Théorie des groupes

C'est au cours du XIXe *siècle qu'émerge la notion abstraite de groupe. Deux sortes de lois de composition interne sont à l'origine du concept : celle relative aux classes d'équivalences en Arithmétique (introduites de manière implicite dans les* Disquisitiones arithmeticæ *de Gauss) et la composition des permutations sur un ensemble fini étudiée notamment par Galois et dont la théorie fut largement développée par Jordan dans son* Traité des substitutions. *Le premier à rapprocher les points de vue et à concevoir que la structure de groupe est indépendante de la nature des objets considérés est Cayley qui donne une première définition abstraite d'un groupe dans* On the theory of groups as depending on the symbolic equation $\theta^n = 1$ *(1854). Il dresse des tables de multiplication pour les groupes de petit ordre. Il connaît les deux groupes d'ordre* 6 *(à isomorphisme près), les cinq d'ordre* 8 *et fournit des exemples d'une grande variété : ensembles de matrices inversibles, de quaternions, groupe des racines n-ième de l'unité... Jordan approfondira ce travail et étudiera de manière très poussée le groupe linéaire et ses sous-groupes. Il est notamment à l'origine de la notion de groupe quotient et de la théorie des représentations linéaires (*i.e. *l'étude des morphismes d'un groupe dans le groupe linéaire d'un espace vectoriel). Cette réalisation géométrique des groupes permet de traduire les propriétés géométriques en propriétés algébriques et inversement. L'étude des groupes de transformations permet la classification des géométries de Felix Klein. Il faut toutefois reconnaître que durant tout ce siècle le terme de «groupe» fut employé de manière très vague, sans que les exemples classiques des groupes additif* $\mathbb{Z}$ *ou multiplicatif* $\mathbb{Q}^*$ *soient relevés et ce n'est qu'en 1898 que le mathématicien Weber en donne la définition connue aujourd'hui.*

Commençons par un exercice élémentaire sur les lois de composition, posé au concours de l'École polytechnique.

2.1. Existence d'un idempotent

Soit E un ensemble fini muni d'une loi de composition interne associative. Montrer qu'il existe $s \in$ E tel que $s^2 = s$.

(École polytechnique)

▷ **Solution.**

Soit a un élément quelconque de E. L'associativité de la loi permet de donner un sens à a^k pour tout entier $k \in \mathbb{N}^*$. Comme E est fini, la suite $u_n = a^{2^n}$ (obtenue à partir de $u_0 = a$ par itération de $s \mapsto s^2$) ne peut pas être injective. On peut donc trouver $n \in \mathbb{N}^*$ et $p > 0$ tels que $u_{n+p} = u_n$. Si on pose $b = a^{2^n}$, on a alors $b^{2^p} = b$. Si $p = 1$ c'est gagné. Pour avoir des idées regardons ce qui se passe pour $p = 2$. On a $b^4 = b$. On obtient alors $(b^3)^2 = b^6 = b^4b^2 = bb^2 = b^3$ et b^3 est idempotent. En fait de manière générale, si $x^m = x$ avec $m \geqslant 2$, alors x^{m-1} est idempotent puisque $(x^{m-1})^2 = x^{2m-2} = x^m \cdot x^{m-2} = x \cdot x^{m-2} = x^{m-1}$. Donc ici, $s = b^{2^p-1}$ convient. ◁

Les exercices suivants concernent les notions de sous-groupes et de morphismes de groupes.

2.2. Groupes dont l'ensemble des sous-groupes est fini

> Caractériser les groupes dont l'ensemble des sous-groupes est fini.
> (**École normale supérieure**)

▷ **Solution.**

Les groupes finis vérifient de manière évidente cette condition. Nous allons démontrer que ce sont les seuls. Soit G un groupe dont l'ensemble E des sous-groupes est fini. Tout x de G est d'ordre fini car un élément d'ordre infini engendre un sous-groupe isomorphe à $\mathbb{Z}$ et $\mathbb{Z}$ admet une infinité de sous-groupes. Si E′ désigne le sous-ensemble de E formé des groupes monogènes, on a $G = \bigcup_{H \in E'} H$. Comme E′ est fini et que les éléments de E′ sont des ensembles finis d'après ce qui précède, G est fini. ◁

2.3. Morphismes de $\mathbb{Q}$ dans $\mathbb{Z}$

> Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
> (**École normale supérieure**)

▷ **Solution.**

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$. Son image est un sous-groupe de $\mathbb{Z}$, c'est-à-dire un certain $n\mathbb{Z}$, $n \in \mathbb{N}$. Si $n \geqslant 1$, on choisit un antécédent x de n. On obtient alors $2f(\frac{x}{2}) = f(x) = n$ et donc $\frac{n}{2} = f(\frac{x}{2}) \in n\mathbb{Z}$, ce qui est absurde. On a donc $n = 0$ et f est nul. ◁

L'exercice suivant doit être rapproché de l'exercice 6.15, plus classique, où il s'agit de démontrer la même équivalence pour un endomorphisme f d'un espace vectoriel E *de dimension finie. La démonstration est quasiment la même : on passe d'une inclusion à une égalité ensembliste en invoquant ici un argument de cardinal et là un argument de dimension ; une relation entre le cardinal de* $\operatorname{Im} f$ *et celui de* $\operatorname{Ker} f$ *remplace le théorème du rang.*

2.4. Équivalence $\operatorname{Ker} f = \operatorname{Ker} f^2 \Longleftrightarrow \operatorname{Im} f = \operatorname{Im} f^2$

Soit G un groupe fini et f un morphisme de G dans G. Montrer que

$$\operatorname{Ker} f = \operatorname{Ker} f^2 \Longleftrightarrow \operatorname{Im} f = \operatorname{Im} f^2.$$

(École normale supérieure)

Solution.

• On observe que l'on a $\operatorname{Ker} f \subset \operatorname{Ker} f^2$ et $\operatorname{Im} f^2 \subset \operatorname{Im} f$. Ces ensembles étant tous finis, on en déduit que $\operatorname{Ker} f = \operatorname{Ker} f^2$ équivaut à $|\operatorname{Ker} f| = |\operatorname{Ker} f^2|$ et $\operatorname{Im} f = \operatorname{Im} f^2$ à $|\operatorname{Im} f| = |\operatorname{Im} f^2|$. Il s'agit de démontrer que ces deux égalités de cardinaux sont équivalentes.

• Montrons que si $f : \mathrm{G} \to \mathrm{G}$ est un morphisme de groupes, alors $|\mathrm{G}| = |\operatorname{Im} f| \times |\operatorname{Ker} f|$. Soit $\mathcal{R}$ la relation d'équivalence associée à f : $x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$. L'ensemble quotient $\mathrm{G}/\mathcal{R}$ est équipotent à $\operatorname{Im} f$. Mais d'autre part, $f(x) = f(y)$ équivaut à $f(x^{-1}y) = 1$, puisque f est un morphisme et donc à $x^{-1}y \in \operatorname{Ker} f$. La classe $\overline{x}$ d'un élément x pour $\mathcal{R}$ est donc la classe à gauche modulo $\operatorname{Ker} f$: $\overline{x} = x \operatorname{Ker} f$. Ainsi, $\overline{x}$ est équipotent à $\operatorname{Ker} f$ (par la bijection $g \in \operatorname{Ker} f \longmapsto xg \in \overline{x}$). Les classes ont donc toutes même cardinal, celui de $\operatorname{Ker} f$. On en déduit que

$$|\mathrm{G}| = |\mathrm{G}/\mathcal{R}| \times |\operatorname{Ker} f| = |\operatorname{Im} f| \times |\operatorname{Ker} f|.$$

On a donc, pour tout morphisme f de G,

$$|\mathrm{G}| = |\operatorname{Im} f| \times |\operatorname{Ker} f|.$$

On obtient de même

$$|\mathrm{G}| = |\operatorname{Im} f^2| \times |\operatorname{Ker} f^2|.$$

Ces deux égalités impliquent l'équivalence entre $|\operatorname{Im} f| = |\operatorname{Im} f^2|$ et $|\operatorname{Ker} f| = |\operatorname{Ker} f^2|$, ce qui établit le résultat demandé. ◁

Voici quelques rappels sur la notion de groupe quotient dans le cas abélien. Soit G *un groupe abélien, et* H *un sous-groupe de* G. *La relation*

$\mathrm{R_H}$ *(dite de congruence modulo* H*) définie sur* G *par* $x\mathrm{R_H}y \Leftrightarrow x^{-1}y \in \mathrm{H}$ *est une relation d'équivalence. On note* $\overline{x} = x\mathrm{H} = \mathrm{H}x$ *la classe d'un élément* x *de* G *et* G/H *l'ensemble quotient. La loi de* G *est alors compatible avec le passage au quotient, c'est-à-dire que la classe* $\overline{xy}$ *ne dépend pas du choix de* x *dans* $\overline{x}$ *et de* y *dans* $\overline{y}$*. Cela permet de définir une loi de composition interne sur* G/H *par* $\overline{x}.\overline{y} = \overline{xy}$*, loi qui munit* G/H *d'une structure de groupe, appelé groupe quotient de* G *par* H*. Les quotients de* $\mathbb{Z}$ *sont des exemples fondamentaux qui ont été étudiés en cours.*

Rappelons enfin le premier théorème d'isomorphisme dans le cas abélien. Si $f : \mathrm{G} \to \mathrm{G}'$ *est un morphisme de groupes, alors la relation d'équivalence associée à* f *et la relation de congruence modulo* $\operatorname{Ker} f$ *sont égales et la bijection canonique* $\overline{f}$ *de* $\mathrm{G}/\operatorname{Ker} f$ *sur* $\operatorname{Im} f$ *induite par* f *est un isomorphisme de groupes.*

2.5. Sous-groupes finis de $\mathbb{Q}/\mathbb{Z}$

> Montrer que, pour tout $n \geqslant 1$, il existe un unique sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ de cardinal n.
>
> **(École polytechnique)**

▷ **Solution.**

Soit $n \geqslant 1$ et G un sous-groupe de cardinal n de $\mathbb{Q}/\mathbb{Z}$. Si $x \in \mathbb{Q}$ est tel que $\overline{x} \in \mathrm{G}$, l'ordre de $\overline{x}$ divise n et donc $\overline{nx} = n\overline{x} = \overline{0}$. On en déduit qu'il existe $p \in \mathbb{Z}$ tel que $x = \dfrac{p}{n}\cdot$ Si r désigne le résidu de p modulo n, on a même $\overline{x} = \overline{\left(\dfrac{r}{n}\right)}$. Ceci montre que $\mathrm{G} \subset \left\{\overline{\left(\dfrac{r}{n}\right)}, 0 \leqslant r \leqslant n-1\right\}$. Les n éléments de cet ensemble sont distincts et ils forment un sous-groupe de $\mathbb{Q}/\mathbb{Z}$, le sous-groupe engendré par $\overline{\left(\dfrac{1}{n}\right)}$. D'après ce qui précède, c'est le seul sous-groupe de $(\mathbb{Q}/\mathbb{Z}, +)$ de cardinal n. ◁

Les exercices suivants concernent la notion d'ordre d'un élément dans un groupe. L'ordre d'un élément x *d'un groupe* G *est le cardinal (fini ou infini) du sous-groupe de* G *engendré par* x*. Si l'ordre de* x *est fini égal à* m*, ce sous-groupe est égal à* $\{e, x, x^2, \ldots, x^{m-1}\}$ *et isomorphe à* $\mathbb{Z}/m\mathbb{Z}$*. L'entier* m *est le plus petit* $k \in \mathbb{N}^*$ *tel que* $x^k = e$*. Dans le cas où l'ordre de* x *est infini, le sous-groupe qu'il engendre est isomorphe à* $\mathbb{Z}$*.*

Lorsque G *est fini, l'ordre de tout* x *divise le cardinal de* G *(c'est un corollaire du théorème de Lagrange). Bien entendu il n'y a pas, en général, d'élément d'ordre* d *pour tout diviseur* d *de* $|\mathrm{G}|$ *(sans quoi tous les groupes finis seraient cycliques). Le lemme de Cauchy, qui fera plus loin l'objet d'un exercice, montre que si* G *est fini de cardinal* n*, alors*

G admet, pour tout diviseur premier p de n, des éléments d'ordre p. Les deux exercices qui suivent deviennent très simples dès lors que l'on dispose de ce lemme. Nous en donnons toutefois des solutions n'y faisant pas appel et qui sont sans doute plus dans l'esprit de ce qu'attendait l'examinateur.

2.6. Groupes abéliens de cardinal pq

Soit G un groupe abélien d'ordre pq, où p et q sont deux nombres premiers distincts. Montrer que G est cyclique.

(École normale supérieure)

▷ **Solution.**

Nous noterons la loi du groupe multiplicativement. Comme p et q sont premiers, les éléments de G différents de 1 sont d'ordre pq, p ou q d'après le théorème de Lagrange.

• Montrons que si G admet un élément x d'ordre p et un élément y d'ordre q, alors xy est d'ordre pq. On a $xy \neq 1$, car sinon $y = x^{-1}$ a même ordre que x, $(xy)^p = y^p \neq 1$ car q ne divise pas p et, de même, $(xy)^q \neq 1$. L'ordre de xy ne peut être que pq. À l'aide du lemme de Cauchy (voir 2.10) on pourrait donc conclure ici.

• Si G n'est pas cyclique, *i.e.* ne possède pas d'élément d'ordre pq, on en déduit que les éléments de G distincts de 1 sont tous d'ordre p ou tous d'ordre q. Supposons-les par exemple tous d'ordre p. Soit x un élément d'ordre p et H le sous-groupe qu'il engendre. On considère le groupe quotient G/H de cardinal q. Comme q est premier, le cours assure que G/H est cyclique. Soit $z \in$ G tel que $\overline{z}$ engendre G/H ; $\overline{z}$ est donc d'ordre q. Mais on a aussi $\overline{z}^p = \overline{z^p} = \overline{1}$. Comme $\overline{z}$ est d'ordre q, on en déduit q divise p, ce qui est absurde.

Conclusion. G est cyclique. ◁

Le résultat n'est bien entendu plus vrai si G *n'est pas supposé abélien : le groupe $\mathcal{S}_3$ est d'ordre $6 = 2 \times 3$ et n'est pas abélien (donc non cyclique).*

2.7. Un cas particulier du lemme de Cauchy

Soit G un groupe de cardinal $2p$ avec p premier. Montrer que G contient un élément d'ordre p.

(École normale supérieure)

▷ **Solution.**

D'après le théorème de Lagrange, les éléments de G sont d'ordre 1, 2, p ou $2p$. Raisonnons par l'absurde et supposons qu'il n'y ait pas

d'élément d'ordre p. Dans ces conditions, G n'est pas cyclique (car si x est un générateur de G, alors x^2 est d'ordre p) et si $x \in \mathrm{G}$, x est d'ordre 1 (si x est l'élément neutre) ou 2. En particulier, $p \geqslant 3$ et pour tout $x \in \mathrm{G}$, $x^2 = 1$. On peut alors prouver le lemme suivant, intéressant en soi :

Lemme. *Soit* G *un groupe tel que pour tout* $x \in \mathrm{G}$, $x^2 = 1$. *Alors* G *est abélien et* Card G *est une puissance de* 2.

Démonstration.

• Soit x et y dans G. Pour tout $z \in \mathrm{G}$ on a $z^2 = 1$, *i.e.* $z = z^{-1}$. On en déduit que

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

et G est abélien.

• Montrons par récurrence sur Card G que Card G est une puissance de 2.

Il n'y a rien à vérifier si $\mathrm{Card}\,\mathrm{G} = 1$.

Supposons $\mathrm{Card}\,\mathrm{G} \geqslant 2$. On considère les sous-groupes de G distincts de G ; il en existe, $\{1\}$ par exemple. On en choisit un de cardinal maximal que l'on note H. D'après l'hypothèse de récurrence, Card H est une puissance de 2. Soit $a \in \mathrm{G}\backslash\mathrm{H}$. Montrons que $\mathrm{H} \cup a\mathrm{H}$ est un sous-groupe de G ; en effet, il est égal au sous-groupe H′ engendré par a et H :

$*$ on a clairement $\mathrm{H} \cup a\mathrm{H} \subset \mathrm{H}'$;

$*$ réciproquement, a étant d'ordre 2, tout élément de H′ s'écrit $a^\alpha h$, avec $\alpha \in \{0, 1\}$ et $h \in \mathrm{H}$. D'où le résultat annoncé.

Les ensembles H et aH sont disjoints car sinon il existerait $h \in \mathrm{H}$ qui s'écrirait $h = ak$ avec $k \in \mathrm{H}$ et on aurait $a = hk^{-1} \in \mathrm{H}$, ce qui est exclu. On en déduit que $\mathrm{Card}(\mathrm{H} \cup a\mathrm{H}) = 2\,\mathrm{Card}\,\mathrm{H}$. Par maximalité du cardinal de H, $\mathrm{H} \cup a\mathrm{H} = \mathrm{G}$. En particulier, $\mathrm{Card}\,\mathrm{G} = 2\,\mathrm{Card}\,\mathrm{H}$ est une puissance de 2. ◇

Le cardinal de notre groupe G devrait être une puissance de 2. Mais $\mathrm{Card}\,\mathrm{G} = 2p$, avec $p \geqslant 3$ et premier. C'est contradictoire et G possède donc un élément d'ordre p. ◁

Un élégant argument d'algèbre linéaire permet de mieux saisir encore la structure de G *lorsque pour tout* $x \in \mathrm{G}$, $x^2 = e$ *:* G *est alors naturellement muni d'une structure d'espace vectoriel sur le corps* $\mathbb{Z}/2\mathbb{Z}$, *la loi externe étant définie par* $0.x = e$ *(neutre de* G*) et* $1.x = x$ *pour tout* x *de* G, *et la loi de groupe étant bien entendu celle de* G. *La propriété vérifiée par* G *intervient dans l'axiome de distributivité :* $(1 + 1).x = 0.x = e$ *et* $(1.x)(1.x) = x^2 = e$. *On laisse au lecteur le soin de vérifier les autres axiomes. Comme* G *est fini, il est de dimension finie en tant que* $\mathbb{Z}/2\mathbb{Z}$*-espace vectoriel. Si on note* n *cette dimension,* G *est isomorphe à* $(\mathbb{Z}/2\mathbb{Z})^n$ *en tant qu'espace vectoriel et* a fortiori *en tant que groupe.*

Le fait qu'un groupe abélien fini d'exposant 2 (voir ci-après) est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^k$ résulte aussi du théorème de structure des groupes abéliens finis (cf. exercice 2.20 pour l'unicité et 7.22 pour l'existence).

2.8. Exposant d'un groupe abélien fini

Soit G un groupe abélien fini. Pour tout $x \in G$, on note $O(x)$ l'ordre de x.

1. Soit $(x, y) \in G^2$, $m = O(x)$, $n = O(y)$. On suppose que m et n sont premiers entre eux. Montrer que $O(xy) = mn$. Si on ne suppose plus m premier avec n, a t-on $O(xy) = \text{ppcm}(m, n)$?

2. Soit $(m, n) \in (\mathbb{N}^*)^2$. Montrer l'existence de $(m', n') \in (\mathbb{N}^*)^2$ tel que $m'|m$, $n'|n$, $\text{pgcd}(m', n') = 1$ et $\text{ppcm}(m, n) = m'n'$.

3. Montrer qu'il existe $z \in G$ tel que $O(z)$ soit le ppcm des ordres des éléments de G (ce ppcm est appelé l'exposant du groupe G).

4. Soit K un corps commutatif, G un sous-groupe fini du groupe multiplicatif K^*. Montrer que G est cyclique.

(**École normale supérieure**)

1. Solution.

1. Supposons m et n premiers entre eux et considérons $k \in \mathbb{Z}$ tel que $(xy)^k = 1$. Élevons cette égalité à la puissance n. Comme G est abélien il vient $x^{kn} = 1$. Donc m divise kn. Comme $n \wedge m = 1$, le lemme de Gauss garantit que m divise k. On montre de la même manière que n divise k, puis que nm divise k, à nouveau parce que $n \wedge m = 1$. Comme $(xy)^{mn} = 1$, il en résulte que $O(xy) = mn$.

L'hypothèse «m et n sont premiers entre eux» est essentielle : en effet, si on prend par exemple $y = x^{-1}$, l'élément $xy = 1$ est d'ordre 1 alors que $O(x) = O(y)$ et donc que $\text{ppcm}(O(x), O(y)) = n$.

2. Écrivons $m = \prod_{p \in \mathcal{P}} p^{\nu_p(m)}$ et $n = \prod_{p \in \mathcal{P}} p^{\nu_p(n)}$, où $\mathcal{P}$ désigne l'ensemble des nombres premiers. On a alors

$$\text{ppcm}(m, n) = \prod_{p \in \mathcal{P}} p^{\max(\nu_p(m), \nu_p(n))}.$$

Soit $(m', n') \in \mathbb{N}^*$. Pour que $m'|m$ et $n'|n$, il faut et il suffit que pour tout $p \in \mathcal{P}$, $\nu_p(m') \leqslant \nu_p(m)$ et $\nu_p(n') \leqslant \nu_p(n)$. Pour que m' et n' soient premiers entre eux, il faut et il suffit que pour tout $p \in \mathcal{P}$, $\nu_p(m') = 0$ ou $\nu_p(n') = 0$. Enfin, pour que $m'n' = \text{ppcm}(m, n)$, il faut et il suffit que pour tout $p \in \mathcal{P}$, $\nu_p(m') + \nu_p(n') = \max(\nu_p(m), \nu_p(n))$. Tout cela nous invite à poser

$$m' = \prod_{p \in \mathcal{P}} p^{\alpha_p} \quad \text{et} \quad n' = \prod_{p \in \mathcal{P}} p^{\beta_p}$$

avec, pour tout $p \in \mathcal{P}$,

$$\alpha_p = \begin{cases} \nu_p(m) & \text{si } \nu_p(m) > \nu_p(n) \\ 0 & \text{si } \nu_p(n) \geqslant \nu_p(m) \end{cases} \quad \text{et} \quad \beta_p = \begin{cases} 0 & \text{si } \nu_p(m) > \nu_p(n) \\ \nu_p(n) & \text{si } \nu_p(n) \geqslant \nu_p(m). \end{cases}$$

Les entiers m' et n' vérifient alors toutes les conditions demandées.

3. Considérons un élément z de G d'ordre maximal m. Soit x un élément de G d'ordre n. On choisit m' et n' comme à la question 2. L'élément $z^{m/m'}$ est d'ordre m' : en effet, on a $(z^{m/m'})^{m'} = z^m = 1$ et si $(z^{m/m'})^k = 1$, avec $k > 0$, on obtient $z^{mk/m'} = 1$ et nécessairement $mk/m' \geqslant m$, *i.e.* $k \geqslant m'$. De même, $x^{n/n'}$ est d'ordre n'. D'après la question 1, $z^{m/m'}x^{n/n'}$ est d'ordre $m'n' = \text{ppcm}(m,n)$. Or, par construction, cet ordre est inférieur à m. On a donc $\text{ppcm}(m,n) \leqslant m$, c'est-à-dire $\text{ppcm}(m,n) = m$ et n divise m.

L'ordre m de z est donc multiple de tous les ordres des éléments de G. C'est évidemment le plus petit, m étant lui-même l'ordre de z. C'est donc le ppcm des ordres des éléments de G.

4. Soit m le ppcm des ordres des éléments de G et n le cardinal de G. Comme $x^m = 1$ pour tout x de G, on a

$$\mathrm{G} \subset \{x \in \mathrm{K},\ x^m - 1 = 0\}.$$

Or, l'ensemble des racines de $\mathrm{X}^m - 1 \in \mathrm{K}[\mathrm{X}]$ est fini, de cardinal au plus m. On a donc $n \leqslant m$. Mais l'inégalité $m \leqslant n$ est également vérifiée puisqu'il existe $z \in \mathrm{G}$ d'ordre m. Finalement on obtient $m = n$ et z est un générateur de G, qui est cyclique. $\lhd$

Il résulte notamment de la question 4 que, pour p premier, le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ est cyclique. Le lecteur trouvera une autre preuve de ce résultat très important dans l'exercice 4.13.

2.9. Puissances dans un groupe abélien d'exposant fini

Soit G un groupe abélien. On suppose qu'il existe $n \in \mathbb{N}^*$ tel que $x^n = 1$ pour tout $x \in \mathrm{G}$.

1. On suppose que $n = ab$, avec $\text{pgcd}(a,b) = 1$, et on considère $\mathrm{G}_a = \{x^a,\ x \in \mathrm{G}\}$. Montrer que G_a est un sous-groupe de G. On définit de même G_b. Montrer que pour tout $x \in \mathrm{G}$, il existe un unique $(u,v) \in \mathrm{G}_a \times \mathrm{G}_b$ tel que $x = uv$.

2. Soit k un entier naturel premier avec n. Montrer que l'application $x \longmapsto x^k$ est un automorphisme de G. Déterminer l'application réciproque.

(École normale supérieure)

Solution.

1. Pour tout entier k, l'application $f_k : x \longmapsto x^k$ est un morphisme de groupes de G dans G, car G est abélien. Cela montre que $G_a = \operatorname{Im} f_a$ et $G_b = \operatorname{Im} f_b$ sont des sous-groupes de G.

Considérons le morphisme de groupes $\psi : G_a \times G_b \to G$ qui au couple (u, v) associe uv. Il s'agit de prouver que ψ est un isomorphisme.

• Injectivité. Soit $(u, v) \in G_a \times G_b$ tel que $uv = e$. Comme u s'écrit sous la forme $u = w^a$, on a $u^b = w^{ab} = e$. Donc l'ordre de u divise b. De même, l'ordre de v divise a. Or, $v = u^{-1}$ a le même ordre que u. Cet ordre divise donc a et b et comme a et b sont premiers entre eux, c'est 1. Ainsi $u = v = e$ et $\operatorname{Ker} \psi = \{(e, e)\}$.

• Surjectivité. Soit $x \in G$. Par le théorème de Bezout on peut trouver α et β tels que $1 = \alpha a + \beta b$. On a alors $x = (x^\alpha)^a (x^\beta)^b = \psi((x^\alpha)^a, (x^\beta)^b)$. D'où le résultat.

2. Montrons que f_k est injective en cherchant son noyau. Soit x dans $\operatorname{Ker} f_k$. On a $x^k = e$ et $x^n = e$ par hypothèse. L'ordre de x divise k et n ; c'est donc 1 puisque $\operatorname{pgcd}(n, k) = 1$. Ainsi, $x = e$ et $\operatorname{Ker} f_k = \{e\}$. Pour la surjectivité, on écrit une relation de Bezout entre k et n : $rk + sn = 1$. On a alors, pour tout $x \in G$, $x = x^{rk+sn} = (x^r)^k$. Donc f_k est bijective et $f_k^{-1} = f_r$. ◁

Les actions de groupe jouent un rôle essentiel dans bien des domaines des mathématiques. Tout d'abord en théorie des groupes. En regardant diverses actions d'un groupe G*, on peut obtenir beaucoup d'informations sur* G *lui-même (voir par exemple la preuve du lemme de Cauchy en 2.10). La théorie des représentations linéaires (*i.e. *des opérations linéaires d'un groupe sur un espace vectoriel) forme par exemple un pan entier de la théorie des groupes. Mais cette notion peut aussi se rencontrer en combinatoire lorsqu'on cherche à dénombrer les configurations d'un objet sur lequel un groupe agit : on se reportera par exemple à l'exercice 1.10 ou encore à l'exercice 6.21 qui donne une preuve de la formule de Burnside. Enfin, la notion d'opération de groupe est au cœur de la géométrie. Depuis le programme d'Erlangen de Felix Klein (1872), on comprend une géométrie comme l'étude de propriétés invariantes sous l'action d'un certain groupe.*

Dans le programme de Spéciales, le lecteur pourra avec un peu de recul se rendre compte que beaucoup de résultats sont des descriptions d'orbites pour certaines opérations de groupes : définition des angles orientés, recherche des classes de similitude de $\mathcal{M}_n(K)$*, classification des formes quadratiques...*

Voici un petit rappel de l'essentiel.

• *Une opération d'un groupe* G *sur un ensemble non vide* E *est un morphisme* φ *de* G *dans* $\mathcal{S}_E$ *le groupe symétrique de* E*. On note usuellement* $g \cdot x$ *au lieu de* $\varphi(g)(x)$ *pour* $(g, x) \in G \times E$.

• *Si* G *opère sur* E *la relation* $x\mathrm{R}y \iff \exists g \in \mathrm{G},\ g \cdot x = y$ *est une relation d'équivalence sur* E *dont les classes sont appelées orbites. L'opération est dite transitive s'il n'y a qu'une seule orbite. Si* $x \in \mathrm{E}$ *on note* $\mathrm{G}_x = \{g \in \mathrm{G},\ g \cdot x = x\}$ *le stabilisateur de* x. *C'est un sous-groupe de* G.

• *Dans les exercices on utilisera plusieurs fois l'important résultat suivant : si* G *est fini et si* x *est un élément de* E, *le cardinal de l'orbite de* x *sous l'action de* G *est égal à l'indice du stabilisateur de* x. *Démontrons-le. Notons* Ω_x *l'orbite de* x. *L'application* $f : \mathrm{G} \to \Omega_x$ *qui à* g *associe* $g \cdot x$ *est surjective par définition. Étudions la relation d'équivalence* R_f *associée à* f :

$$\begin{aligned} g\mathrm{R}_f g' &\iff f(g) = f(g') \iff g \cdot x = g' \cdot x \iff (g^{-1}g') \cdot x = x \\ &\iff g^{-1}g' \in \mathrm{G}_x \iff g' \in g\mathrm{G}_x. \end{aligned}$$

La classe d'équivalence de $g \in \mathrm{G}$ *est donc la classe à droite* $g\mathrm{G}_x$; *elle est de cardinal* $|\mathrm{G}_x|$. *Toutes les classes d'équivalence ont donc le même cardinal. Comme l'ensemble quotient* G/R_f *est en bijection avec* Ω_x *on a bien*

$$\boxed{\operatorname{Card} \Omega_x = \frac{\operatorname{Card} \mathrm{G}}{\operatorname{Card} \mathrm{G}_x}}.$$

• *L'équation aux classes consiste à écrire, lorsque* E *est fini, que le cardinal de* E *est égal à la somme des cardinaux des différentes orbites. Elle permet souvent des raisonnements combinatoires ou arithmétiques comme dans la preuve suivante du lemme de Cauchy donnée par MacKay en 1959.*

2.10. Lemme de Cauchy

1. Soit G un groupe fini de cardinal p^m (avec p premier et m dans $\mathbb{N}^*$) qui opère sur un ensemble fini non vide E. On considère

$$\mathrm{E}^{\mathrm{G}} = \{x \in \mathrm{E},\ \forall g \in \mathrm{G},\ g \cdot x = x\}.$$

Montrer que $|\mathrm{E}^{\mathrm{G}}| \equiv |\mathrm{E}| \pmod p$.

2. Soit H un groupe fini d'ordre n et p un diviseur premier de n. Montrer que H contient un élément d'ordre p (*lemme de Cauchy*). On pourra, pour ce faire, utiliser une opération de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble E des $(x_1, \ldots, x_p) \in \mathrm{H}^p$ tels que $x_1 x_2 \ldots x_p = e$.

3. Soit H un groupe fini d'ordre n et m dans $\mathbb{N}^*$ tel que, pour tout $x \in \mathrm{H}$, $x^m = e$. Montrer que n divise une puissance de m.

(**École normale supérieure**)

Solution.

1. Si $x \in \mathrm{E}$, on notera $\mathrm{O}(x)$ l'orbite de x sous l'action de G. Les éléments de E^{G} sont exactement les éléments x de E tels que $\mathrm{O}(x) = \{x\}$. Notons $w_1, w_2, \ldots, w_p$ les orbites de E de cardinal strictement supérieur à 1. On sait que si x_i est un élément de w_i, le cardinal de w_i est l'indice du stabilisateur de x_i dans G : c'est donc une puissance de p. Il résulte de l'équation aux classes que

$$|\mathrm{E}| = |\mathrm{E}^{\mathrm{G}}| + \sum_{i=1}^{p} |w_i| \equiv |\mathrm{E}^{\mathrm{G}}| \quad [p].$$

2. Soit $(x_1, \ldots, x_p)$ un élément de E. On a donc $x_1 x_2 \ldots x_p = e$. En multipliant à gauche par x_1^{-1} et à droite par x_1 il vient $x_2 x_3 \ldots x_p x_1 = e$, c'est-à-dire $(x_2, \ldots, x_p, x_1) \in \mathrm{E}$.

Notons c le cycle $(1, 2, \ldots, p)$ élément du groupe symétrique $\mathcal{S}_p$. Il s'agit d'un élément d'ordre p qui engendre un groupe cyclique K isomorphe à $\mathbb{Z}/p\mathbb{Z}$. On définit une opération de K sur l'ensemble H^p par $c \cdot (x_1, \ldots, x_p) = (x_{c(1)}, x_{c(2)}, \ldots, x_{c(p)}) = (x_2, \ldots, x_p, x_1)$. La remarque ci-dessus montre que E est stable par cette opération. Appliquons alors le résultat de la question précédente à l'opération induite sur E. On a : $|\mathrm{E}| \equiv |\mathrm{E}^{\mathrm{K}}| \; [p]$. Le cardinal de E est n^{p-1} : on peut choisir $x_1, \ldots, x_{p-1}$ quelconques ; x_p est alors déterminé de manière unique. Comme p divise n, $|\mathrm{E}^{\mathrm{K}}|$ est nul modulo p. Or, les éléments de E^{K} sont justement les p-uplets $(x, x, \ldots, x)$ avec $x^p = e$. Comme E^{K} est non vide puisqu'il contient le p-uplet $(e, e, \ldots, e)$, il a un cardinal supérieur à p. Il y a donc au moins $p - 1$ éléments d'ordre p dans H.

3. Il suffit de montrer que tous les facteurs premiers de n sont des facteurs premiers de m. Soit p premier divisant n. Le lemme de Cauchy garantit l'existence d'un élément $x \in \mathrm{H}$ d'ordre p. Or, par hypothèse $x^m = e$. C'est donc que p divise m. $\lhd$

Le défaut de commutativité d'un groupe G *se mesure à l'aide de son centre. Il s'agit du sous-groupe* Z(G) *formé des éléments de* G *qui commutent avec tous les autres. Le lecteur montrera par exemple que le centre du groupe symétrique* $\mathcal{S}_n$ *est réduit à l'identité pour* $n \geqslant 3$. *L'exercice suivant se propose de prouver que le centre d'un* p*-groupe ne peut pas être trivial.*

2.11. Centre d'un p-groupe

Soit G un groupe fini et $a \in \mathrm{G}$.

1. Montrer que le nombre de conjugués de a est égal à l'indice dans G du centralisateur de a.

On suppose que G est de cardinal p^m avec p premier et $m \geqslant 1$.
2. Montrer que le centre de G est d'ordre p^k avec $0 < k \leqslant m$.
3. On suppose $m = 2$. Montrer que G est abélien.
(École polytechnique)

▷ **Solution.**

1. On considère l'action de G sur lui-même par conjugaison : si g et x sont dans G, $g \cdot x = gxg^{-1}$. L'ensemble Ω_a des conjugués de a est l'orbite de a et le centralisateur de a $\{g \in \mathrm{G},\ ga = ag\}$ n'est autre que le stabilisateur $\{g \in \mathrm{G}, gag^{-1} = a\} = \mathrm{G}_a$ de a pour cette opération. On a donc

$$\boxed{\operatorname{Card}\Omega_a = \frac{\operatorname{Card}\mathrm{G}}{\operatorname{Card}\mathrm{G}_a}}.$$

2. Notons $\mathrm{Z(G)} = \{a \in \mathrm{G},\ \forall g \in \mathrm{G},\ ag = ga\}$ le centre de G. Pour $a \in \mathrm{G}$, nous avons les équivalences :

$$a \in \mathrm{Z(G)} \iff \forall g \in \mathrm{G},\ gag^{-1} = a \iff \Omega_a = \{a\}$$

Écrivons que G est réunion disjointe des classes de conjugaison. La question précédente assure que le cardinal d'une classe de conjugaison est un diviseur de $\operatorname{Card}\mathrm{G} = p^m$. Si elle n'est pas réduite à un singleton, son cardinal est de la forme p^k avec $k \geqslant 1$ donc est nul modulo p. Ainsi, on obtient

$$\operatorname{Card}\mathrm{G} = \sum_{\Omega \text{ orbite}} \operatorname{Card}\Omega = \operatorname{Card}\mathrm{Z(G)} + \sum_{\substack{\Omega \text{ orbite} \\ \operatorname{Card}\Omega \geqslant 2}} \operatorname{Card}\Omega$$

et, modulo p, il reste $0 \equiv \operatorname{Card}\mathrm{G} \equiv \operatorname{Card}\mathrm{Z(G)}$. Donc p divise $\operatorname{Card}\mathrm{Z(G)}$. Or, Z(G) est un sous-groupe de G, donc son cardinal est de la forme p^k avec $0 \leqslant k \leqslant m$, d'après le théorème de Lagrange. Comme p divise $\operatorname{Card}\mathrm{Z(G)}$, k est nécessairement supérieur ou égal à 1.

3. Soit $\varphi : g \in \mathrm{G} \longmapsto \varphi_g \in \mathcal{S}_\mathrm{G}$ où $\mathcal{S}_\mathrm{G}$ est le groupe des permutations de G et φ_g le morphisme de conjugaison $x \longmapsto gxg^{-1}$. On a pour tout $g, g' \in \mathrm{G}$, $\varphi_{gg'} = \varphi_g \circ \varphi'_g$ et l'application φ est un morphisme[1] de G sur un sous-groupe de $\mathcal{S}_\mathrm{G}$, noté Int G et appelé groupe des automorphismes intérieurs de G. Le noyau de φ est exactement le centre de G. Comme ce centre n'est pas réduit à l'élément neutre d'après la question précédente, la relation $|\mathrm{G}| = |\operatorname{Im}\varphi|.|\operatorname{Ker}\varphi|$ (voir exercice 2.4) donne $|\operatorname{Int}\ \mathrm{G}| = 1$ ou p. Comme p est premier, Int G est cyclique dans les deux cas. Il existe

1. Cela traduit le fait que la conjugaison est une opération de groupes.

donc $g_0 \in G$ tel que, pour tout $g \in G$, il existe $k \in \mathbb{Z}$ vérifiant $\varphi_g = \varphi_{g_0}^k$, c'est-à-dire

$$\forall x \in G, \quad gxg^{-1} = g_0^k x g_0^{-k}.$$

Mais alors, g_0 est dans le centre de G puisque $gg_0g^{-1} = g_0^k g_0 g_0^{-k} = g_0$ et $gg_0 = g_0 g$. Ainsi φ_{g_0} est l'identité et $|\operatorname{Int} G| = 1$. Donc, $Z(G) = G$ et G est un groupe abélien. $\lhd$

Il existe en revanche des groupes non abéliens d'ordre p^3 et par suite des groupes non abéliens d'ordre p^m pour tout $m \geqslant 3$.

L'exercice suivant évalue la proportion d'éléments d'un groupe non abélien qui commutent, proportion qui est reliée au nombre de classes de conjugaison.

2.12. Nombre de classes de conjugaison

Soit G un groupe fini non abélien. On note $n(G)$ le nombre de couples d'éléments de G qui commutent divisé par le nombre total de couples de G. Montrer que $n(G) \leqslant \frac{5}{8}$.

(École polytechnique)

Solution.

• On va commencer par interpréter $n(G)$. Pour tout $a \in G$, on note C_a le centralisateur de a, c'est-à-dire l'ensemble des éléments de G qui commutent avec a. On obtient alors

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

Or, on sait que l'indice de C_a dans G est égal au cardinal de la classe de conjugaison de a. En notant $w_1, \ldots, w_k$ les classes de conjugaison de G, il vient alors

$$n(G) = \frac{1}{|G|^2} \sum_{i=1}^{k} \sum_{a \in w_i} |C_a| = \frac{1}{|G|^2} \sum_{i=1}^{k} \sum_{a \in w_i} \frac{|G|}{|w_i|} = \frac{1}{|G|^2} \sum_{i=1}^{k} |G| = \frac{k}{|G|}.$$

On est ramené à prouver que pour un groupe fini non commutatif, on a $k \leqslant \frac{5}{8}|G|$. Le résultat est bien entendu faux si G est abélien, puisque dans ce cas il y a $|G|$ classes de conjugaison (réduites à des singletons).

• De manière générale, la classe de conjugaison d'un élément a de G est un singleton si et seulement si a est dans le centre de G, que l'on notera $Z(G)$. Les autres classes ayant au moins deux éléments, on a l'inégalité

$$|Z(G)| + 2(k - |Z(G)|) \leqslant |G|.$$

Celle-ci, divisée par $|G|$ montre que

$$n(G) = \frac{k}{|G|} \leqslant \frac{1}{2} + \frac{|Z(G)|}{2|G|}.$$

Il nous suffit donc, pour conclure, de prouver que $\frac{|Z(G)|}{2|G|} \leqslant \frac{1}{8}$, c'est-à-dire que l'indice de $Z(G)$ dans G est supérieur ou égal à 4.

Nous raisonnons par l'absurde. L'indice de $Z(G)$ dans G est supérieur ou égal à 2, car G n'est pas commutatif.

Supposons d'abord que $Z(G)$ soit d'indice 2 : $|G| = 2|Z(G)|$. On a alors $G = Z(G) \cup aZ(G)$, où a est un élément quelconque n'appartenant pas à $Z(G)$. Par définition, a commute avec les éléments de $Z(G)$. Soit $b \in aZ(G)$, que l'on écrit az, où z est central. Alors a commute avec a lui-même et avec z, donc avec b. Ainsi, a commute avec tous les éléments de G : c'est absurde.

Supposons maintenant que $Z(G)$ soit d'indice 3 : $|G| = 3|Z(G)|$. On considère les classes à droite modulo $Z(G)$: $Z(G)$, $aZ(G)$ et $bZ(G)$. L'élément a commute avec tout élément de $Z(G)$ et avec tout élément de $aZ(G)$ (comme précédemment). Montrons qu'il commute aussi avec les éléments de $bZ(G)$. Pour cela, il suffit de prouver qu'il commute avec b. Or, ab n'est pas dans $aZ(G)$, car b n'est pas central. S'il est dans $bZ(G)$, alors $b^{-1}ab$ est central. On en déduit que $ab = bb^{-1}ab = b^{-1}ab^2$ et donc que $ba = ab$. Sinon, ab est dans $Z(G)$. Mais alors, $aba^{-1} = a^{-1}ab = b$ et donc $ab = ba$. Dans tous les cas, on obtient que a commute avec b, donc est central, ce qui est faux. $\lhd$

En fait, le lecteur connaissant la notion de groupe quotient pourra montrer plus généralement que si $G/Z(G)$ est un groupe cyclique alors G est abélien (et le quotient est donc trivial). Comme tout groupe d'ordre 2 ou 3 est cyclique, il en résulte que dans un groupe non abélien le centre est au moins d'indice 4. On retrouve aussi qu'un groupe d'ordre p^2 avec p premier est cyclique (question 3 de l'exercice 2.11).

2.13. Sous-groupe d'indice infini

Soit G un groupe et H un sous-groupe de G d'indice infini, c'est-à-dire qu'il existe une suite infinie (x_n) d'éléments de G telle que les x_nH soient deux à deux distincts. Soit $H_1, ..., H_p$ des sous-groupes de G tels que $G = H \cup H_1 \cup \cdots \cup H_p$. Montrer que $G = H_1 \cup \cdots \cup H_p$.

(École normale supérieure)

1 · **Solution.**

Raisonnons par l'absurde et supposons l'existence d'un élément h dans $\mathrm{H}\setminus(\mathrm{H}_1\cup\ldots\cup\mathrm{H}_p)$. On considère une suite $(x_n)_{n\in\mathbb{N}}$ de G telle que les $x_n\mathrm{H}$ sont deux à deux distincts. En particulier, au plus un des $x_n\mathrm{H}$ peut être égal à H et dans ce cas, on peut supposer que c'est le premier $x_0\mathrm{H}$. On supposera donc que, pour $n\geqslant 1$, les x_n ne sont pas dans H.

Pour tout $n\geqslant 1$, il existe $i\in[\![1,p]\!]$ tel que $x_n\in\mathrm{H}_i$. D'après le lemme des tiroirs, il existe $i_1\in[\![1,p]\!]$ tel que $x_n\in\mathrm{H}_{i_1}$ pour une infinité d'indices n. On peut donc extraire de $(x_n)_{n\geqslant 1}$ une suite $(x_n^{(1)})_{n\geqslant 0}$ d'éléments de $\mathrm{H}_{i_1}\setminus\mathrm{H}$. Pour $n\neq m$, on a $x_n^{(1)}\mathrm{H}\neq x_m^{(1)}\mathrm{H}$.

Considérons pour $n\in\mathbb{N}$, $y_n=hx_n^{(1)}$ qui n'est ni dans H (sinon $x_n^{(1)}\in\mathrm{H}$), ni dans H_{i_1} (sinon $h\in\mathrm{H}_{i_1}$). Pour tout n, y_n est dans l'un des H_i avec $i\neq i_1$. Il existe donc une sous-suite $(z_n)_{n\in\mathbb{N}}$ de $(y_n)_{n\in\mathbb{N}}$ dont les éléments sont dans le même sous-groupe H_{i_2} avec $i_2\neq i_1$. On pose $x_n^{(2)}=z_0^{-1}z_n$ pour $n\in\mathbb{N}$. On a $x_n^{(2)}\in\mathrm{H}_{i_2}$ puisque H_{i_2} est un sous-groupe. D'autre part, de $z_0=hx_k^{(1)}$ et $z_n=hx_\ell^{(1)}$ avec $k,\ell\in\mathbb{N}$, on déduit $x_n^{(2)}=\left[x_k^{(1)}\right]^{-1}x_\ell^{(1)}\in\mathrm{H}_{i_1}$. De plus, si $m\in\mathbb{N}$ et $z_m=hx_r^{(1)}$, on a

$$x_m^{(2)}\mathrm{H}=x_n^{(2)}\mathrm{H}\iff z_m\mathrm{H}=z_n\mathrm{H}\iff x_r^{(1)}\mathrm{H}=x_\ell^{(1)}\mathrm{H}\iff r=\ell$$

et finalement,

$$x_m^{(2)}\mathrm{H}=x_n^{(2)}\mathrm{H}\iff m=n.$$

On dispose donc d'une suite $\left(x_n^{(2)}\right)_{n\geqslant 0}$ de $\mathrm{H}_{i_1}\cap\mathrm{H}_{i_2}$ pour laquelle les $x_n^{(2)}\mathrm{H}$ sont deux à deux distincts.

On réitère le procédé : supposons construite pour $q<p$ une suite $\left(x_n^{(q)}\right)_{n\geqslant 0}$ de $\mathrm{H}_{i_1}\cap\ldots\cap\mathrm{H}_{i_q}$ pour laquelle les $x_n^{(q)}\mathrm{H}$ sont deux à deux distincts. Au plus un terme de la suite peut être dans H et on peut supposer que c'est le premier $x_0^{(q)}$.

Considérons pour $n\in\mathbb{N}^*$, $y_n=hx_n^{(q)}$ qui n'est ni dans H (sinon $x_n^{(q)}\in\mathrm{H}$), ni dans $\mathrm{H}_{i_1}\cap\ldots\cap\mathrm{H}_{i_q}$ par hypothèse sur h. Pour tout n, y_n est dans l'un des H_i avec $i\notin\{i_1,\ldots i_q\}$. Il existe donc une sous-suite $(z_n)_{n\in\mathbb{N}}$ de $(y_n)_{n\in\mathbb{N}}$ dont les éléments sont dans le même sous-groupe $\mathrm{H}_{i_{q+1}}$ avec $i_{q+1}\notin\{i_1,\ldots,i_q\}$. On pose $x_n^{(q+1)}=z_0^{-1}z_n$ pour $n\in\mathbb{N}$. On a $x_n^{(q+1)}\in\mathrm{H}_{i_{q+1}}$ puisque $\mathrm{H}_{i_{q+1}}$ est un sous-groupe. De manière analogue à ce qui a été fait précédemment, $x_n^{(q+1)}$ s'écrit après simplification comme produit de deux éléments de $\mathrm{H}_{i_1}\cap\ldots\cap\mathrm{H}_{i_q}$ et les $x_n^{(q+1)}\mathrm{H}$ sont des parties deux à deux distinctes. On dispose donc d'une suite $\left(x_n^{(q+1)}\right)_{n\geqslant 0}$ de $\mathrm{H}_{i_1}\cap\ldots\cap\mathrm{H}_{i_q}\cap\mathrm{H}_{i_{q+1}}$ pour laquelle les $x_n^{(q+1)}\mathrm{H}$ sont deux à deux distincts.

Au final, on obtient une suite $\left(x_n^{(p)}\right)_{n\geqslant 0}$ de $\mathrm{H}_{i_1}\cap\ldots\cap\mathrm{H}_{i_p}$, c'est-à-dire de $\mathrm{H}_1\cap\ldots\cap\mathrm{H}_p$ avec les $x_n^{(p)}\mathrm{H}$ deux à deux distincts. On choisit $n\in\mathbb{N}$ tel que $x=x_n^{(p)}\notin\mathrm{H}$. Dans ces conditions, xh ne peut appartenir ni à H, ni à aucun des H_i. Comme $\mathrm{G}=\mathrm{H}\cup\mathrm{H}_1\cup\ldots\cup\mathrm{H}_p$, on aboutit à une contradiction. $\lhd$

2.14. Un théorème de Frobenius (1895)

Soit G un groupe fini, H un sous-groupe de G. On suppose que $\operatorname{Card}\mathrm{G}=p\operatorname{Card}\mathrm{H}$, où p est le plus petit diviseur premier de Card G. Montrer que H est distingué dans G, c'est-à-dire que l'on a, pour tout $x\in\mathrm{G}$, $x\mathrm{H}x^{-1}=\mathrm{H}$.

(**École polytechnique**)

$\rhd$ **Solution.**

• On considère les classes à gauche modulo H *i.e.* les $g\mathrm{H}$ où g parcourt G. On notera G/H l'ensemble de ces classes. Comme elles ont toutes le même cardinal que H, on obtient $\operatorname{Card}\mathrm{G}/\mathrm{H}=\dfrac{\operatorname{Card}\mathrm{G}}{\operatorname{Card}\mathrm{H}}\cdot$ Le groupe G agit naturellement sur G/H par translation à gauche : si $g\in\mathrm{G}$ et $x\in\mathrm{G}$, $g\cdot x\mathrm{H}=(gx)\mathrm{H}$. Mais on ne peut pas avoir d'information intéressante dans l'écriture de l'équation aux classes pour cette action, puisqu'il n'y qu'une seule orbite de cardinal p. On va plutôt regarder la restriction de cette action à H définie, pour $h\in\mathrm{H}$ et $x\in\mathrm{G}$, par $h\cdot x\mathrm{H}=(hx)\mathrm{H}$.

• On note $(\Omega_i)_{1\leqslant i\leqslant n}$ les orbites de G/H pour cette action. On sait que le cardinal de chaque Ω_i divise celui de H, donc celui de G. Écrivons alors l'équation aux classes qui exprime le fait que G/H est réunion disjointe des orbites sous l'action de H :

$$p=\operatorname{Card}\mathrm{G}/\mathrm{H}=\sum_{i=1}^{n}\operatorname{Card}\Omega_i.$$

L'orbite de H est bien sûr réduite au singleton $\{\mathrm{H}\}$. Les orbites qui ne sont pas des singletons ont un cardinal divisant $|\mathrm{G}|$; par hypothèse, un tel cardinal est supérieur ou égal à p. S'il existait une telle orbite, on aurait $\sum\limits_{i=1}^{n}\operatorname{Card}\Omega_i\geqslant p+1$, ce qui est impossible. Toutes les orbites sont donc réduites à des singletons.

• Ainsi, pour tout $x\in\mathrm{G}$ et tout $h\in\mathrm{H}$, on a

$$h\cdot x\mathrm{H}=(hx)\mathrm{H}=x\mathrm{H}$$

et donc $x^{-1}hx\in\mathrm{H}$. On obtient, pour tout $x\in\mathrm{G}$, l'inclusion $x^{-1}\mathrm{H}x\subset\mathrm{H}$

et donc l'égalité $x^{-1}\mathrm{H}x = \mathrm{H}$ puisque H et $x^{-1}\mathrm{H}x$ ont le même cardinal, ce qui montre que H est distingué dans G. ◁

L'exercice suivant montre que dans un groupe fini, un sous-groupe propre ne peut pas couper toutes les classes de conjugaison.

2.15. Classes de conjugaison

1. Soit G un groupe fini. H un sous-groupe strict de G. Montrer qu'il existe $x \in \mathrm{G}$ tel que la classe de conjugaison de x ne rencontre pas H.

2. Donner un contre-exemple si G n'est pas fini.

(École normale supérieure)

Solution.

1. Pour x et g dans G, on a $gxg^{-1} \in \mathrm{H} \iff x \in g^{-1}\mathrm{H}g$. Le problème revient donc à démontrer que la réunion $\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}$ des conjugués de H, n'est pas égale à G. Pour cela on va majorer le cardinal de cette réunion et montrer qu'elle contient strictement moins d'éléments que G (la seconde question peut nous faire songer à un argument combinatoire). On observe que si g et g' sont dans la même classe à gauche modulo H, c'est-à-dire s'il existe $h \in \mathrm{H}$ tel que $g' = gh$, alors $g'\mathrm{H}g'^{-1} = g(h\mathrm{H}h^{-1})g^{-1} = g\mathrm{H}g^{-1}$. Dans la réunion ci-dessus, on peut donc se contenter de prendre un système de représentants des classes à gauche modulo H. Soit $g_1, \ldots, g_k$ un tel système de représentants, $k = |\mathrm{G}|/|\mathrm{H}|$ étant l'indice de H dans G. Les conjugués de H ayant au moins l'élément neutre en commun, il vient

$$\left|\bigcup_{g\in\mathrm{G}} g\mathrm{H}g^{-1}\right| = \left|\bigcup_{i=1}^{k} g_i\mathrm{H}g_i^{-1}\right| \leqslant 1 + (|\mathrm{H}|-1)k = |\mathrm{G}| + 1 - \frac{|\mathrm{G}|}{|\mathrm{H}|} < |\mathrm{G}|,$$

car $|\mathrm{H}| < |\mathrm{G}|$ par hypothèse.

2. La preuve précédente utilise fortement la finitude de G. Le résultat ne s'étend pas à un groupe infini. Prenons par exemple $\mathrm{G} = \mathrm{GL}_n(\mathbb{C})$ et H le sous-groupe de G formé des matrices triangulaires supérieures inversibles. Toute matrice de $\mathrm{M}_n(\mathbb{C})$ étant trigonalisable, la classe de conjugaison de toute matrice A de G rencontre H. ◁

Une manière très féconde pour obtenir des groupes consiste à regarder le groupe de symétrie d'un «objet géométrique». Ainsi, dans l'espace euclidien de dimension 3, *la recherche des sous-groupes finis du groupe des*

rotations est-elle liée aux polyèdres réguliers. Ces derniers, au nombre de 5, étaient déjà connus de Platon. L'exercice suivant propose la partie analyse du travail et détermine les caractéristiques que doit avoir un sous-groupe fini de $\mathrm{SO}_3(\mathbb{R})$.

2.16. Sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$

Soit X un ensemble et G un sous-groupe fini du groupe $\mathcal{S}_{\mathrm{X}}$ des bijections de X. Pour $y \in \mathrm{X}$, on note $\mathrm{X}_y = \{g(y),\ g \in \mathrm{G}\}$ l'orbite de y sous l'action de G et $\mathrm{G}_y = \{g \in \mathrm{G},\ g(y) = y\}$ le stabilisateur de y dans G.

1. Pour tout $y \in \mathrm{X}$, prouver que $|\mathrm{G}| = |\mathrm{G}_y| \times |\mathrm{X}_y|$.

2. Montrer que pour $(x, y) \in \mathrm{X}^2$, si $x \in \mathrm{X}_y$, alors $\mathrm{X}_x = \mathrm{X}_y$.

3. a. Désormais, X est la sphère unité de $\mathbb{R}^3$ muni de sa structure euclidienne canonique et G un sous-groupe fini du groupe des rotations. On note $\mathcal{T} = \{\mathrm{X}_y, y \in \mathrm{X}\}$ et pour $\mathrm{T} = \mathrm{X}_y \in \mathcal{T}$, $\nu(\mathrm{T}) = |\mathrm{G}_y|$. Prouver que

$$2|\mathrm{G}| - 2 = \sum_{\mathrm{T} \in \mathcal{T}} (\nu(\mathrm{T}) - 1)|\mathrm{T}|.$$

b. Quelles sont les valeurs possibles de $\nu(\mathrm{T})$?

(**École polytechnique**)

▷ **Solution.**

1. Cela a été rappelé dans le préambule aux exercices sur les opérations de groupes.

2. Soit $(x, y) \in \mathrm{X}^2$, avec $x \in \mathrm{X}_y$. On écrit $x = g_0(y)$ avec $g_0 \in \mathrm{G}$. On a alors $y = g_0^{-1}(x)$ et $y \in \mathrm{X}_x$. Si $z \in \mathrm{X}_x$, il existe $g \in \mathrm{G}$ tel que $z = g(x)$, d'où résulte $z = gg_0(y)$ et $z \in \mathrm{X}_y$. Ainsi $\mathrm{X}_x \subset \mathrm{X}_y$. Comme $y \in \mathrm{X}_x$, par symétrie du problème, on a $\mathrm{X}_y \subset \mathrm{X}_x$ et finalement l'égalité demandée.

3. a. Avant tout, remarquons que $|\mathrm{G}_y|$ ne dépend pas du choix de l'élément y, ce qui justifie la définition de $\nu(\mathrm{T})$. En effet, si $\mathrm{T} = \mathrm{X}_x = \mathrm{X}_y$, on a

$$|\mathrm{G}_x| = |\mathrm{G}|/|\mathrm{X}_x| = |\mathrm{G}|/|\mathrm{X}_y| = |\mathrm{G}_y|.$$

Rappelons qu'une rotation de $\mathbb{R}^3$ qui n'est pas l'identité admet une droite vectorielle (son axe) comme ensemble de points invariants. Par conséquent, si on note $\mathrm{G}' = \mathrm{G}\backslash\{\mathrm{I}\}$, où I désigne l'identité de $\mathbb{R}^3$, tout élément de G' admet exactement deux points fixes dans X (les points d'intersection de l'axe de la rotation avec la sphère X). Considérons

$$\mathrm{E} = \{(g, x) \in \mathrm{G}' \times \mathrm{X},\ g(x) = x\}$$

D'après ce que nous venons de dire, on a

$$|E| = 2|G'| = 2(|G| - 1) = 2|G| - 2.$$

Si on note $X' = \{x \in X,\ \exists g \in G',\ g(x) = x\}$, on obtient

$$E = \coprod_{x \in X'} \{(g, x) \in G' \times X,\ g(x) = x\},$$

le symbole $\coprod$ signifiant que la réunion est disjointe.

Or, si $x \in X$ est fixé, $\{(g, x) \in G' \times X,\ g(x) = x\} = (G_x \backslash \{I\}) \times \{x\}$ est de cardinal $\nu(X_x) - 1$. En particulier, $x \in X'$ si $\nu(X_x) > 1$. On en déduit que

$$|E| = \sum_{x \in X'} (\nu(X_x) - 1).$$

Puisque, pour $x \in X \setminus X'$, on a $\nu(X_x) - 1 = 0$, on peut encore écrire

$$|E| = \sum_{x \in X} (\nu(X_x) - 1).$$

Sachant que X est réunion disjointe des orbites T et que, quand x varie dans une orbite T, $\nu(X_x)$ reste égal à $\nu(T)$, on obtient

$$|E| = \sum_{T \in \mathcal{T}} (\nu(T) - 1)|T|.$$

On conclut que

$$2|G| - 2 = \sum_{T \in \mathcal{T}} (\nu(T) - 1)|T|.$$

b. La dernière relation peut s'écrire

$$(*) \quad 2 - \frac{2}{|G|} = \sum_{T \in \mathcal{T}} \left(1 - \frac{1}{\nu(T)}\right)$$

puisque $|G| = \nu(T)|T|$, pour toute orbite T.

La quantité $2 - \dfrac{2}{|G|}$ est strictement inférieure à 2 et pour tout $T \in \mathcal{T}$ tel que $\nu(T) \geqslant 2$, on a $1 - \dfrac{1}{\nu(T)} \geqslant \dfrac{1}{2}$. Par conséquent, il ne peut y avoir plus de trois termes non nuls dans la somme $\sum_{T \in \mathcal{T}} \left(1 - \dfrac{1}{\nu(T)}\right)$.

• Imaginons qu'il n'y a qu'une seule orbite avec $\nu(T) \geqslant 2$. Alors on a

$$0 < \frac{1}{\nu(T)} = \frac{2}{|G|} - 1 \leqslant 0,$$

ce qui est impossible. Il y a donc deux ou trois orbites T telles que $\nu(T) \geqslant 2$.

• Supposons qu'il y a deux orbites T avec $\nu(\mathrm{T}) \geqslant 2$: T_1 et T_2. N'oublions pas que $\nu(\mathrm{T}_1)$ et $\nu(\mathrm{T}_2)$ divisent $|\mathrm{G}|$ d'après le théorème de Lagrange. Écrivons $|\mathrm{G}| = \nu(\mathrm{T}_1)d_1 = \nu(\mathrm{T}_2)d_2$. Alors $(*)$ devient

$$2 - \frac{2}{|\mathrm{G}|} = 2 - \frac{d_1}{|\mathrm{G}|} - \frac{d_2}{|\mathrm{G}|},$$

d'où résulte $2 = d_1 + d_2$ et nécessairement $d_1 = d_2 = 1$. Les orbites T_1 et T_2 ont un seul élément.

Ainsi, on a deux points de X qui sont invariants par tous les éléments de G, ce qui signifie qu'ils sont sur les axes des rotations de G'. Ces deux points sont opposés et finalement toutes les rotations de G' admettent le même axe D. Le groupe G est alors abélien. Les restrictions des éléments de G au plan $\mathrm{P} = \mathrm{D}^{\perp}$ forment un sous-groupe fini de $\mathrm{SO}(\mathrm{P})$. Nous savons qu'un tel sous-groupe est cyclique, engendré par une rotation d'angle $\frac{2\pi}{n}$ (P étant muni d'une orientation arbitraire). G est donc constitué des rotations d'axe fixe D et d'angle $\frac{2k\pi}{n}$, $0 \leqslant k \leqslant n-1$.

• Supposons qu'il y a trois orbites T avec $\nu(\mathrm{T}) \geqslant 2$: T_1, T_2 et T_3. Notons $\nu_i = \nu(\mathrm{T}_i)$ pour tout $1 \leqslant i \leqslant 3$. On peut supposer $\nu_1 \leqslant \nu_2 \leqslant \nu_3$. L'égalité $(*)$ s'écrit alors

$$1 + \frac{2}{|\mathrm{G}|} = \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3}.$$

On ne peut avoir $\nu_1 \geqslant 3$ car sinon

$$1 < 1 + \frac{2}{|\mathrm{G}|} = \frac{1}{\nu_1} + \frac{1}{\nu_2} + \frac{1}{\nu_3} \leqslant 3.\frac{1}{3} = 1.$$

On a nécessairement $\nu_1 = 2$ et $(*)$ s'écrit $\frac{1}{2} + \frac{2}{|\mathrm{G}|} = \frac{1}{\nu_2} + \frac{1}{\nu_3}$.
On ne peut avoir $\nu_2 \geqslant 4$ car sinon

$$\frac{1}{2} < \frac{1}{2} + \frac{2}{|\mathrm{G}|} = \frac{1}{\nu_2} + \frac{1}{\nu_3} \leqslant 2.\frac{1}{4} = \frac{1}{2}.$$

Donc ν_2 vaut 2 ou 3.

⋆ Supposons $\nu_2 = 2$. Alors $\nu_3 = |\mathrm{G}|/2$ et $|\mathrm{G}|$ est pair.

⋆ Supposons $\nu_2 = 3$. Alors $(*)$ devient

$$\frac{1}{6} + \frac{2}{|\mathrm{G}|} = \frac{1}{\nu_3}$$

et on a nécessairement $\nu_3 < 6$ et ν_3 vaut 3, 4 ou 5. La formule donne alors la valeur de $|\mathrm{G}|$.

On conclut donc sur les valeurs possibles de $\nu(\mathrm{T})$ dans le cas de trois orbites :

Cas	ν_1	ν_2	ν_3	$\lvert G\rvert$
1	2	2	$n/2$	n
2	2	3	3	12
3	2	3	4	24
4	2	3	5	60

Pour achever l'étude, il reste à effectuer un important travail de synthèse. On peut prouver qu'il existe bien un sous-groupe correspondant à ces quatre derniers cas-là comme on l'a fait dans le cas où on avait deux orbites T *avec* $\nu(\mathrm{T}) \geqslant 2$. *Le cas* 1 *est réalisé par le groupe des rotations laissant stables un polygone régulier à* $n/2$ *cotés, contenu dans un plan. On parle alors de groupe diédral. Le cas* 2 *est réalisé par le groupe des rotations laissant stable un tétraèdre régulier; il est isomorphe à* $\mathcal{A}_4$. *Le cas* 3 *est réalisé par le groupe des rotations laissant stable le cube, qui est isomorphe à* $\mathcal{S}_4$ *et enfin le dernier cas est obtenu par le groupe des rotations laissant stable le dodécaèdre régulier, qui est isomorphe à* $\mathcal{A}_5$. *Les deux polyèdres réguliers restants sont l'octaèdre et l'icosaèdre qui ont respectivement le même groupe que le cube et le dodécaèdre.*

2.17. Groupe dérivé

Soit G un groupe (noté multiplicativement). On note D le sous-groupe de G engendré par les éléments de la forme $xyx^{-1}y^{-1}$ (avec x, y dans G) et C le sous-groupe de G engendré par les éléments de la forme x^2 ($x \in \mathrm{G}$).

1. Montrer que $\mathrm{D} \subset \mathrm{C}$.

2. On suppose que G est engendré par les éléments x qui vérifient $x = x^{-1}$. Montrer que $\mathrm{C} = \mathrm{D}$.

3. Soit $\mathrm{G} = \mathrm{O}_2(\mathbb{Q})$ le groupe multiplicatif des matrices $(2,2)$ qui sont orthogonales et à coefficients dans $\mathbb{Q}$. Montrer que dans ce cas D est un sous-groupe strict de $\mathrm{SO}_2(\mathbb{Q})$.

(**École normale supérieure**)

Solution.

1. Pour montrer que D est inclus dans C il suffit de prouver que tout élément $z \in \mathrm{G}$ de la forme $z = xyx^{-1}y^{-1}$ est dans C. Il suffit pour cela d'observer que

$$z = xyx^{-1}y^{-1} = x^2(x^{-1}y)^2(y^{-1})^2.$$

Indiquons qu'un tel élément z s'appelle un commutateur et que le groupe D est appelé le groupe dérivé de G.

2. Si x, y sont dans G, nous noterons $[x, y] = xyx^{-1}y^{-1}$ le commutateur associé. Comme précédemment, pour prouver que $\mathrm{C} = \mathrm{D}$, il nous suffit de montrer que tout carré de G est dans D. Soit $x \in \mathrm{G}$. Par hypothèse, il existe des involutions $x_1, \ldots, x_p$ (c'est-à-dire des éléments vérifiant $x_i = x_i^{-1}$) tels que $x = x_1 x_2 \ldots x_p$. On va travailler par récurrence sur p. Si $p = 1$, on a $x^2 = x_1^2 = e$, où e est le neutre de G. Si $p = 2$, on a

$$x^2 = x_1 x_2 x_1 x_2 = x_1 x_2 x_1^{-1} x_2^{-1} = [x_1, x_2] \in \mathrm{D}.$$

Supposons que le carré d'un produit de $p - 1$ involutions soit dans D. On a alors,

$$\begin{aligned} x^2 &= (x_1 \ldots x_p)(x_1 \ldots x_p) = x_1(x_2 \ldots x_p) x_1 (x_2 \ldots x_p)^{-1} (x_2 \ldots x_p)^2 \\ &= [x_1, x_2 \ldots x_p](x_2 \ldots x_p)^2 \in \mathrm{D} \end{aligned}$$

en tant que produit d'un commutateur et d'un élément qui est dans D par hypothèse de récurrence.

3. Notons que $\mathrm{G} = \mathrm{O}_2(\mathbb{Q})$ est bien un sous-groupe du groupe orthogonal $\mathrm{O}_2(\mathbb{R})$: il est non vide, stable par le produit puisque le produit de deux matrices à coefficients dans $\mathbb{Q}$ est encore une matrice à coefficients dans $\mathbb{Q}$, et stable par inverse puisque l'inverse d'une matrice orthogonale est simplement sa transposée. Les éléments de G de déterminant -1 sont des involutions (des symétries axiales géométriquement). Nous savons de plus, que n'importe quelle matrice de $\mathrm{SO}_2(\mathbb{R})$ peut se décomposer comme un produit de deux symétries, l'une des deux pouvant être choisie arbitrairement. En particulier, si $\mathrm{A} \in \mathrm{SO}_2(\mathbb{Q})$ on peut décomposer A comme un produit de deux involutions de G puisqu'il suffit d'écrire $\mathrm{A} = \mathrm{S}(\mathrm{SA})$ avec $\mathrm{S} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. La condition de la question 2 est donc vérifiée : G est bien engendré par les involutions.

Il est évidemment clair que D est inclus dans $\mathrm{SO}_2(\mathbb{Q})$ (un commutateur à un déterminant égal à 1). Supposons par l'absurde que $\mathrm{D} = \mathrm{C} = \mathrm{SO}_2(\mathbb{Q})$. Comme tout élément de $\mathrm{G} \setminus \mathrm{SO}_2(\mathbb{Q})$ a un carré égal au neutre, C est engendré par les carrés des éléments de $\mathrm{SO}_2(\mathbb{Q})$. Mais comme $\mathrm{SO}_2(\mathbb{Q})$ est commutatif, un produit de carrés est encore un carré et tout élément de $\mathrm{SO}_2(\mathbb{Q})$ est alors un carré. On va voir que ce n'est pas le cas. Considérons $\mathrm{M} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ la matrice qui correspond à la rotation d'angle $\frac{\pi}{2}$ et supposons qu'il existe $\mathrm{N} \in \mathrm{G}$ telle que $\mathrm{N}^2 = \mathrm{M}$. On a forcément $\mathrm{N} \in \mathrm{SO}_2(\mathbb{Q})$ et on peut écrire $\mathrm{N} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ avec $(a, b) \in \mathbb{Q}^2$.

Mais on a alors $(a+ib)^2 = i$, ce qui donne $a+ib = \pm\left(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}\right)$. C'est absurde car $\sqrt{2}$ est irrationnel. ◁

Les exercices qui suivent concernent l'étude de quelques exemples de groupes.

2.18. Groupes quasi-cycliques de Prüfer

Soit $p \in \mathbb{N}^*$ un entier premier et U_p le groupe multiplicatif de $\mathbb{C}^*$ engendré par l'ensemble des nombres $\exp\left(\frac{2i\pi}{p^\alpha}\right)$ où α décrit $\mathbb{N}$.

1. Quels sont les sous-groupes de U_p ?

2. Montrer que U_p est indécomposable, c'est-à-dire n'est pas isomorphe à un produit direct de deux groupes non triviaux.

(École normale supérieure)

▷ **Solution.**

1. Pour $\alpha \in \mathbb{N}$, notons G_α le sous-groupe de $\mathbb{C}^*$ engendré par $\exp\left(\frac{2i\pi}{p^\alpha}\right)$. C'est le groupe des racines p^α-ièmes de l'unité. On a, pour tout $\alpha \in \mathbb{N}$, $G_\alpha \subset G_{\alpha+1}$, car $\exp\left(\frac{2i\pi}{p^\alpha}\right) = \left(\exp\left(\frac{2i\pi}{p^{\alpha+1}}\right)\right)^p$ et *a fortiori*, $G_\beta \subset G_\alpha$ si $\beta \leqslant \alpha$. On en déduit que $\bigcup_{\alpha\in\mathbb{N}} G_\alpha$ est un sous-groupe de $\mathbb{C}^*$. En effet, deux éléments de cette réunion appartiennent à un même G_α, qui contient aussi leur produit. On a donc

$$U_p = \bigcup_{\alpha\in\mathbb{N}} G_\alpha.$$

Examinons les sous-groupes de U_p. Il y a évidemment les G_α, qui sont finis et U_p lui-même. On va montrer que ce sont les seuls.

Tout d'abord, pour tout $\alpha \in \mathbb{N}$, les sous-groupes de G_α sont les G_β avec $\beta \leqslant \alpha$. Il a déjà été noté que ce sont des sous-groupes de G_α. Inversement, si G est un sous-groupe de G_α, le cardinal de G divise celui de G_α d'après le théorème de Lagrange, et il existe donc $\beta \leqslant \alpha$ tel que $|G| = p^\beta$. Mais alors, on a $x^{p^\beta} = 1$ pour tout x de G (toujours d'après le théorème de Lagrange) et donc $G \subset G_\beta$. Les deux groupes ayant même cardinal, l'inclusion est une égalité.

Soit maintenant un sous-groupe G de U_p qui n'est pas un G_α. D'après ce qui précède, G n'est contenu dans aucun G_α. Pour tout $\alpha \in \mathbb{N}$, il existe $x \in G$ tel que $x \notin G_\alpha$. Considérons le plus petit entier naturel n tel que $x \in G_n$. On note que $\alpha < n$ (car sinon, on aurait $x \in G_n \subset G_\alpha$).

On écrit $x = \exp\left(\dfrac{2ik\pi}{p^n}\right)$, avec $k \in \mathbb{Z}$. Puisque, par définition de n, x n'appartient pas à G_{n-1}, on a $x^{p^{n-1}} = \exp\left(\dfrac{2ik\pi}{p}\right) \neq 1$. On en déduit que p ne divise pas k ; p étant un nombre premier, k est premier avec p et donc premier avec p^n. Mais ceci est la condition pour que x engendre G_n. Comme $x \in G$, G_n est contenu dans G. On a, *a fortiori*, $G_\alpha \subset G$, car $\alpha < n$ implique $G_\alpha \subset G_n$. Puisque α est un entier quelconque, on en déduit que G, qui contient tous les G_α, est égal à U_p.

Il en résulte que l'ensemble des sous-groupes de U_p est totalement ordonné par l'inclusion.

2. Supposons qu'il existe deux groupes H, K et un isomorphisme φ de $H \times K$ sur U_p. Posons $\tilde{H} = H \times \{1\}$: c'est un sous-groupe de $H \times K$ isomorphe à H. De même $\tilde{K} = \{1\} \times K$ est isomorphe à K et $\tilde{H} \cap \tilde{K} = \{(1,1)\}$. Les images par φ des sous-groupes $\tilde{H}$ et $\tilde{K}$ sont des sous-groupes de U_p d'intersection égale à $\{1\}$. D'après le point précédent l'un des deux est réduit à $\{1\}$. Donc soit H, soit K est trivial. $\lhd$

2.19. Le groupe modulaire

Soit $P = \{z \in \mathbb{C},\ \operatorname{Im} z > 0\}$ le *demi-plan de Poincaré*. À toute matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $SL_2(\mathbb{Z})$ on associe la fonction homographique f_A définie pour $z \in P$ par $f_A(z) = \dfrac{az+b}{cz+d}$.

1. Montrer que l'application $\psi : A \longmapsto f_A$ est un morphisme de groupes de $SL_2(\mathbb{Z})$ dans le groupe des permutations de P. Déterminer $\operatorname{Ker}\psi$. On note G l'image de ψ ; on l'appelle le *groupe modulaire*.

2. Pour $z \in P$, on pose $I_z = \{\operatorname{Im} g(z),\ \ g \in G\}$. Montrer que I_z est une partie de $\mathbb{R}_+^*$ admettant un plus grand élément. (On pourra prouver que pour tout réel $\alpha > 0$, l'ensemble des $g \in G$ tels que $\operatorname{Im} g(z) > \alpha$ est fini).

3. On note G_0 le sous-groupe de G engendré par $u : z \longmapsto z+1$ et $v : z \longmapsto -\dfrac{1}{z}$. Soit $z \in P$. Montrer qu'il existe $g_0 \in G_0$ tel que, pour tout $g \in G_0$, $\operatorname{Im} g(z) \leqslant \operatorname{Im} z_0$, où $z_0 = g_0(z)$.

4. Soit $D = \{z \in P,\ |\operatorname{Re} z| \leqslant \dfrac{1}{2},\ |z| \geqslant 1\}$ le *domaine fondamental du groupe modulaire*. Montrer qu'on peut choisir z_0 dans D.

5. En déduire que $G_0 = G$.

(**École normale supérieure**)

Solution.

1. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $B = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$ et $z \in P$. On a

$$f_A(z) = \frac{az+b}{cz+d} = \frac{(az+b)(c\overline{z}+d)}{|cz+d|^2} = \frac{ac|z|^2 + bd + adz + bc\overline{z}}{|cz+d|^2}$$

Il en résulte, en prenant la partie imaginaire, que

$$\operatorname{Im}(f_A(z)) = \frac{(ad-bc)\operatorname{Im} z}{|cz+d|^2} = \frac{\operatorname{Im} z}{|cz+d|^2} > 0.$$

On en déduit que $f_A(P) \subset P$. On a ensuite

$$f_A(f_B(z)) = \frac{a\dfrac{a'z+b'}{c'z+d'} + b}{c\dfrac{a'z+b'}{c'z+d'} + d} = \frac{(aa'+bc')z + (ab'+bd')}{(ca'+dc')z + cb' + dd'} = f_{AB}(z).$$

Comme $f_I = \mathrm{Id}_P$, l'application f_A est bijective et sa bijection réciproque est $f_{A^{-1}}$. Le résultat précédent prouve alors que ψ est un morphisme de groupes de $SL_2(\mathbb{Z})$ dans le groupe des permutations de P.

Supposons que $A \in \operatorname{Ker}\psi$. On a $f_A(z) = z$ pour tout $z \in P$ ce qui donne pour tout $z \in P$, $az + b = cz^2 + dz$. D'où l'on déduit $c = b = 0$ et $a = d$. Comme $ad - bc = 1$ on a $a = \pm 1$. Il en résulte que $\operatorname{Ker}\psi = \{\pm I\}$.

2. Soit $z \in P$ et $\alpha > 0$. On suit l'indication de l'énoncé. Pour $g \in G$, $\operatorname{Im} g(z) \geqslant \alpha$ équivaut à $|cz+d|^2 \leqslant \dfrac{\operatorname{Im} z}{\alpha}$ où c, d sont les coefficients de la seconde ligne d'une matrice $A \in SL_2(\mathbb{Z})$ telle que $f_A = g$ (cette matrice est unique au signe près d'après la question précédente). Il n'y a qu'un nombre fini de couples $(c,d) \in \mathbb{Z}^2$ vérifiant cette inégalité. En effet, on a

$$c^2(\operatorname{Im} z)^2 \leqslant |cz+d|^2 \leqslant \frac{\operatorname{Im} z}{\alpha} \text{ et donc } c^2 \leqslant \frac{1}{\alpha \operatorname{Im} z}, \text{ puis}$$
$$d^2 \leqslant |cz|^2 + |cz+d|^2 \leqslant c^2|z|^2 + \frac{\operatorname{Im} z}{\alpha}.$$

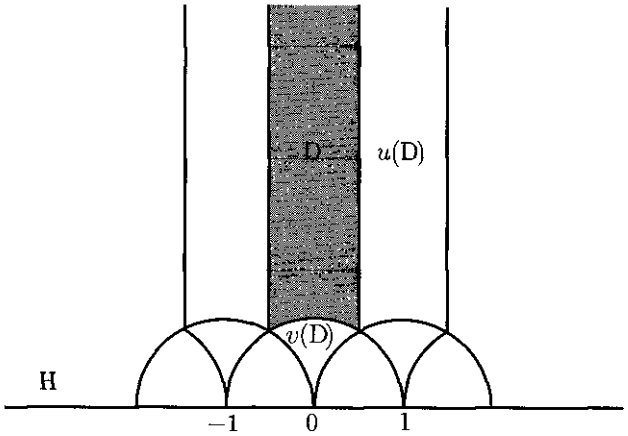
Il en résulte que $I_z \cap [\alpha, +\infty[$, qui est l'ensemble des nombres réels qui s'écrivent $\dfrac{\operatorname{Im} z}{|cz+d|^2}$, avec $(c,d) \in \mathbb{Z}^2$ vérifiant l'inégalité ci-dessus, est fini (éventuellement vide).

On en déduit que I_z admet un plus grand élément : si on choisit $\alpha > 0$ tel que $I_z \cap [\alpha, +\infty[$ soit non vide (on prend $\alpha = g(z)$ avec g élément quelconque de G), le plus grand élément de I_z est le plus grand élément de $I_z \cap [\alpha, +\infty[$.

3. Posons $J_z = \{\operatorname{Im} g(z),\ \ z \in G_0\}$. Comme $J_z \subset I_z$, pour tout $\alpha > 0$, $J_z \cap [\alpha, +\infty[$ est aussi fini. Donc J_z admet également un plus grand élément. D'où l'existence de $g_0 \in G_0$ tel que l'on ait, pour tout $g \in G_0$, $\operatorname{Im} g(z) \leqslant \operatorname{Im} z_0 = \operatorname{Im} g_0(z)$.

4. Supposons que $\operatorname{Re} z_0 = m + t$ où $m \in \mathbb{Z}$ et $t \in \left]-\frac{1}{2}, \frac{1}{2}\right]$. Alors $u^{-m}(z_0)$ admet t comme partie réelle et possède la même partie imaginaire que z_0. Comme $u^{-m}(z_0)$ est égal à $(u^{-m} \circ g_0)(z)$, on peut donc en remplaçant $g_0(z)$ par $(u^{-m} \circ g_0)(z)$, supposer $|\operatorname{Re} z_0| \leqslant \frac{1}{2}$. Mais alors, on a obligatoirement $|z_0| \geqslant 1$. En effet, on observe que $\operatorname{Im} v(z_0) = \frac{\operatorname{Im} z_0}{|z_0|^2}$ de sorte que si $|z_0| < 1$, on a $\operatorname{Im}(v \circ g_0)(z) > \operatorname{Im} z_0$, ce qui contredit le choix de g_0.

5. Représentons D.



Les groupes G et G_0 opèrent naturellement sur P. La question précédente a montré que la G_0-orbite de tout point z de P rencontre ce domaine D. On va maintenant regarder si deux points z et z' de D peuvent être dans la même G-orbite.

Supposons donc qu'il existe $g \in G$ tel que $z' = g(z)$. Quitte à remplacer le couple (z, z') par le couple (z', z), où $z = g^{-1}(z')$, on peut supposer que $\operatorname{Im} g(z) \geqslant \operatorname{Im} z$. Soit $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ telle que $g = f_A$. On a $|cz + d|^2 \leqslant 1$ car $\operatorname{Im} g(z) \geqslant \operatorname{Im} z$. En posant $z = x + iy$, avec $(x, y) \in \mathbb{R}^2$, on obtient

$$1 \geqslant (cx + d)^2 + c^2y^2 \geqslant c^2y^2 \geqslant \frac{3}{4}c^2,$$

car $z \in D$. On en déduit que $|c| < 2$, ce qui donne $c \in \{1, 0, -1\}$. Comme il est loisible de changer les signes des coefficients de A, le cas $c = -1$ se ramène au cas $c = 1$.

• Supposons $c = 0$. On a alors $ad = 1$ et donc $a = d = \pm 1$. Dans ce cas, g est une translation : $g(z) = z + k$, avec $k \in \mathbb{Z}$. Si $k = 0$, $g = \mathrm{Id}_P$ et $z' = z$. Si $k \neq 0$, $\operatorname{Re} z$ et $\operatorname{Re} z'$ étant tous les deux dans l'intervalle

$\left[-\frac{1}{2}, \frac{1}{2}\right]$, on a obligatoirement $k = \pm 1$; l'un des deux nombres $\operatorname{Re} z$ et $\operatorname{Re} z'$ doit être égal à $-\frac{1}{2}$ et l'autre à $\frac{1}{2}$.

• Supposons $c = 1$. De $|z + d| \leqslant 1$, on déduit que

$$1 \geqslant (x+d)^2 + y^2 = |z|^2 + 2dx + d^2 \geqslant 1 - 2|d||x| + d^2 \geqslant 1 - |d| + d^2$$

et donc $d^2 \leqslant |d|$. Cela impose $d \in \{0, -1, 1\}$. On a alors $1 - |d| + d^2 = 1$ et les inégalités précédentes sont des égalités. Cela entraîne

$$|z| = 1 \quad \text{et} \quad 2dx = -2|d||x| = -|d|.$$

⋆ Si $d = 0$, on obtient $b = -1$ et $z' = g(z) = a - \frac{1}{z} = a - \overline{z}$. En particulier $\operatorname{Re}(z') = a - \operatorname{Re}(z)$. Si $\operatorname{Re}(z) \neq \pm\frac{1}{2}$, c'est-à-dire si $z \neq j$ et $z \neq -j^2$, alors $a = 0$ et $z' = -\overline{z}$. Si $z = j$, on peut avoir $a = 0$ ou -1 ; on obtient alors $z' = -j^2$ ou j. De même, si $z = -j^2$, alors $z' = j$ ou $-j^2$. Dans tous les cas, on note que $|z'| = 1$.

⋆ Si $d = 1$, on a $|z| = 1$ et $x = -\frac{1}{2}$, c'est-à-dire $z = j$. On obtient alors $b = 1$ et $z' = g(z) = a - \frac{1}{z+1} = a - \frac{1}{j+1} = a + j$. Ceci nécessite $a = 0$ ou 1 et $z' = j$ ou $-j^2$.

⋆ Si $d = -1$, on obtient de même, $z = -j^2$ et $z' = j$ ou $-j^2$.

On observe que, dans tous les cas, si $z \neq z'$, z et z' sont sur la *frontière* de D. De plus, si z n'est pas sur la frontière de D, la seule application g telle que $z = g(z)$ est Id_{P}. Nous allons déduire de cela que $\mathrm{G} = \mathrm{G}_0$.

En effet, prenons $g \in \mathrm{G}$ et z un point intérieur à D (par exemple $z = 2i$). Puisque $g(z) \in \mathrm{P}$, la question 4 montre qu'il existe $g_0 \in \mathrm{G}_0$ tel que $g_0(g(z)) \in \mathrm{D}$. D'après ce qu'on vient de voir, cela impose $g_0 \circ g(z) = z$ et $g_0 \circ g = \mathrm{Id}_{\mathrm{P}}$. On a donc $g = g_0^{-1}$ et $g \in \mathrm{G}_0$. ◁

On déduit de ce résultat que le groupe $\mathrm{SL}_2(\mathbb{Z})$ *est engendré par les deux matrices* $\mathrm{U} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *et* $\mathrm{V} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. *On trouvera une autre preuve de ce résultat par des manipulations élémentaires dans le chapitre sur le groupe linéaire dans le tome 2 d'algèbre.*

Un problème majeur de la théorie des groupes finis, qui n'est pas encore totalement résolu de nos jours, est celui de la classification à isomorphisme près. Après un travail colossal de plusieurs dizaines d'années la classification est terminée pour les groupes finis simples, c'est-à-dire sans sous-groupe distingué non trivial. Avec les outils du programme des classes préparatoires on peut s'attaquer à un problème incomparablement

plus facile : la classification des groupes finis abéliens. L'énoncé ci-après démontre la partie unicité du théorème suivant :

Théorème. *Si* G *est un groupe abélien fini avec* $|\mathrm{G}| \geqslant 2$, *il existe une unique suite* $(a_1, \ldots, a_n)$ *telle que* $2 \leqslant a_1|a_2|\cdots|a_n$ *et* $\mathrm{G} \simeq \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$.

L'entier a_n *n'est autre que l'exposant du groupe* G *(cf. exercice 2.8). Pour la partie existence nous renvoyons le lecteur à l'exercice 7.22.*

2.20. Unicité dans le théorème de structure des groupes abéliens finis

Soit $(a_1, \ldots, a_n, b_1, \ldots, b_m) \in (\mathbb{N}^*)^{m+n}$ vérifiant

$$2 \leqslant a_1|a_2|\cdots|a_n \quad \text{et} \quad 2 \leqslant b_1|b_2|\cdots|b_m.$$

On suppose qu'il existe un isomorphisme de groupes

$$\prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z} \simeq \prod_{i=1}^{m} \mathbb{Z}/b_i\mathbb{Z}.$$

Montrer que $m = n$ et que $a_i = b_i$ pour tout $i \in [\![1, n]\!]$.

(École normale supérieure)

▷ **Solution.**

Notons $\mathrm{G}_1 = \prod_{i=1}^{n} \mathbb{Z}/a_i\mathbb{Z}$ et $\mathrm{G}_2 = \prod_{i=1}^{m} \mathbb{Z}/b_i\mathbb{Z}$. Démontrons le résultat d'unicité par récurrence sur $n \geqslant 0$.

• Supposons $n = 0$. On a alors

$$\mathrm{G}_1 = \{0\} \simeq \prod_{i=1}^{m} \mathbb{Z}/b_i\mathbb{Z}.$$

Ceci implique $1 = \operatorname{Card} \mathrm{G}_1 = \operatorname{Card} \mathrm{G}_2 = b_1 \ldots b_m$. D'où $m = 0$.

• Supposons $n \geqslant 1$ et la propriété établie jusqu'au rang $n - 1$. Pour faire chuter n, nous allons considérer le groupe $a_1 \cdot \mathrm{G}_1$. Il est constitué des éléments de la forme

$$a_1 \cdot \mathrm{X} = a_1 \cdot (x_1, \ldots, x_n) = (a_1 \cdot x_1, \ldots, a_1 \cdot x_n),$$

où $\mathrm{X} = (x_1, \ldots, x_n)$ est un élément quelconque de G_1 et où $a_1 \cdot x$ désigne l'élément $x + \cdots + x$ avec a_1 termes. En fait $a_1 \cdot \mathrm{G}_1$ est l'image de G_1 par le morphisme de groupes $\mathrm{X} \longmapsto a_1 \cdot \mathrm{X}$. C'est donc bien un sous-groupe de G_1 et on a clairement,

$$a_1 \cdot \mathrm{G}_1 = (a_1 \cdot (\mathbb{Z}/a_1\mathbb{Z})) \times (a_1 \cdot (\mathbb{Z}/a_2\mathbb{Z})) \times \cdots \times (a_1 \cdot (\mathbb{Z}/a_n\mathbb{Z})) \text{ et}$$
$$a_1 \cdot \mathrm{G}_2 = (a_1 \cdot (\mathbb{Z}/b_1\mathbb{Z})) \times (a_1 \cdot (\mathbb{Z}/b_2\mathbb{Z})) \times \cdots \times (a_1 \cdot (\mathbb{Z}/b_m\mathbb{Z})).$$

Comme $G_1 \simeq G_2$, on a $a_1 \cdot G_1 \simeq a_1 \cdot G_2$. Regardons d'un peu plus près les groupes $a_1 \cdot (\mathbb{Z}/a_i\mathbb{Z})$ et $a_1 \cdot (\mathbb{Z}/b_j\mathbb{Z})$ qui interviennent ci-dessus. Pour cela, établissons un petit lemme.

Lemme. *Si n, p sont des entiers naturels non nuls, le groupe $p \cdot (\mathbb{Z}/n\mathbb{Z})$ est cyclique, isomorphe au groupe $\mathbb{Z}/\left(\dfrac{n}{\operatorname{pgcd}(p,n)}\right)\mathbb{Z}$.*

Démonstration. On note $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ le morphisme surjectif de groupes qui à un entier $x \in \mathbb{Z}$ associe $\overline{x}$ sa classe modulo n. Pour tout x dans $\mathbb{Z}$, on a

$$p\pi(x) = p\overline{x} = \overline{px} = \pi(px).$$

Il en résulte que $p \cdot (\mathbb{Z}/n\mathbb{Z})$ est l'image par π du sous-groupe $p\mathbb{Z}$ de $\mathbb{Z}$. C'est donc le sous-groupe cyclique de $\mathbb{Z}/n\mathbb{Z}$ engendré par $\pi(p) = \overline{p}$. Or, l'ordre de $\overline{p}$ est le plus petit entier naturel non nul k tel que kp soit divisible par n, c'est-à-dire $\dfrac{n}{\operatorname{pgcd}(p,n)}$, ce qui démontre le lemme. $\diamondsuit$

Comme pour tout $i \in [\![1, n]\!]$, $a_1 | a_i$, on a $\operatorname{pgcd}(a_1, a_i) = a_1$ et, d'après le lemme, $a_1 \cdot (\mathbb{Z}/a_i\mathbb{Z}) \simeq \mathbb{Z}/\dfrac{a_i}{a_1}\mathbb{Z}$. Ainsi on obtient

$$a_1 \cdot G_1 \simeq \prod_{1 \leqslant i \leqslant n} \mathbb{Z}/\frac{a_i}{a_1}\mathbb{Z}.$$

Du lemme, on tire également que

$$a_1 \cdot G_2 \simeq \prod_{1 \leqslant i \leqslant m} \mathbb{Z}/\left(\frac{b_i}{\operatorname{pgcd}(a_1, b_i)}\right)\mathbb{Z}.$$

Comme $\operatorname{Card} G_1 = \operatorname{Card} G_2$ on a $a_1 \ldots a_n = b_1 \ldots b_m$. Comme $a_1 \cdot G_1$ et $a_1 \cdot G_2$ sont isomorphes, on a également

$$\prod_{1 \leqslant i \leqslant n} \frac{a_i}{a_1} = \prod_{1 \leqslant i \leqslant m} \frac{b_i}{\operatorname{pgcd}(a_1, b_i)},$$

ce qui donne

$$\frac{\prod\limits_{1 \leqslant i \leqslant n} a_i}{a_1^n} = \frac{\prod\limits_{1 \leqslant i \leqslant m} b_i}{\prod\limits_{1 \leqslant i \leqslant m} \operatorname{pgcd}(a_1, b_i)}.$$

On a donc $a_1^n = \prod\limits_{1 \leqslant i \leqslant m} \operatorname{pgcd}(a_1, b_i) \leqslant a_1^m$ car $\operatorname{pgcd}(a_1, b_i) \leqslant a_1$, ce qui implique $n \leqslant m$. Comme G_1 et G_2 jouent des rôles symétriques (si $n = 1$, alors nécessairement $m \geqslant 1$), on peut démontrer de même que $m \leqslant n$ et ainsi $n = m$. Les majorations des $\operatorname{pgcd}(a_1, b_i)$ par a_1 effectuées ci-dessus sont alors nécessairement des égalités. On a donc pour tout

$i \in [\![1,n]\!]$, $a_1 = \mathrm{pgcd}(a_1, b_i)$, *i.e.* $a_1 | b_i$. En particulier, $a_1 | b_1$. Toujours pour des raisons de symétrie, $b_1 | a_1$ et finalement $a_1 = b_1$.

Revenons alors à l'isomorphisme $a_1 \cdot \mathrm{G}_1 \simeq a_1 \cdot \mathrm{G}_2 = b_1 \cdot \mathrm{G}_2$. Il s'écrit

$$\prod_{1 \leqslant i \leqslant n} \mathbb{Z}/\frac{a_i}{a_1}\mathbb{Z} \simeq \prod_{1 \leqslant i \leqslant n} \mathbb{Z}/\frac{b_i}{a_1}\mathbb{Z}.$$

Si $a_i = a_1$ $(1 \leqslant i \leqslant n)$, alors $\mathbb{Z}/\dfrac{a_i}{a_1}\mathbb{Z} = \{0\}$. C'est vrai en particulier pour $i = 1$. Nous avons fait chuter n et allons pouvoir appliquer l'hypothèse de récurrence. Si tous les a_i sont égaux à a_1, $a_1 \cdot \mathrm{G}_1 = \{0\} = a_1 \cdot \mathrm{G}_2$ et tous les b_i sont égaux à a_1. L'unicité est alors prouvée.

Dans le cas contraire, on peut considérer r le plus petit entier de $[\![2,n]\!]$ tel que $a_r > a_1$. Nécessairement, il existe $i \in [\![1,n]\!]$ tel que $b_i > b_1 = a_1$. On note s le plus petit de ces entiers. On a $s \geqslant 2$. Dans ces conditions, l'isomorphisme devient

$$\mathbb{Z}/\frac{a_r}{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\frac{a_n}{a_1}\mathbb{Z} \simeq \mathbb{Z}/\frac{b_s}{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/\frac{b_n}{a_1}\mathbb{Z}.$$

Par hypothèse de récurrence, on a $r = s$ (et si $i < r$, $a_i = a_1 = b_i$) et

$$\frac{a_r}{a_1} = \frac{b_r}{b_1}, \ldots, \frac{a_n}{a_1} = \frac{b_n}{a_1}.$$

On conclut donc à l'égalité $a_i = b_i$ pour tout $1 \leqslant i \leqslant n$, ce qui termine la démonstration par récurrence. $\lhd$

Le groupe symétrique d'un ensemble E, *noté* $\mathcal{S}_{\mathrm{E}}$, *est le groupe des permutations de* E. *On note* $\mathcal{S}_n$ *le groupe symétrique de* $[\![1,n]\!]$ *pour tout* $n \geqslant 1$. *L'étude des groupes de permutation finis se ramène à l'étude des* $\mathcal{S}_n$ *car si* E *est de cardinal* n, $\mathcal{S}_{\mathrm{E}}$ *est isomorphe à* $\mathcal{S}_n$.

On rappelle que toute permutation $\sigma \in \mathcal{S}_n$ *admet une décomposition en cycles à supports disjoints et que cette décomposition est unique à l'ordre des cycles près. Un cycle* c *de longueur* p *ou encore* p*-cycle, sera noté* $c = (a_1, a_2, \ldots, a_p)$ *où pour tout* i, $a_{i+1} = c(a_i)$ *(lire les indices modulo* p*). Une transposition est un cycle de longueur* 2. *Pour tout* $n \geqslant 2$, *le groupe* $\mathcal{S}_n$ *est engendré par les transpositions. En fait, les transpositions* $(1,i)$ *pour* $2 \leqslant i \leqslant n$ *suffisent, ce qui peut se voir par récurrence sur* n *ou simplement à partir du résultat précédent puisque pour* $i \neq j$, $(i,j) = (1,i)(1,j)(1,i)$. *L'exercice suivant s'intéresse au nombre minimal de transpositions permettant de générer* $\mathcal{S}_n$.

2.21. Génération du groupe symétrique

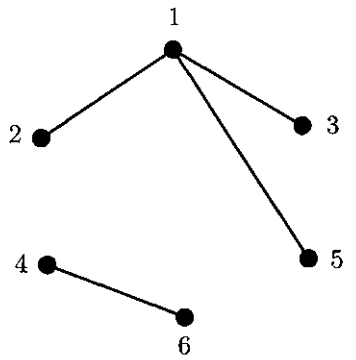
Soit $n \geqslant 2$. Quel est le nombre minimal de transpositions engendrant le groupe symétrique $\mathcal{S}_n$?

(École normale supérieure)

Solution.

On a rappelé plus haut que les transpositions $(1,2),\ldots,(1,n)$ engendrent $\mathcal{S}_n$. Ainsi, $n-1$ transpositions suffisent et intuitivement, il semble difficile de faire mieux, ce que semble confirmer l'étude des premières valeurs de n. En effet, pour $n=2$ il nous faut au moins une transposition (la seule !) et pour $n=3$, il nous en faut au moins 2 puisque une seule transposition engendre un sous-groupe à deux éléments.

Donnons-nous des transpositions $\tau_1,\ldots,\tau_k$, avec $k \leqslant n-2$. Pour visualiser le problème nous allons représenter les entiers de 1 à n par des points du plan. On fait en sorte que trois quelconques des points ne soient pas alignés. Si la transposition (a,b) apparaît dans la liste $\tau_1,\ldots,\tau_k$ on joint par un segment les points correspondant aux entiers a et b. On obtient ce qu'on appelle un graphe[2]. Par exemple, pour $n=6$, $k=4$, $\tau_1=(1,2)$, $\tau_2=(1,3)$, $\tau_3=(1,5)$ et $\tau_4=(4,6)$, on obtient le graphe suivant :



Il est assez clair qu'une condition nécessaire pour que $\tau_1,\ldots,\tau_k$ engendrent $\mathcal{S}_n$ est qu'on puisse passer de n'importe quel sommet $i \in [\![1,n]\!]$ à n'importe quel autre sommet $j \in [\![1,n]\!]$ en suivant les arêtes du graphe. Un graphe vérifiant cette propriété est dit *connexe*. Il est aisé de dessiner des graphes connexes sur un ensemble de cardinal n qui contiennent $n-1$ arêtes. On peut par exemple choisir un sommet et le relier à tous

2. Formellement, un graphe G est un couple (S, A) où S est un ensemble fini, et A un ensemble de paires d'éléments de S. Les éléments de S sont appelés les sommets du graphe, ceux de A les arêtes.

les autres. Mais il semble impossible d'y arriver avec seulement $n-2$ arêtes. On a effectivement le résultat suivant :

Lemme. *Si un graphe* G *sur un ensemble* E *de cardinal* $n \geqslant 2$ *est connexe, alors il a au moins* $n-1$ *arêtes.*

Démonstration. On procède par récurrence sur n, le résultat étant clair pour $n = 2$. Supposons le résultat prouvé au rang $n-1$. Soit G un graphe à n sommets. Si x est un sommet de G on note $\delta(x)$ sa *valence* c'est-à-dire le nombre d'arêtes qui arrivent en x. On a aisément

$$\sum_{x \in \mathrm{E}} \delta(x) = 2a(\mathrm{G}),$$

où $a(\mathrm{G})$ est le nombre d'arêtes de G (car une arête correspond à deux sommets). La connexité de G impose évidemment $\delta(x) \geqslant 1$ pour tout x. Deux cas se présentent :

• Pour tout x, $\delta(x) \geqslant 2$. Alors on a directement grâce à l'égalité ci-dessus $a(\mathrm{G}) \geqslant n$.

• Il existe un sommet x_0 de valence 1. Retirons ce sommet x_0 et l'unique arête qui y aboutit. On obtient un nouveau graphe G′ sur l'ensemble $\mathrm{E}' = \mathrm{E} \backslash \{x_0\}$ qui est encore connexe. Par hypothèse de récurrence, $a(\mathrm{G}') \geqslant |\mathrm{E}'| - 1 = n-2$ et donc $a(\mathrm{G}) = a(\mathrm{G}') + 1 \geqslant n-1$. ◁

2.22. Plongement de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.

(École normale supérieure)

▷ **Solution.**

On considère l'application $\psi : \mathcal{S}_n \to \mathcal{A}_{n+2}$ définie par $\psi(\sigma) = \sigma$ si σ est une permutation paire et $\psi(\sigma) = \sigma \circ (n+1, n+2)$ si σ est impaire. L'application ψ est injective par unicité de la décomposition en cycles à supports disjoints. Et il est aisé de constater que ψ est un morphisme de groupes. ◁

Le lecteur qui a un peu plus de connaissances en théorie des groupes (simplicité du groupe alterné $\mathcal{A}_n$ pour $n \geqslant 5$) pourra démontrer qu'il est impossible d'injecter le groupe $\mathcal{S}_n$ dans $\mathcal{A}_{n+1}$ pour $n \geqslant 2$.

Les deux exercices suivants montrent l'intérêt qu'il y a à connaître des parties génératrices d'un groupe. Si X *est une partie génératrice d'un groupe* G, *la connaissance de la restriction d'un morphisme de groupes*

$f : \mathrm{G} \to \mathrm{G}'$ à X caractérise f de manière unique. Cette idée permettra au lecteur de montrer facilement que les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ sont les applications $x \longmapsto ax$: il suffit de regarder l'image du générateur $\overline{1}$. Dans le second tome algèbre on trouvera d'autres utilisations des parties génératrices dans l'étude du groupe linéaire.

2.23. Morphismes d'un sous-groupe de $\mathcal{S}_p$ dans $\mathbb{Z}/p\mathbb{Z}$

Soit p un nombre premier et G un sous-groupe du groupe symétrique $\mathcal{S}_p$. Déterminer le cardinal de l'ensemble des homomorphismes de G dans $\mathbb{Z}/p\mathbb{Z}$.

(École normale supérieure)

▷ **Solution.**

Soit f un morphisme de $(\mathrm{G}, \circ)$ dans $(\mathbb{Z}/p\mathbb{Z}, +)$. La composée de deux éléments σ_1 et σ_2 sera notée $\sigma_1\sigma_2$ et l'application identité 1.

On sait que tout élément σ de $\mathcal{S}_p$ peut se décomposer en produit (commutatif) de cycles à supports disjoints : on écrit $\sigma = c_1c_2\cdots c_k$ et l'on note n_i l'ordre du cycle c_i. On a donc $n_1 + \cdots + n_k \leqslant p$. L'ordre de σ est $n = \mathrm{ppcm}(n_1, \ldots, n_k)$. On a $\sigma^n = 1$ donc $n.f(\sigma) = f(\sigma^n) = 0$. L'ordre de tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est p car il divise l'ordre p du groupe. Donc si $f(\sigma) \neq 0$, p divise $n = \mathrm{ppcm}(n_1, \ldots, n_k)$ et comme p est premier, il divise un des n_i. On a donc alors $n_i \geqslant p$ et comme $n_i \leqslant n_1 + \cdots + n_k \leqslant p$, $n_i = p$. Ainsi $k = 1$ et σ est un p-cycle. On a donc montré que si $\sigma \in \mathcal{S}_p$ et n'est pas un p-cycle, $f(\sigma) = 0$. Cela montre déjà que si G ne contient pas de p-cycle, $f = 0$.

Si G contient le p-cycle c, alors G contient le sous-groupe engendré par c, $gr(c) = \{c^k,\ k \in [\![0, p-1]\!]\}$. Examinons le cas où G contient de plus un élément σ qui n'appartient pas à $gr(c)$.

Supposons que σ est un p-cycle c' que l'on note $c' = (a_1, \ldots, a_p)$. Il existe $k \in [\![1, p-1]\!]$ tel que $c^k(a_1) = a_2$, par définition d'un p-cycle. On en déduit que $c^{-k}c'(a_1) = a_1$, donc $c^{-k}c'$ n'est pas un p-cycle donc $f(c^{-k}c') = -kf(c) + f(c') = 0$. Comme $c' \notin gr(c)$, $c^{-k}c' \neq 1$ et il existe $j \in [\![2, p]\!]$ tel que $c^{-k}c'(a_j) \neq a_j$; soit $i \in [\![1, p-1]\!]$ tel que $c^{-k}c'(a_j) = a_{i+j} = c'^i(a_j)$ (les indices sont notés modulo p). On a alors $c'^{-i}c^{-k}c'(a_j) = a_j$ et l'on montre que $-kf(c) + (1-i)f(c') = 0$ comme précédemment . On en déduit que $if(c') = 0$ et comme i est premier avec p, $f(c') = 0$, puis $-kf(c) = 0$ et comme k est premier avec p, $f(c) = 0$.

Si σ n'est pas un p-cycle, on le décompose en produit de cycles à supports disjoints $c'c_2 \ldots c_i$, où l'ordre de c' est supérieur ou égal à 2 (car σ n'est pas l'identité). Si $c' = (a_1a_2 \ldots a_j)$, on considère $k \in [\![1, p-1]\!]$ tel que $c^k(a_1) = a_2$. On a alors $c^{-k}c'(a_1) = a_1$. Comme a_1 n'est pas dans le

support de $c_2 \dots c_i$, on a également $c^{-k}\sigma(a_1) = a_1$. Ainsi $c^{-k}\sigma$ n'est pas un p-cycle donc $f(c^{-k}\sigma) = -kf(c) + f(\sigma) = 0$ et $f(c) = 0$ car $f(\sigma) = 0$.

Le seul cas où il existe un morphisme non nul de G dans $\mathbb{Z}/p\mathbb{Z}$ est celui où $\mathrm{G} = gr(c)$ où c est un p-cycle. Mais alors G est un groupe cyclique d'ordre p. On peut choisir comme image de c un élément quelconque de $\mathbb{Z}/p\mathbb{Z}$. On obtient p morphismes de G dans $\mathbb{Z}/p\mathbb{Z}$.

Conclusion. Si G est un sous-groupe de $\mathcal{S}_p$ engendré par un p-cycle, il y a p morphismes de G dans $\mathbb{Z}/p\mathbb{Z}$. Dans tous les autres cas, il n'y en a qu'un : l'application nulle. $\lhd$

2.24. Morphismes de $\mathcal{S}_4$ dans $\mathcal{S}_3$

Déterminer les morphismes du groupe $\mathcal{S}_4$ dans le groupe $\mathcal{S}_3$.
(École normale supérieure)

$\rhd$ **Solution.**

Dans la suite , nous noterons Id_4 et Id_3 les éléments neutres respectifs de $\mathcal{S}_4$ et $\mathcal{S}_3$. Il est bien connu que $\mathcal{S}_4$ est engendré par les transpositions $(1,2),(1,3),(1,4)$. On observera aussi que l'image par un morphisme de groupes f d'un élément x d'ordre n est un élément dont l'ordre est un diviseur de n puisque $(f(x))^n = f(x^n) = e$. Soit f un morphisme de groupes de $\mathcal{S}_4$ dans le groupe $\mathcal{S}_3$. Pour $2 \leqslant i \leqslant 4$, notons $\tau_i = f((1,i))$. Comme $(1,i)$ est d'ordre 2, τ_i est d'ordre 1 ou 2. Les seuls éléments de $\mathcal{S}_3$ d'ordre 2 étant les transpositions, τ_i est soit une transposition, soit l'identité. À partir de là, plusieurs cas sont possibles.

• Soit il existe $i \in [\![2,4[\![$ tel que $\tau_i = \mathrm{Id}_3$. Pour $j \in [\![2,4]\!]$, $j \neq i$, on a $(1,j)(1,i) = (1,i,j)$. On en déduit : $f((1,i,j)) = f((1,j))f((1,i)) = \tau_j$. Mais $(1,i,j)$ est d'ordre 3, donc $\tau_j^3 = \mathrm{Id}_3$ et comme $\tau_j^2 = \mathrm{Id}_3$, on obtient que $\tau_j = \mathrm{Id}_3$. On a donc $f((1,j)) = \mathrm{Id}_3$, pour tout $j \in [\![2,4]\!]$. Ces transpositions engendrant $\mathcal{S}_4$, f est le morphisme constant :

$$s \in \mathcal{S}_4 \longmapsto \mathrm{Id}_3 \in \mathcal{S}_3.$$

Dans tous les autres cas, τ_2, τ_3, τ_4 seront des transpositions.

• Supposons qu'il existe une transposition τ de $\mathcal{S}_3$ telle que l'on ait $\tau_2 = \tau_3 = \tau_4 = \tau$. Toute permutation paire (resp. impaire) étant produit d'un nombre pair (resp. impair) d'éléments de $\{(1,2),(1,3),(1,4)\}$, on en déduit que :

$$\begin{cases} f(s) = \mathrm{Id}_3 & \text{si } s \text{ est une permutation paire de } \mathcal{S}_4 \\ f(s) = \tau & \text{si } s \text{ est une permutation impaire de } \mathcal{S}_4. \end{cases}$$

Réciproquement, si τ est une transposition quelconque de $\mathcal{S}_3$, toute application de $\mathcal{S}_4$ dans $\mathcal{S}_3$ ainsi définie est un morphisme de groupes qui s'iden-

lifie à la signature. On peut définir 3 tels morphismes, car $\mathcal{S}_3$ possède 3 transpositions.

• Supposons que parmi les trois transpositions τ_2, τ_3, τ_4, deux soient égales et la troisième distincte des deux autres. On peut donc déterminer (i, j, k) et (a, b, c) tels que $\{i, j, k\} = \{2, 3, 4\}$, $\{a, b, c\} = \{1, 2, 3\}$, $\tau_i = \tau_j = (a, b)$ et $\tau_k = (a, c)$. On obtient alors

$$f((1,i,j)) = f((1,j)(1,i)) = (a,b)(a,b) = \mathrm{Id}_3$$
$$f((1,i,k)) = f((1,k)(1,i)) = (a,c)(a,b) = (a,b,c).$$

On remarque que $(1,i,k)(1,i,j) = (1,k)(i,j)$, d'où l'on déduit que $f((1,k)(i,j)) = f((1,i,k))f((1,i,j)) = (a,b,c)$. Mais le produit de transpositions de supports disjoints $(1,k)(i,j)$ est d'ordre 2. On obtient ainsi,

$$(a,c,b) = (a,b,c)^2 = f(((1,k)(i,j))^2) = f(\mathrm{Id}_4) = \mathrm{Id}_3\,.$$

C'est impossible. Ce troisième cas ne peut jamais être obtenu.

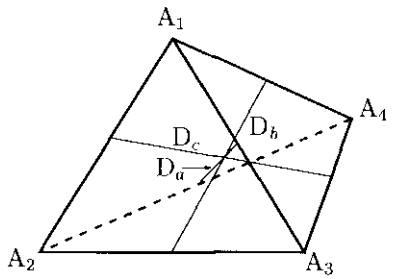
• Supposons enfin que τ_2, τ_3, τ_4 sont trois transpositions distinctes. On obtient à l'ordre près les trois transpositions de $\mathcal{S}_3$, $(1,2), (2,3), (1,3)$. Il existe a, b, c tels que $\{a, b, c\} = \{1, 2, 3\}$ et $\tau_2 = (a, b), \tau_3 = (b, c)$ et $\tau_4 = (c, a)$. Étant donnés a, b, c, il existe au plus un morphisme f de $\mathcal{S}_4$ dans $\mathcal{S}_3$ ayant ces valeurs pour τ_2, τ_3 et τ_4, puisque $(1,2), (1,3)$ et $(1,4)$ engendrent $\mathcal{S}_4$.

Pour montrer l'existence d'un tel morphisme f, nous en donnerons une réalisation géométrique. Il y a plusieurs manières d'obtenir $\mathcal{S}_4$ comme groupe d'isométries. On peut, par exemple l'identifier aux isométries laissant un tétraèdre régulier invariant ou aux isométries positives laissant un cube invariant. Dans chacun des cas, ces isométries induisent une action sur un ensemble à 3 éléments : perpendiculaires communes aux couples d'arêtes opposées pour le tétraèdre ; axes des faces pour le cube. On définit ainsi une application de $\mathcal{S}_4$ dans $\mathcal{S}_3$. Montrons cela de manière plus précise.

⋆ Soit $\mathcal{T}$ un tétraèdre régulier de sommets $\mathrm{A}_1, \mathrm{A}_2, \mathrm{A}_3, \mathrm{A}_4$ et $\mathrm{Is}(\mathcal{T})$ les isométries de l'espace laissant $\mathcal{T}$ invariant. L'action de $\mathrm{Is}(\mathcal{T})$ sur les sommets du tétraèdre définit un morphisme de groupes $\varphi : \mathrm{Is}(\mathcal{T}) \longmapsto \mathcal{S}_4$. La réflexion par rapport au plan médiateur de $[\mathrm{A}_i, \mathrm{A}_j]$ $(1 \leqslant i < j \leqslant 4)$ a pour image par φ la transposition de A_i et A_j dans l'ensemble des sommets. Les transpositions étant dans $\mathrm{Im}\,\varphi$ et engendrant $\mathcal{S}_4$, φ est surjective. Comme $(\mathrm{A}_1, \mathrm{A}_2, \mathrm{A}_3, \mathrm{A}_4)$ est un repère affine de l'espace, la seule application laissant fixes les sommets du tétraèdre $\mathcal{T}$ est l'identité. Le noyau de φ est donc réduit à l'identité ; ainsi φ est injective et finalement φ est un isomorphisme de $\mathrm{Is}(\mathcal{T})$ sur $\mathcal{S}_4$.

Dans un tétraèdre régulier, la perpendiculaire commune à deux arêtes opposées est le segment qui joint les milieux de ces arêtes. L'ensemble des

perpendiculaires communes aux trois couples d'arêtes opposées sera noté $\mathcal{D} = \{D_a, D_b, D_c\}$. Elles sont numérotées de telle façon que D_a (resp. D_b, resp. D_c) soit la perpendiculaire commune à $[A_1, A_3]$ et $[A_2, A_4]$ (resp. $[A_1, A_4]$ et $[A_2, A_3]$, resp. $[A_1, A_2]$ et $[A_3, A_4]$).

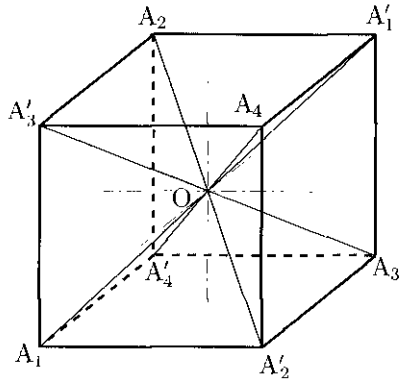


Soit $u \in \mathcal{S}_4$, $s = \varphi^{-1}(u)$ l'isométrie de $\mathcal{T}$ associée. L'isométrie s transforme un couple d'arêtes opposées en un autre couple d'arêtes opposées, ceci de manière injective. Elle transforme donc un élément de $\mathcal{D}$ en un élément de $\mathcal{D}$, de manière injective. Elle induit donc une permutation u' de $\mathcal{D}$ qui s'identifie à un élément de $\mathcal{S}_3$. Soit f l'application qui à $u \in \mathcal{S}_4$ associe $u' \in \mathcal{S}_3$. Par construction, l'application qui à s associe u' est un morphisme (pour la loi $\circ$). Puisque φ^{-1} est aussi un morphisme, on en déduit que f est un morphisme de groupes de $\mathcal{S}_4$ dans $\mathcal{S}_3$.

Pour $i \in \{2, 3, 4\}$, posons $\{j, k\} = \{2, 3, 4\} \setminus \{i\}$. Alors $\varphi^{-1}((1, i))$ est la réflexion par rapport au plan médiateur de $[A_1, A_i]$. Cette réflexion échange A_1 et A_i et laisse invariants A_j et A_k ; elle laisse invariants les milieux de $[A_1, A_i]$ et $[A_j, A_k]$ et échange les milieux de $[A_1, A_j]$ et $[A_1, A_k]$ et les milieux de $[A_i, A_j]$ et $[A_i, A_k]$. Elle laisse donc invariante la perpendiculaire commune à $[A_1, A_i]$ et $[A_j, A_k]$ et échange les deux autres. Ces remarques permettent de déterminer les images par $\varphi^{-1}((1, i))$ des éléments de $\mathcal{D}$ et donc $\tau_i = f((1, i))$. On trouve $\tau_2 = (a, b)$, $\tau_3 = (b, c)$ et $\tau_4 = (c, a)$.

Ceci démontre l'existence d'un morphisme de groupes f de $\mathcal{S}_4$ dans $\mathcal{S}_3$ ayant les propriétés voulues. Puisque (a, b, c) étant une permutation quelconque de $(2, 3, 4)$, on trouve 6 morphismes de ce type.

$\star$ Venons-en au cas du cube. Soit $\mathcal{C}$ un cube de centre O, de sommets A_1, A_2, A_3, A_4, A'_1, A'_2, A'_3, A'_4, les sommets étant numérotés de telle façon que A'_i soit le symétrique de A_i par rapport à O et que $A_1A'_2A_3A'_4$ soit un carré. Notons $\mathrm{Is}^+(\mathcal{C})$ l'ensemble des isométries positives laissant $\mathcal{C}$ invariant. Les éléments de $\mathrm{Is}^+(\mathcal{C})$ sont des rotations dont l'axe contient O. Soit Δ l'ensemble des diagonales du cube, c'est-à-dire l'ensemble des quatre droites $\delta_i = (A_iA'_i)$ $(1 \leqslant i \leqslant 4)$.



Tout élément de $\mathrm{Is}^+(\mathcal{C})$ transforme une diagonale du cube en une autre diagonale. Étant bijectif, il réalise une permutation des éléments de Δ. On obtient donc un morphisme de groupes $\Psi : \mathrm{Is}^+(\mathcal{C}) \longrightarrow \mathcal{S}_4$.

Si $s \in \mathrm{Ker}\,\Psi$, s laisse les quatre droites de Δ invariantes. La restriction de s à chaque droite de Δ est l'identité ou la symétrie par rapport à O. L'application vectorielle associée à s est donc $\pm\mathrm{Id}$. La symétrie par rapport au point O n'étant pas une isométrie positive, $s = \mathrm{Id}$. L'application Ψ est donc injective.

Soit δ_{12} la droite passant par O qui joint les milieux des arêtes $[\mathrm{A}_1, \mathrm{A}'_2]$ et $[\mathrm{A}'_1, \mathrm{A}_2]$ et s_{12} le retournement d'axe δ_{12}. Il est immédiat que s_{12} échange les diagonales δ_1 et δ_2. La droite δ_{12} est orthogonale au plan P contenant A_3, A_4, A'_3 et A'_4. La restriction de s_{12} à P est donc la symétrie de centre O. L'application s_{12} laisse donc invariantes les diagonales δ_3 et δ_4. L'image de s_{12} par Ψ est la transposition des diagonales δ_1 et δ_2. On montre de même que $\Psi(\mathrm{Is}^+)$ contient toutes les transpositions et on conclut que ψ est surjective. Finalement Ψ est un isomorphisme de Is^+ sur $\mathcal{S}_4$.

Considérons maintenant les trois axes des faces, c'est-à-dire les trois droites passant par O et orthogonales à deux des faces du cube. On notera $\mathcal{A} = \{d_a, d_b, d_c\}$ l'ensemble de ces axes. Ils sont numérotés de telle façon que d_a (resp. d_b, resp. d_3) soient respectivement les axes des faces $\mathrm{A}_1\mathrm{A}'_2\mathrm{A}_3\mathrm{A}'_4$, $\mathrm{A}_1\mathrm{A}'_2\mathrm{A}_4\mathrm{A}'_3$ et $\mathrm{A}_1\mathrm{A}'_3\mathrm{A}_2\mathrm{A}'_4$.

Tout élément de $\mathrm{Is}^+(\mathcal{C})$ transformant une face du cube en une autre face et laissant O invariant, transforme un élément de $\mathcal{A}$ en un élément de $\mathcal{A}$. Elle opère donc une permutation de $\mathcal{A}$. En associant à tout élément u de $\mathcal{S}_4$ l'isométrie $\Psi^{-1}(u)$, puis à celle-ci une permutation de $\mathcal{A}$, identifiée à un élément de $\mathcal{S}_3$, on obtient comme précédemment pour le tétraèdre un morphisme f de $\mathcal{S}_4$ dans $\mathcal{S}_3$. Sachant qu'avec les notations précédentes, on a $\Psi(s_{1i}) = (1, i)$, on peut déterminer $\tau_i = f((1, i))$, pour $1 \leqslant i \leqslant 3$. On trouve de nouveau $\tau_2 = (a, b)$, $\tau_3 = (b, c)$ et $\tau_4 = (c, a)$ et on conclut de la même façon.

Conclusion. Au total, on trouve 10 morphismes de groupes de $\mathcal{S}_4$ dans $\mathcal{S}_3$. Le premier est constant, les trois suivants ont pour images les trois groupes de cardinal 2 de $\mathcal{S}_3$, les 6 autres sont surjectifs. $\lhd$

L'ensemble Aut(G) *des automorphismes d'un groupe* G, *muni de la composition est un groupe. Les conjugaisons* $f_a : x \longmapsto axa^{-1}$, *pour* $a \in$ G, *sont des automorphismes remarquables appelés automorphismes intérieurs de* G *(les autres seront dits extérieurs). L'ensemble des automorphismes intérieurs forme un sous-groupe de* Aut(G). *Ce sous-groupe est bien entendu trivial lorsque* G *est abélien. La connaissance de* Aut(G) *est importante en théorie des groupes pour les questions d'extension. Le lecteur pourra montrer à titre d'exercice que pour tout* $n \geqslant 2$, Aut$(\mathbb{Z}/n\mathbb{Z})$ *est isomorphe au groupe des inversibles de l'anneau* $\mathbb{Z}/n\mathbb{Z}$. *L'exercice suivant étudie les automorphismes du groupe symétrique.*

2.25. Automorphismes de $\mathcal{S}_n$

Soit $n \in \mathbb{N}^*$, $n \neq 6$. Montrer que les automorphismes de $\mathcal{S}_n$ sont intérieurs *i.e.* de la forme $s \longmapsto \sigma \circ s \circ \sigma^{-1}$ où $\sigma \in \mathcal{S}_n$. On s'intéressera aux images des transpositions.

(École normale supérieure)

$\rhd$ **Solution.**

• Soit φ un automorphisme du groupe symétrique. Nous savons que l'ensemble T des transpositions forme une partie génératrice de $\mathcal{S}_n$. L'automorphisme φ sera donc uniquement déterminé si l'on connaît les images par φ des transpositions. Pour commencer, examinons l'image d'une transposition et même l'image d'un élément quelconque de $\mathcal{S}_n$ par un automorphisme intérieur. Soit $\sigma \in \mathcal{S}_n$ et $(a_1, \ldots, a_k)$ un cycle de longueur k (on dira k-cycle). On a alors

$$\boxed{\sigma \circ (a_1, \ldots, a_k) \circ \sigma^{-1} = (\sigma(a_1), \ldots, \sigma(a_k))}. \quad (*)$$

Le lecteur vérifiera cette égalité sans grande difficulté. Un k-cycle est donc transformé en un k-cycle par tout automorphisme intérieur. En particulier une transposition est transformée en une transposition.

Plus généralement, si s est un élément de $\mathcal{S}_n$ et $s_1, \ldots, s_k$ les cycles apparaissant dans la décomposition de s en produit de cycles à support disjoint ($s = s_1 s_2 \ldots s_k$), on obtient

$$\boxed{\sigma s \sigma^{-1} = (\sigma s_1 \sigma^{-1})(\sigma s_2 \sigma^{-1}) \ldots (\sigma s_k \sigma^{-1})}. \quad (**)$$

Pour tout i, $\sigma s_i \sigma^{-1}$ est un cycle de même longueur que s_i d'après la formule $(*)$. Si $\{a_1, \ldots, a_p\}$ est le support de s_i, $\{\sigma(a_1), \ldots, \sigma(a_p)\}$ est le

support de $\sigma s_i \sigma^{-1}$. En particulier les $\sigma s_i \sigma^{-1}$ sont des cycles à supports disjoints.

Nous allons démontrer, pour commencer, que φ transforme toute transposition en une transposition. Un automorphisme de $\mathcal{S}_n$ conserve les propriétés algébriques des éléments de $\mathcal{S}_n$. Si τ est une transposition, τ est d'ordre 2, donc $\varphi(\tau)$ est aussi d'ordre 2. Cependant, cela ne suffit pas pour affirmer que $\varphi(\tau)$ est une transposition puisqu'il existe d'autres éléments d'ordre 2, les produits de transpositions à support disjoints (il n'y a qu'elles, puisque l'ordre d'une permutation est le ppcm des longueurs des cycles intervenant dans sa décomposition en produit de cycles à supports disjoints). Notons T_k l'ensemble des permutations de $\mathcal{S}_n$ qui sont produit d'exactement k transpositions à supports disjoints (pour $2k \leqslant n$). On a en particulier $\mathrm{T}_1 = \mathrm{T}$. Nous proposons deux démonstrations différentes du fait qu'un élément de T_1 est transformé par φ en un élément de T_1.

$\star$ D'après la relation $(**)$, chaque ensemble T_k est une classe de conjugaison de $\mathcal{S}_n$. L'image par φ d'une classe de conjugaison est encore une classe de conjugaison (car $\varphi(\sigma \circ \tau \circ \sigma^{-1}) = \varphi(\sigma) \circ \varphi(\tau) \circ \varphi(\sigma)^{-1}$). L'ensemble $\varphi(\mathrm{T}_1)$ est donc l'un des T_k.

On va montrer par un argument de cardinalité que, pour $n \neq 6$, on ne peut pas avoir $\varphi(\mathrm{T}_1) = \mathrm{T}_k$ avec $k \neq 1$. Pour cela, on va calculer le cardinal de T_k. On a $|\mathrm{T}_1| = \mathrm{C}_n^2 = \dfrac{n(n-1)}{2}$, car une transposition est déterminée par son support. Pour $k \geqslant 2$, on obtient $|\mathrm{T}_k| = \dfrac{\mathrm{C}_n^2 \mathrm{C}_{n-2}^2 \dots \mathrm{C}_{n-2k+2}^2}{k!}$: on choisit les supports des k transpositions et on divise par $k!$ car l'ordre n'importe pas. En simplifiant, il vient

$$|\mathrm{T}_k| = \frac{n(n-1)\dots(n-2k+1)}{2^k k!}.$$

Nous allons montrer que si $n \neq 6$, l'équation $|\mathrm{T}_k| = |\mathrm{T}_1|$, c'est-à-dire

$$k! 2^{k-1} = (n-2)(n-3)\dots(n-2k+1),$$

n'a pas de solution k strictement supérieure à 1 (avec $2k \leqslant n$).

En effet, pour $k = 2$, on obtient $(n-2)(n-3) = 4$, équation qui n'a pas de solution dans $\mathbb{N}$. Pour $k \geqslant 3$, il vient $\mathrm{C}_{n-k}^k (n-2)\dots(n-k+1) = 2^{k-1}$, ce qui ne peut arriver que si $n-k+1 = n-2$ (sinon le terme de gauche a un facteur impair), soit $k = 3$. Mais on a alors $(n-2)\mathrm{C}_{n-3}^3 = 4$ qui entraîne $n = 6$, cas qui est justement écarté. On a donc $\varphi(\mathrm{T}_1) = \mathrm{T}_1$

$\star$ Pour montrer qu'une transposition est transformée en une

transposition, on peut[3] s'intéresser au centralisateur d'une transposition τ, qui est transformé en celui de $\varphi(\tau)$ par l'automorphisme φ.

Soit s un élément de T_k qu'on écrit $s = \tau_1\tau_2\dots\tau_k$, où $\tau_1,\dots,\tau_k$ sont des transpositions à supports disjoints. La permutation σ est dans le centralisateur de s si elle vérifie $\sigma s\sigma^{-1} = s$. Nous avons vu que $\sigma s\sigma^{-1} = (\sigma\tau_1\sigma^{-1})\dots(\sigma s_k\sigma^{-1})$, où les $\sigma\tau_i\sigma^{-1}$ sont des transpositions à supports disjoints. Par unicité de la décomposition en produit de cycles à supports disjoints, on en déduit que les $\sigma\tau_i\sigma^{-1}$ doivent s'obtenir par permutation des τ_i. Il y a $k!$ possibilités pour σ de permuter les τ_i. Supposons une telle permutation des transpositions fixée, et par exemple qu'une transposition (a,b) est envoyé sur (a',b'). On doit avoir

$$(a',b') = \sigma(a,b)\sigma^{-1} = (\sigma(a),\sigma(b)),$$

c'est-à-dire $\{\sigma(a),\sigma(b)\} = \{a',b'\}$. On a donc 2 possibilités différentes pour définir σ sur l'ensemble $\{a,b\}$ sachant que cet ensemble est envoyé sur $\{a',b'\}$. Il reste ensuite à déterminer σ sur les éléments qui n'appartiennent pas au support d'une des transpositions τ_i. Pour ces $n-2k$ éléments, il y a $(n-2k)!$ choix possibles. Au total, il y a $2^k k!(n-2k)!$ permutations qui commutent avec s.

Soit maintenant une transposition τ. Son centralisateur est de cardinal $2(n-2)!$. Si $\varphi(\tau)$ appartient à T_k, son centralisateur possède $(n-2k)!k!2^k$ éléments. Nous avons donc $2(n-2)! = (n-2k)!k!2^k$, c'est-à-dire

$$k!2^{k-1} = (n-2)(n-3)\dots(n-2k+1).$$

Nous obtenons la même équation que dans la méthode précédente et la conclusion est la même.

Le fait que les deux méthodes conduisent à la même équation n'a rien de mystérieux. En effet le cardinal de la classe de conjugaison d'un élément est égal à l'indice de son centralisateur dans $\mathcal{S}_n$. Il revient donc au même de dire que deux éléments de $\mathcal{S}_n$ ont des classes de conjugaison de même cardinal et des centralisateurs de même cardinal (cf. exercice 2.11)

• On a donc $\varphi(\mathrm{T}) = \mathrm{T}$. On va s'intéresser aux images des transpositions $(1,k)$ pour $k \in [\![2,n]\!]$. Celles-ci suffisent à générer $\mathcal{S}_n$. Il existe a_1 et a_2 distincts tels que $\varphi((1,2)) = (a_1,a_2)$. De même, il existe a et b distincts tels que $\varphi((1,3)) = (a,b)$. Comme $(1,2)$ et $(1,3)$ ne commutent pas, (a_1,a_2) et (a,b) non plus, ce qui nécessite $\{a_1,a_2\}\cap\{a,b\} \neq \emptyset$. On peut supposer que $a = a_1$ et on note $a_3 = b$. On a donc $\varphi((1,3)) = (a_1,a_3)$. L'injectivité de φ assure que $a_2 \neq a_3$.

3. Comme le fait Daniel Perrin dans son *Cours d'algèbre*, Ellipses, 1996, p. 30-33. On y trouvera une étude précise des centralisateurs des éléments d'ordre 2 qui explique mieux en quoi le cas $n = 6$ se distingue.

Montrons par récurrence sur $i \in [\![2, n]\!]$ que $\varphi((1,i))$ s'écrit (a_1, a_i) où a_i est distinct des a_k pour $k < i$. C'est vrai pour $i = 2$ et 3. Supposons $i > 3$. Alors $\varphi((1,i))$ est une transposition dont le support rencontre celui de $\varphi((1,k)) = (a_1, a_k)$ pour $2 \leqslant k \leqslant i-1$ (par hypothèse de récurrence), car $(1,i)$ et $(1,k)$ ne commutent pas (la démonstration est la même que pour $i = 3$). Si a_1 n'était pas dans le support de $\varphi((1,i))$, les a_k pour $k \in [\![2, i-1]\!]$ y seraient. Comme ils sont au nombre de $i - 2 \geqslant 2$, cela ne peut se produire que si $i = 4$. Dans ces conditions $\varphi((1,4)) = (a_2, a_3) = (a_1, a_3)(a_2, a_1)(a_1, a_3) = \varphi((3,1)(1,2)(1,3))$ et par injectivité, on a $(1,4) = (3,1)(1,2)(1,3)$, ce qui est faux.

Donc a_1 est dans le support de $\varphi((1,i))$. Cette dernière s'écrit (a_1, a_i) et par injectivité de φ, a_i est bien distincts des a_k pour $k < i$.

• On se retrouve donc avec n éléments de $[\![1, n]\!]$, $a_1, \ldots, a_n$ deux à deux distincts tels que $\varphi((1,i)) = (a_1, a_i)$ pour tout $2 \leqslant i \leqslant n$. Si on considère la permutation σ qui à $i \in [\![1, n]\!]$ associe a_i, on a d'après la remarque préliminaire

$$\sigma \circ (1,i) \circ \sigma^{-1} = (a_1, a_i).$$

Autrement dit, φ coïncide sur l'ensemble des transpositions $(1,i)$ (où $2 \leqslant i \leqslant n$), avec l'automorphisme intérieur $\varphi_\sigma : s \longmapsto \sigma \circ s \circ \sigma^{-1}$. Comme φ est un morphisme et que les $(1,i)$ forment un système générateur de $\mathcal{S}_n$, on a $\varphi = \varphi_\sigma$.

Conclusion. Pour $n \neq 6$, tout automorphisme de $\mathcal{S}_n$ est intérieur. $\lhd$

Dans le cas exceptionnel $n = 6$, on peut montrer que $|\operatorname{Aut}(\mathcal{S}_6)| = 1440$, mais qu'il n'y a que 720 automorphismes intérieurs[4].

Nous terminons ce chapitre avec un exercice concernant la structure de groupe ordonné. Un groupe abélien $(\mathrm{G}, +)$ est dit ordonné s'il est muni d'un ordre total $\leqslant$ compatible avec la loi $+$, c'est-à-dire vérifiant

$$\forall (x,y,z) \in \mathrm{G}^3, \quad x \leqslant y \implies x + z \leqslant y + z.$$

Dans ce cas, on montre facilement que l'ensemble $\mathrm{P} = \{x \in \mathrm{G},\ 0 \leqslant x\}$ des éléments positifs de G possèdent les trois propriétés suivantes :

$$\mathrm{P} \cup (-\mathrm{P}) = \mathrm{G}, \quad \mathrm{P} \cap (-\mathrm{P}) = \{0\} \quad \textit{et} \quad \mathrm{P} + \mathrm{P} \subset \mathrm{P}.$$

Réciproquement, si P est une partie de G qui vérifient ces trois propriétés, alors la relation binaire $\leqslant$ définie par $x \leqslant y \iff y - x \in \mathrm{P}$ est une relation d'ordre total qui est compatible avec la loi $+$. Dans l'exercice suivant il s'agit de déterminer toutes les structures de groupe ordonné sur $\mathbb{Z}^2$.

4. On pourra se reporter à tout bon traité de théorie des groupes, par exemple le livre de Daniel Perrin déjà mentionné ou ROTMAN (J.), *An Introduction to the Theory of Groups*, GTM 148, 4e éd., Springer, 1995. p. 160-162.

2.26. Structure de groupe ordonné sur $\mathbb{Z}^2$

Si P est une partie non vide de $\mathbb{Z}^2$ on note

$$-\mathrm{P} = \{-p,\ p \in \mathrm{P}\} \quad \text{et} \quad \mathrm{P}+\mathrm{P} = \{p+q,\ (p,q) \in \mathrm{P}^2\}.$$

Trouver les parties P de $\mathbb{Z}^2$ vérifiant les points suivants :

(*i*) $\mathrm{P} \cup (-\mathrm{P}) = \mathbb{Z}^2$;

(*ii*) $\mathrm{P} \cap (-\mathrm{P}) = \{0\}$;

(*iii*) $\mathrm{P}+\mathrm{P} \subset \mathrm{P}$.

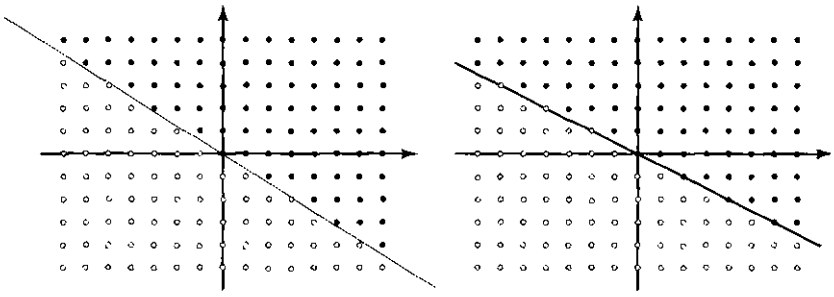
(École normale supérieure)

▷ **Solution.**

Il est clair que l'intersection de $\mathbb{Z}^2$ avec un demi-plan fermé de $\mathbb{R}^2$ dont la frontière contient $(0,0)$ convient si cette frontière ne contient pas d'autre point de $\mathbb{Z}^2$ que l'origine. On obtient donc une solution au problème posé en prenant pour P l'ensemble

$$\mathrm{P}_{a,b} = \{(x,y) \in \mathbb{Z}^2,\ ax+by \geqslant 0\},$$

avec $\dfrac{b}{a}$ irrationnel.



$\mathrm{P}_{a,b}$ avec b/a irrationnel $\qquad$ $\mathrm{P}^2_{1,2}$

Si la droite $ax+by=0$ contient des points de $\mathbb{Z}^2$, donc si $\dfrac{b}{a}$ est rationnel, ou si $a=0$, ces points sont tous les multiples entiers d'un même point (p,q), et on obtient deux ensembles P qui conviennent en ajoutant à l'ensemble

$$\{(x,y) \in \mathbb{Z}^2,\ ax+by > 0\}$$

soit les multiples entiers positifs, soit les multiples entiers négatifs de (p,q).

Il y a deux choix possibles pour (p, q). On choisira celui pour lequel la base $((a, b), (p, q))$ est orientée positivement. Les ensembles P ci-dessus sont donc

$$\mathrm{P}^1_{a,b} = \{(x, y) \in \mathbb{Z}^2,\ ax + by > 0\} \cup \mathbb{N}(p, q),$$
$$\mathrm{P}^2_{a,b} = \{(x, y) \in \mathbb{Z}^2,\ ax + by > 0\} \cup \mathbb{N}(-p, -q)$$

Soit maintenant une partie P de $\mathbb{Z}^2$ vérifiant (i), (ii), (iii). Montrons que P est de l'une des formes ci-dessus. Pour trouver une droite pouvant servir de «frontière» à P, il est naturel de considérer

$$\mathrm{P}^+ = \{(x, y) \in \mathrm{P},\ x > 0\} \quad \text{et} \quad m = \sup\left\{\frac{y}{x},\ (x, y) \in \mathrm{P}^+\right\}.$$

Afin d'éviter d'avoir à distinguer plusieurs cas de figure, on suppose que $(1, 0)$ et $(0, -1)$ sont dans P. On peut toujours se ramener à ce cas, d'abord parce que soit $(1, 0)$, soit son opposé est dans P, et de même pour $(0, -1)$, ensuite parce que les symétries par rapport à l'axe des x et par rapport à l'axe des y conservent les propriétés (i), (ii), (iii), ainsi que celle d'être de la forme $\mathrm{P}_{a,b}$ ou $\mathrm{P}^i_{a,b}$ ($i = 1$ ou 2).

La solution repose sur deux observations.

• Soit $(x, y) \in \mathbb{Z}^2$ et k un entier > 0. Alors $(x, y) \in \mathrm{P}$ si et seulement si $(kx, ky) \in \mathrm{P}$.

Le sens direct résulte de (ii). D'autre part, pour $(x, y) \neq 0$, on a

$$(x, y) \notin \mathrm{P} \Rightarrow (-x, -y) \in \mathrm{P} \Rightarrow (-kx, -ky) \in \mathrm{P} \Rightarrow (kx, ky) \notin \mathrm{P}.$$

• Soit $(x_0, y_0) \in \mathbb{Z}^2$, $(x, y) \in \mathbb{Z}^2$. Si $x_0 > 0$, $(x, y) \in \mathrm{P}^+$ et si

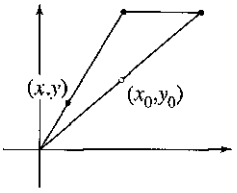
$$\frac{y_0}{x_0} < \frac{y}{x},$$

alors $(x_0, y_0) \in \mathrm{P}^+$.

En effet, tout point entier (x_0, y_0) tel que $y_0 < 0$ est dans P, puisque c'est une combinaison linéaire à coefficients positifs de $(1, 0)$ et $(0, -1)$. On peut donc supposer $y_0 > 0$ et $y > 0$. Il suffit alors de trouver des entiers k, ℓ, $n > 0$ tels que

$$k(x_0, y_0) = \ell(x, y) + n(1, 0).$$

On peut prendre $k = y$, $\ell = y_0$, $n = yx_0 - y_0x$ (on vérifie qu'on a bien $n > 0$).



Premier cas : m est fini. Soit $(x_0, y_0) \in \mathbb{Z}^2$ tel que $y_0 < mx_0$.

Si $x_0 > 0$, il existe, par définition de m, un point $(x, y) \in \mathrm{P}^+$ tel que $\frac{y_0}{x_0} < \frac{y}{x}$ et, d'après ce qui précède, $(x_0, y_0) \in \mathrm{P}$.

Si $x_0 < 0$, on a $\frac{-y_0}{-x_0} > m$, le point $(-x_0, -y_0)$ n'est pas dans P, et donc $(x_0, y_0) \in \mathrm{P}$.

Si $x_0 = 0$, alors (x_0, y_0) est un multiple entier positif de $(0, -1)$, et donc $(x_0, y_0) \in \mathrm{P}$.

Autrement dit, P contient $\mathrm{P}_{m,-1}$. Si m est irrationnel, l'ensemble P ne contient aucun des points entiers tels que $y > mx$, parce que leurs opposés sont dans P, et $\mathrm{P} = \mathrm{P}_{m,-1}$.

Si m est rationnel, disons $m = \frac{q}{p}$ (fraction irréductible, $p > 0$), le réseau $\mathbb{Z}^2$ se partitionne en trois parties : $\mathrm{P}_{m,-1}$, $-\mathrm{P}_{m,-1}$, et l'ensemble des points entiers situés sur la droite $y = mx$, qui est aussi l'ensemble des multiples entiers de (p, q). L'ensemble P contient soit (p, q) (et tous ses multiples positifs), soit $(-p, -q)$ (et tous ses multiples positifs), il est donc de la forme $\mathrm{P}^i_{m,-1}$, $i = 1$ ou 2.

Deuxième cas : $m = +\infty$. Pour tout point $(x_0, y_0) \in \mathbb{Z}^2$ tel que $x_0 > 0$, il existe $(x, y) \in \mathrm{P}^+$ tel que $\frac{y_0}{x_0} < \frac{y}{x}$, et, par, conséquent, $(x_0, y_0) \in \mathrm{P}$. On en déduit que P est formé des points entiers (x, y) tels que $x > 0$ ou $x = 0$ et $y \geqslant 0$. Autrement dit, $\mathrm{P} = \mathrm{P}^2_{1,0}$. $\lhd$

On a ainsi montré qu'une structure d'ordre sur $\mathbb{Z}^2$ (voir les commentaires précédant l'exercice) peut être définie de deux façons :

- soit on se donne une forme linéaire $f(x, y) = ax + by$ à coefficients réels tels que $\frac{b}{a}$ soit irrationnel, et les éléments $\geqslant 0$ de $\mathbb{Z}^2$ sont les éléments (x, y) tels que $f(x, y) \geqslant 0$;

- soit on se donne d'abord une forme linéaire $f(x, y) = ax + by$ à coefficients réels tels que $\frac{b}{a}$ soit rationnel ou $a = 0$, et on doit se donner une seconde forme linéaire g indépendante de f (on peut par exemple prendre $g(x, y) = -bx + ay$ ou $g(x, y) = bx - ay$; les autres choix ne donnent rien de différent). Les éléments $\geqslant 0$ de $\mathbb{Z}^2$ sont alors les éléments (x, y) tels que $f(x, y) > 0$ ou $f(x, y) = 0$, $g(x, y) \geqslant 0$. On retrouve l'ordre lexicographique sur $\mathbb{Z}^2$ comme cas particulier.

Chapitre 3

Anneaux et corps

À l'origine de la théorie des anneaux, se trouvent des recherches de théorie des nombres. Vers 1831, Gauss a été amené, dans ses travaux sur les résidus biquadratiques et sur les fonctions elliptiques, à étudier les propriétés de divisibilité dans l'anneau $\mathbb{Z}[i]$. *En 1844, Eisenstein utilisa* $\mathbb{Z}[j]$ *(où* $j^3 = 1$*). Dans les anneaux* $\mathbb{Z}[i]$ *et* $\mathbb{Z}[j]$, *l'arithmétique est semblable à celle de* $\mathbb{Z}$ *; en particulier, ce sont des anneaux factoriels (tout élément de l'anneau se décompose de manière unique – à un élément inversible près – en produits d'irréductibles). Les recherches sur le grand théorème de Fermat, en particulier la résolubilité de l'équation* $x^p + y^p = z^p$, *avec* p *premier impair, amènent à l'étude de l'anneau* $\mathbb{Z}[\zeta]$, *où* ζ *est une racine primitive* p*-ième de l'unité. Celui-ci se révéla avoir pour certaines valeurs de* p, *et contrairement à ce qu'on avait cru initialement (jusqu'en 1840), des propriétés arithmétiques totalement différentes de celles de* $\mathbb{Z}$.

À partir de 1847, Kummer grâce à l'introduction des concepts de nombres idéaux et de classes d'idéaux, élucide le problème de la divisibilité dans $\mathbb{Z}[\zeta]$ *et démontre la conjecture de Fermat dans de nombreux cas. En 1871, Dedekind, généralisant les travaux de Kummer, définit, dans le cadre de la théorie des entiers algébriques, la notions d'*idéal *et démontre qu'un idéal peut s'écrire comme produit d'*idéaux premiers. *Le terme d'*anneau *ne sera introduit que par Hilbert en 1897 : à partir du début du* XXe *siècle, il a fini par désigner tout ensemble sur lequel sont définies une loi de groupe additif et une multiplication associative et distributive.*

L'idée d'appartenance à un sous-corps de $\mathbb{C}$ *– le corps engendré par les racines d'une équation – est assez claire pour Abel et Galois, mais ils n'ont pas de mot pour désigner l'ensemble de ses éléments. C'est Dedekind qui introduit le terme de* corps *(en 1871), entendant par là des sous-corps de* $\mathbb{C}$, *pour lesquels il étudie en détail les notions d'intersection et d'automorphisme. Kronecker donne en 1882, les premiers exemples de corps définis abstraitement, corps de classes résiduelles de polynômes à coefficients rationnels modulo un polynôme* P. *Il faut attendre 1893 pour que Weber donne à l'expression corps commutatif le sens général actuel. Un peu plus tard vint l'abandon de la notion de commutativité, ce qui conduisit à considérer l'ensemble des quaternions définis par Hamilton en 1843 comme un corps. Weddeburn prouva que tout corps fini est nécessairement commutatif.*

Les exemples de corps vont se multiplier dans les dernières années du XIXe *siècle : corps des nombres p-adiques, introduit par Hensel, premier exemple de la théorie générale des corps valués; corps des séries formelles. Enfin, vers 1910, Steinitz développe la théorie générale des corps commutatifs et des extensions de corps telle que nous la connaissons aujourd'hui.*

3.1. Inversibilité à droite

Soit A un anneau. Un élément $a \in A$ est dit inversible à droite s'il existe b tel que $ab = 1$. On dit que a est un diviseur de 0 à droite si il existe $c \neq 0$ tel que $ac = 0$. On définit les mêmes notions à gauche.

1. Montrer que si a est inversible à droite il ne peut pas être diviseur de 0 à gauche. Donner un exemple montrant que a peut être inversible à droite et diviseur de 0 à droite.

2. Montrer que si a est inversible à droite et non diviseur de 0 à droite, alors il est inversible.

3. Prouver en fait que si a est inversible à droite et non inversible, alors il admet une infinité d'inverses à droite.

(**École Polytechnique**)

▷ **Solution.**

1. Soit b un inverse à droite de a (donc tel que $ab = 1$) et c tel que $ca = 0$. On multiplie à droite par b. Il vient $0 = (ca)b = c(ab) = c$. Donc a n'est pas diviseur de 0 à gauche. Rappelons que cela équivaut à l'injectivité du morphisme de groupes $x \mapsto xa$.

Donnons maintenant un exemple d'un élément inversible à droite et diviseur de 0 à droite. Prenons pour A l'anneau des endomorphismes d'un K-espace vectoriel E de dimension infinie. Une application linéaire a surjective et non injective va convenir. Par exemple avec $E = \mathbb{R}[X]$ pour espace vectoriel, on peut prendre la dérivation $a : P \mapsto P'$. L'application $b : P \mapsto \int_0^X P(t)dt$ est linéaire et on a $a \circ b = \mathrm{Id}_E$. Donc a est bien inversible à droite. Mais si on prend l'application $c : P \mapsto P(0)$, on a $a \circ c = 0$ donc a est aussi un diviseur de 0 à droite. On voit facilement sur cet exemple que a admet une infinité d'inverses à droite.

2. Soit b un inverse à droite de a. On va montrer que $ba = 1$. On a $a = (ab)a = a(ba)$ de sorte que $a(1-ba) = 0$. Comme a n'est pas diviseur de 0 à droite cela implique $ba = 1$. Donc a est inversible d'inverse b.

Cela montre déjà qu'un élément inversible à droite et non inversible admet au moins deux inverses à droite.

3. Notons D l'ensemble des inverses à droite de a (ensemble supposé

non vide) et $N = \{x \in A, ax = 0\}$ (c'est un sous-groupe additif de A et même un idéal à droite). On a une bijection entre D et N puisque si b est un élément de D, alors $D = b + N$. On va utiliser le fait, vu ci-dessus, que $\alpha = ba - 1$ est dans N. C'est même un élément non nul de N puisque a est supposé non inversible. Pour tout x de N, l'élément $xa + \alpha$ est encore dans N et est *non nul* (car sinon $(x + b)a = 1$ et a serait inversible à gauche donc inversible). Ainsi, $\alpha a + \alpha = \alpha(a+1) \in N$, $\alpha(a+1)a + \alpha = \alpha(a^2 + a + 1) \in N$ etc. Une récurrence facile montre que pour tout $n \geqslant 0$, $u_n = \alpha(a^n + a^{n-1} + \cdots + a + 1)$ est dans N. On va montrer que ces éléments sont deux à deux distincts. Supposons $u_n = u_p$ avec $p < n$. On a alors $\alpha(a^n + \cdots + a^{p+1}) = 0$ et donc $u_{n-p-1}a^{p+1} = 0$. Mais comme a est inversible à droite, on a forcément $u_{n-p-1} = 0$. Ce qui n'est pas possible car les u_n sont tous non nuls. Donc N est infini et par suite D aussi. $\lhd$

En particulier, dans un anneau fini, tout élément inversible à droite est inversible (ce qui est facile à établir directement puisque si a est inversible à droite, $x \mapsto xa$ est injective donc bijective par finitude de A).

3.2. Calcul d'inverse

> Soit A un anneau et $(a, b) \in A^2$. On suppose $1 - ab$ inversible. Montrer que $1 - ba$ est aussi inversible.
>
> **(École normale supérieure)**

1° **Solution.**

• Supposons dans un premier temps que ab est nilpotent et considérons $n \in N^*$ tel que $(ab)^n = 0$. On a alors

$$c = (1 - ab)^{-1} = 1 + ab + (ab)^2 + \cdots + (ab)^{n-1}.$$

Mais ba est alors également nilpotent puisque $(ba)^{n+1} = b(ab)^n a = 0$. Donc $1 - ba$ est aussi inversible et on a

$$\begin{aligned}(1 - ba)^{-1} &= 1 + ba + (ba)^2 + \cdots + (ba)^n \\ &= 1 + b[1 + (ab) + \cdots + (ab)^{n-1}]a = 1 + bca.\end{aligned}$$

• Dans le cas général, posons $c = (1 - ab)^{-1}$ et $d = 1 + bca$. Il est naturel d'essayer cette valeur comme inverse de $1 - ba$. On obtient

$$(1 - ba)d = (1 - ba)(1 + bca) = 1 - ba + bca - babca = 1 + b[c - abc - 1]a = 1$$

et de même $d(1 - ba) = 1$. D'où le résultat. $\lhd$

Les deux exercices suivants étudient des conditions suffisantes pour qu'un anneau soit commutatif. Le premier est un exemple d'anneau vérifiant une identité polynomiale.

3.3. Anneaux tels que $x^3 = x$

Soit A un anneau tel que $x^3 = x$ pour tout $x \in A$.

1. Déterminer les éléments nilpotents de A.

2. Soit $e \in A$ tel que $e^2 = e$, $a \in A$ et $b = ea(1-e)$.

Calculer b^2 et en déduire que $ea = ae$. En déduire que pour tout $x \in A$ $x^2 \in Z(A)$, où $Z(A)$ désigne le centre de A.

3. Montrer que A est commutatif.

(École normale supérieure)

▷ **Solution.**

1. Pour tout $n \in \mathbb{N}^*$ on a $x^n \in \{x, x^2\}$ (comme il résulte d'une récurrence immédiate sur n). Donc si x est nilpotent, il vérifie soit $x = 0$, soit $x^2 = 0$. Mais dans le second cas, on a $x = x^3 = xx^2 = 0$. Le seul élément nilpotent de A est donc 0.

2. On a $b^2 = ea(1-e)ea(1-e) = ea(e-e^2)a(1-e) = 0$. Donc b est nilpotent et d'après la question précédente, $b = 0$, c'est-à-dire $ea = eae$. En considérant de même $c = (1-e)ae$, on obtient $c^2 = 0$, puis $c = 0$ et $ae = eae$. Il en résulte que e commute avec a. On a ainsi montré que tout élément idempotent e est central.

Soit $x \in A$. On a $(x^2)^2 = x^4 = x^3x = x^2$: x^2 est idempotent et donc central.

3. Soit $x \in A$. On a $2x = (x+1)^2 - x^2 - 1 \in Z(A)$, d'après la question précédente, puisque $Z(A)$ est un sous-groupe additif de A. On a, d'autre part, $(x+1)^3 = x+1$. Comme $(x+1)^3 = x^3 + 3x^2 + 3x + 1 = 3x^2 + 4x + 1$, on obtient en simplifiant $3x^2 + 3x = 0$. L'élément $3x = -3x^2$ est donc dans $Z(A)$, puisque x^2 y est. Il en résulte que $x = 3x - 2x \in Z(A)$: tout élément de A est central, donc A est commutatif. ◁

Signalons un théorème dû à Jacobson : un anneau A dans lequel, pour tout élément x, il existe un entier $n(x) > 1$ tel que $x^{n(x)} = x$, est commutatif.

3.4. Commutativité ou anti-commutativité

Un pseudo-anneau est un triplet $(A, +, \cdot)$ qui vérifie tous les axiomes de la structure d'anneau, sauf celui qui affirme l'existence de l'élément-unité. Soit A un pseudo-anneau tel que, pour tout $(x, y) \in A^2$, $yx \in \{xy, -xy\}$. Montrer que A est commutatif ou anti-commutatif. Que dire si A est un anneau ?

(École normale supérieure)

Solution.

Notons Z le centre de A et posons $Z' = \{x \in A, \forall y \in A,\ yx = -xy\}$. Il est clair que Z et Z′ sont deux sous-groupes additifs de A.

Montrons qu'on a $Z \cup Z' = A$. Supposons par l'absurde qu'il existe $x \notin Z \cup Z'$. Alors, comme x n'est pas dans Z, il existe $y_1 \in A$ tel que $y_1 x \neq xy_1$. Par hypothèse on a nécessairement $y_1 x = -xy_1$. De même, comme $x \notin Z'$, il existe $y_2 \in A$ tel que $y_2 x \neq -xy_2$ et alors $y_2 x = xy_2$. Regardons maintenant l'élément $(y_1 + y_2)x = x(y_2 - y_1)$. Par hypothèse, il doit appartenir à $\{x(y_1+y_2), -x(y_1+y_2)\}$. Or, si $x(y_2-y_1) = x(y_1+y_2)$ on obtient $xy_1 = -xy_1 = y_1 x$, ce qui est contraire au choix de y_1. De même, si $x(y_2 - y_1) = -x(y_1 + y_2)$, il vient $xy_2 = -xy_2 = -y_2 x$, ce qui donne une nouvelle contradiction. On a donc $Z \cup Z' = A$.

Il est bien connu qu'un groupe ne peut pas être réunion de deux sous-groupes stricts. On obtient donc soit $Z = A$ auquel cas A est commutatif, soit $Z' = A$ auquel cas A est anti-commutatif.

Supposons que A soit un anneau. Si $Z' = A$, l'élément unité de A étant dans Z′, on a $1 = -1$ et A est de caractéristique 2. Mais dans ce cas, pour tout $(x, y) \in A^2$, $-xy = xy$ et A est commutatif. Ainsi, un anneau vérifiant l'hypothèse de l'exercice est toujours commutatif. ◁

3.5. Anneaux réguliers

Un anneau A est dit régulier si, pour tout $a \in A$, il existe $u \in A$ tel que $aua = a$.

1. Un corps est-il régulier ? $\mathbb{Z}$ est-il régulier ?

2. Trouver une condition nécessaire et suffisante pour que $\mathbb{Z}/n\mathbb{Z}$ soit régulier.

3. Montrer que si E est un K-espace vectoriel de dimension finie, $\mathcal{L}(E)$ est régulier. Soit $A = (a_{ij}) \in M_n(K)$ définie par $a_{i,i+1} = 1$ pour $1 \leqslant i \leqslant n-1$ et $a_{ij} = 0$ sinon. Trouver une matrice $U \in M_n(K)$ telle que $AUA = A$.

4. Montrer que le centre d'un anneau régulier est régulier.

(École normale supérieure)

Solution.

1. Observons que si $a = 0$, tout $u \in A$ vérifie $aua = a = 0$. Par ailleurs, si a est un élément inversible de A, en prenant $u = a^{-1}$ on obtient $aua = a$ et c'est d'ailleurs la seule valeur de u qui convienne. Comme dans un corps, tout élément non nul est inversible, il en résulte qu'un corps est régulier. L'anneau $\mathbb{Z}$ n'est pas régulier, comme on le voit en prenant $a = 2$; l'équation $4u = 2$ n'a pas de solution dans $\mathbb{Z}$. Remarquons d'ailleurs que si A est régulier et intègre, A est nécessairement un

corps. En effet, soit $a \neq 0$ et $u \in \mathrm{A}$ tel que $aua = a$. Par intégrité de A, a est régulier à gauche et à droite, d'où en simplifiant $ua = au = 1$. Donc a est inversible et A est un corps.

2. Il est aisé de voir que si A et B sont deux anneaux réguliers, alors l'anneau produit $\mathrm{A} \times \mathrm{B}$ est régulier. En effet, si $(a, b) \in \mathrm{A} \times \mathrm{B}$, il existe $u \in \mathrm{A}$ tel que $aua = a$ et $v \in \mathrm{B}$ tel que $bvb = b$. Alors, $(a, b)(u, v)(a, b) = (aua, bvb) = (a, b)$. D'où le résultat.

Excluons les cas triviaux $n = 0$, où $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}$ et donc non régulier, et $n = 1$, où l'on obtient l'anneau nul, clairement régulier. Si p est un nombre premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et est donc régulier. Si $n \geqslant 2$ est un entier quadratfrei, c'est-à-dire de la forme $n = p_1 \dots p_k$ où les p_i sont des nombres premiers distincts, on sait que $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$ (théorème chinois). Et d'après la remarque précédente, $\mathbb{Z}/n\mathbb{Z}$ est régulier.

Montrons que si n n'est pas quadratfrei, alors $\mathbb{Z}/n\mathbb{Z}$ n'est pas régulier. On suppose donc qu'il existe $p \in \mathcal{P}$ tel que $\alpha = \nu_p(n) \geqslant 2$. On écrit $n = p^\alpha m$, où p ne divise pas $m \geqslant 1$ et on pose $k = \dfrac{\alpha}{2}$ si α est pair et $k = \dfrac{\alpha+1}{2}$ sinon. Soit a la classe modulo n de $p^k m$. Il est clair que a est non nulle (car $k < \alpha$), mais pour tout $u \in \mathbb{Z}/n\mathbb{Z}$, $aua = ua^2 = 0$ (car $2k \geqslant \alpha$).

Conclusion. Pour $n \geqslant 2$, $\mathbb{Z}/n\mathbb{Z}$ est régulier si et seulement si n est quadratfrei.

3. Soit $a \in \mathcal{L}(\mathrm{E})$ non inversible (si $a \in \mathrm{GL}(\mathrm{E})$, $u = a^{-1}$ convient, cf. 1). On considère un supplémentaire F de $\operatorname{Ker} a$ et un supplémentaire G de $\operatorname{Im} a$. On sait que $a_{|\mathrm{F}}$ établit un isomorphisme entre F et $\operatorname{Im} a$. Si $u = a_{|\mathrm{F}}^{-1} \circ p$, où p est la projection sur $\operatorname{Im} a$ parallèlement à G, alors on a $aua = a$. L'anneau $\mathcal{L}(\mathrm{E})$ est donc régulier.

On considère

$$\mathrm{A} = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & \ddots & 0 & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \dots & 0 & 0 & 0 \end{pmatrix}$$

et l'endomorphisme a de $\mathbb{K}^n$ associé à la matrice A dans la base canonique, notée $(e_1, \dots, e_n)$. On obtient $\operatorname{Im}(a) = \operatorname{Vect}(e_1, \dots, e_{n-1})$, $\operatorname{Ker}(a) = \operatorname{Vect}(e_1)$ et avec les notations précédentes, $\mathrm{F} = \operatorname{Vect}(e_2, \dots, e_n)$ et $\mathrm{G} = \operatorname{Vect}(e_n)$. On vérifie, toujours avec les notations précédentes, que $(p(e_1), \dots, p(e_n)) = (e_1, e_2, \dots, 0)$ et $(u(e_1), \dots, u(e_n)) = (e_2, \dots, e_n, 0)$. La matrice U de u, dans la base canonique, est définie par $u_{i+1,i} = 1$

pour $1 \leqslant i \leqslant n-1$ et $u_{ij} = 0$ sinon. C'est la transposée de la matrice A. Elle vérifie AUA = A, puisque $aua = a$.

4. Soit Z le centre de l'anneau régulier A, $a \in$ Z et $u \in$ A tel que $aua = a$. On cherche un élément $v \in$ Z tel que $ava = a$. On va montrer que $v = uau$ convient. Il est clair que $ava = auaua = aua = a$. Il reste à montrer que v est central. Pour tout $b \in$ A, on a, puisque a est dans Z, $(1-au)bau = (a-aua)bu = 0$ et de même, $aub(1-au) = ub(a-aua) = 0$. Il en résulte que $bau - aubau = aub - aubau = 0$ et donc que $bau = aub$. Ainsi, au est dans Z. Enfin, on obtient, en utilisant le fait que a et au sont éléments de Z, pour tout $b \in$ A, $bv = buau = aubu = ubau = uaub = vb$. Ceci montre que v est dans Z. $\lhd$

Dans tous les exercices qui suivent, les anneaux seront commutatifs. Nous rappelons qu'un anneau A *est dit intègre s'il est commutatif et sans diviseur de* 0*, ce qui veut dire qu'un produit* ab *est nul si et seulement si* a *ou* b *est nul. Un idéal d'un anneau commutatif* A *est un sous-groupe additif* I *tel que pour tout* x *de* I *et tout* a *de* A*,* $ax \in$ I*. L'idéal* I *est dit principal s'il est engendré par un seul élément. On notera* (a) *ou aussi* aA *l'idéal principal engendré par* a*.*

3.6. Idéaux principaux

> Soit A un anneau commutatif. Pour a, b dans A montrer que si l'idéal $(a) + (b)$ est principal, il en est de même de l'idéal $(a) \cap (b)$.
> **(École normale supérieure)**

1. Solution.

Pour avoir des idées, on peut prendre un exemple simple bien connu A = $\mathbb{Z}$. Dans ce cas l'idéal $(a) + (b)$ est engendré par $d = \text{pgcd}(a, b)$ et l'idéal $(a) \cap (b)$ par $m = \text{ppcm}(a, b)$. Si on écrit $a = d\alpha$ et $b = d\beta$, on sait que m est associé à $d\alpha\beta$. Essayons donc ce générateur dans le cas général. On prend les notations ci-dessus : d est un générateur de $(a) + (b)$, $a = d\alpha$, $b = d\beta$ et on pose $m = d\alpha\beta$. Montrons par double inclusion que $(a) \cap (b) = (m)$.

• Soit $x \in (m)$. Il existe $\lambda \in$ A tel que $x = \lambda m = \lambda d\alpha\beta = \lambda\beta a = \lambda\alpha b$, de sorte que $x \in (a) \cap (b)$.

• Réciproquement, soit $x \in (a) \cap (b)$. On écrit $x = ua = vb$. On sait par ailleurs qu'il existe $(\lambda, \mu) \in$ A^2 tel que $d = \lambda a + \mu b$. On a alors

$$x = ua = u\alpha d = u\alpha(\lambda a + \mu b) = \alpha\lambda x + u\mu m = \alpha\lambda vb + u\mu m = m(\lambda v + \mu u).$$

D'où la seconde inclusion. $\lhd$

L'énoncé suivant concerne les idéaux maximaux, c'est-à-dire les idéaux distincts de A *qui sont maximaux au sens de l'inclusion.*

3.7. Idéaux maximaux

Soit A un anneau commutatif et I un idéal de A distinct de A.

1. Montrer que I est maximal pour l'inclusion parmi les idéaux de A distincts de A si et seulement si pour tout $a \in \mathrm{A}\setminus\mathrm{I}$, $\mathrm{I}+a\mathrm{A} = \mathrm{A}$.

On dit qu'un idéal I est premier si $\mathrm{A}\setminus\mathrm{I}$ est stable pour le produit.

2. Montrer que tout idéal maximal est premier.

3. Donner un exemple d'idéal premier.

4. Soit A l'anneau des fonctions de classe $\mathcal{C}^\infty$ de $\mathbb{R}$ dans $\mathbb{R}$ et I l'idéal des fonctions de A s'annulant en 0. L'idéal I est-il principal ? premier ? maximal ?

5. Soit J l'ensemble des fonctions de A telles que $f^{(k)}(0) = 0$ pour tout $k \in \mathbb{N}$. L'ensemble J est-il un idéal ? Si oui, est-il principal ? premier ? maximal ?

(**École Polytechnique**)

▷ **Solution.**

1. Soit I un idéal de A, distinct de A. On note que $\mathrm{I}+a\mathrm{A}$ est encore un idéal. C'est le plus petit idéal de A contenant I et a.

Supposons que I est maximal. Pour tout $a \in \mathrm{A}\setminus\mathrm{I}$, $\mathrm{I}+a\mathrm{A}$ est un idéal de A contenant I et distinct de I, car $a = 0 + a \cdot 1$ appartient à $\mathrm{I}+a\mathrm{A}$. On a donc $\mathrm{I}+a\mathrm{A} = \mathrm{A}$.

Supposons réciproquement que cette propriété est vérifiée. Si J est un idéal de A contenant I et distinct de I, on considère $a \in \mathrm{J}\setminus\mathrm{I}$. Alors J contient $\mathrm{I}+a\mathrm{A} = \mathrm{A}$ donc $\mathrm{J} = \mathrm{A}$ et I est maximal.

2. Soit I un idéal maximal, a et b deux éléments qui ne sont pas dans I. Comme $\mathrm{I}+a\mathrm{A} = \mathrm{A}$, il existe $c \in \mathrm{A}$ et $i \in \mathrm{I}$ tel que $1 = i + ac$. On en déduit $b = bi + abc$. Si $ab \in \mathrm{I}$, alors $abc \in \mathrm{I}$ et comme $bi \in \mathrm{I}$, $b \in \mathrm{I}$. C'est faux donc $ab \notin \mathrm{I}$ et I est premier.

3. Si $\mathrm{A} = \mathbb{Z}$, les idéaux $p\mathbb{Z}$, avec p premier, sont premiers. En effet, si a et b sont deux entiers tels que p divise ab, p divise a ou b. Ce sont les seuls idéaux premiers, car si n est entier naturel non premier, il existe des entiers n_1 et n_2 strictement supérieurs à 1 tels que $n = n_1n_2$. Alors n_1 et n_2 n'appartiennent pas à $n\mathbb{Z}$ et $n_1n_2 \in n\mathbb{Z}$, donc $n\mathbb{Z}$ n'est pas premier.

Notons que les idéaux $p\mathbb{Z}$, avec p premier, sont aussi maximaux. En effet si $a \notin p\mathbb{Z}$, a est premier avec p, donc $a\mathbb{Z} + p\mathbb{Z} = \mathrm{pgcd}(a,p)\mathbb{Z} = \mathbb{Z}$.

4. • La fonction $\mathrm{Id}_\mathbb{R}$ appartient à I. Montrons que I est principal, engendré par $\mathrm{Id}_\mathbb{R}$. Si f est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$ et s'annule en 0, la fonction

g définie par $g(x) = \dfrac{f(x)}{x}$ pour $x \neq 0$ et $g(0) = f'(0)$ est de classe $\mathcal{C}^\infty$ (théorème de division). Ce théorème a été démontré dans le tome 1 d'analyse (exercice 4.37). Rappelons-en rapidement une démonstration.

Pour $x \neq 0$, le changement de variable $t = ux$ donne

$$f(x) = \int_0^x f'(t)\,\mathrm{d}t = x\int_0^1 f'(ux)\,\mathrm{d}u \text{ et donc } g(x) = \int_0^1 f'(ux)\,\mathrm{d}u,$$

formule qui reste vraie pour $x = 0$. La fonction $h : (x,u) \longmapsto f'(xu)$ est indéfiniment dérivables par rapport à x et les dérivées partielles $\dfrac{\partial^k h}{\partial x^k}$: $(x,u) \longmapsto u^k f^{(k+1)}(xu)$ sont continues sur $\mathbb{R} \times [0,1]$. On en déduit que g est de classe $\mathcal{C}^\infty$.

Enfin, $f = g\,\mathrm{Id}_\mathbb{R}$ et $\mathrm{I} = \mathrm{Id}_\mathbb{R}\,\mathrm{A}$.

• L'idéal I est maximal car si f appartient à $\mathrm{A} \setminus \mathrm{I}$ et $g \in \mathrm{A}$, on a $f(0) \neq 0$, donc on peut écrire $g = \left(g - \dfrac{g(0)}{f(0)}f\right) + \dfrac{g(0)}{f(0)}f$; ainsi g appartient à $\mathrm{I} + f\mathrm{A}$. D'après la question 2, I est *a fortiori* premier.

5. • Il est clair que J est un sous-groupe additif de A. Si $f \in \mathrm{J}$ et $g \in \mathrm{A}$, la formule de Leibniz montre que fg a toutes ses dérivées nulles en 0. Elle est donc dans J : c'est un idéal de A.

• Montrons que J n'est pas principal en raisonnant par l'absurde. Soit f tel que $\mathrm{J} = f\mathrm{A}$. Comme $f(0) = 0$, il existe g dans A telle que $f = \mathrm{Id}_\mathbb{R}\,g$. La démonstration de la question 4 montre que $g(x) = \int_0^1 f'(ux)\,\mathrm{d}u$, pour tout réel x et donc que $g^{(k)}(x) = \int_0^1 u^k f^{(k+1)}(ux)\,\mathrm{d}u$, pour tout (k,x) de $\mathbb{N} \times \mathbb{R}$. On a, en particulier $g^{(k)}(0) = \int_0^1 u^k f^{(k+1)}(0)\,\mathrm{d}u = 0$. Ainsi $g \in \mathrm{J}$ et il existe $h \in \mathrm{A}$ telle que $g = fh = \mathrm{Id}_\mathbb{R}\,gh$. Montrons que g ne s'annule qu'en 0. Il est classique que la fonction φ définie sur $\mathbb{R}$ par $\varphi(x) = \begin{cases} e^{-\frac{1}{x^2}} & \text{si } x \neq 0 \\ 0 & \text{si } x = 0 \end{cases}$ appartient à J. Comme $\varphi \in f\mathrm{A}$ et ne s'annule qu'en 0, il en est de même de f et donc de g. On obtient donc $1 = xh(x)$ pour tout $x \neq 0$. En faisant tendre x vers 0, on obtient une contradiction. Donc J n'est pas principal.

• L'idéal J n'est pas maximal car il est contenu strictement dans I.

• Montrons que J est premier. Soit f et g deux éléments de $\mathrm{A} \setminus \mathrm{J}$. Notons $n = \inf\{k \in \mathbb{N}, f^{(k)}(0) \neq 0\}$ et $p = \inf\{k \in \mathbb{N}, g^{(k)}(0) \neq 0\}$. D'après la formule de Leibniz, on a

$$(fg)^{(n+p)}(0) = \sum_{k=0}^{n+p} \mathrm{C}_{n+p}^k f^{(k)}(0) g^{(n+p-k)}(0) = f^{(n)}(0) g^{(p)}(0) \neq 0,$$

car si $k < n$, $f^{(k)}(0) = 0$ et si $k > n$, $n + p - k < p$ et $g^{(n+p-k)}(0) = 0$. Ainsi fg n'appartient pas à J. $\lhd$

Un anneau principal est un anneau intègre dont tout idéal est principal; nous savons, en particulier, que les anneaux $\mathbb{Z}$ *et* $\mathrm{K}[\mathrm{X}]$, *où* K *est un corps, sont principaux. Les exercices suivants sont des études de principalité.*

3.8. Anneau des nombres décimaux

Soit D l'anneau des nombres décimaux :

$$\mathrm{D} = \{x \in \mathbb{Q},\ \exists n \in \mathbb{Z},\ x \cdot 10^n \in \mathbb{Z}\}.$$

Montrer que D est principal.

(École polytechnique)

▷ **Solution.**

Il est évident que D est un sous-anneau de $\mathbb{Q}$. Remarquons que les éléments de D sont les nombres rationnels dont le dénominateur possède comme seuls diviseurs premiers 2 et 5. Tout élément non nul x de D s'écrit donc de manière unique $x = 2^\alpha 5^\beta p$, avec $p \in \mathbb{Z}$ premier avec 10 et α et β dans $\mathbb{Z}$.

La démonstration de la principalité de D sera calquée sur celle de $\mathbb{Z}$. On considère un idéal non nul I de D (car l'idéal nul est évidemment principal). Si, avec les notations précédentes, $x = 2^\alpha 5^\beta p$ est un élément non nul de I, alors $p = 2^{-\alpha}5^{-\beta}x$ est un élément de I, car $2^{-\alpha}5^{-\beta}$ appartient à D. Ainsi $|p|$ appartient à $\mathbb{N}^* \cap \mathrm{I}$. Cet ensemble est une partie non vide de $\mathbb{N}^*$, qui possède un plus petit élément a. On a clairement $a\mathrm{D} \subset \mathrm{I}$. Réciproquement, si $x = 2^\alpha 5^\beta p$ appartient à I, il en est de même de l'entier p. On divise p par a : $p = aq + r$. On obtient que $r = p - aq \in \mathrm{I} \cap \mathrm{N}^*$, avec $0 \leqslant r < a$. De la définition de a, on déduit que $r = 0$, que $p = aq$ et donc que $x = a(q2^\alpha 5^\beta)$. Ceci montre que $\mathrm{I} \subset a\mathrm{D}$ et donc que $\mathrm{I} = a\mathrm{D}$. ◁

Le lecteur pourra montrer de la même manière que tout sous-anneau de $\mathbb{Q}$ *est principal.*

3.9. Anneau $\mathbb{Z}[\mathrm{X}]$

1. L'anneau $\mathbb{Z}[\mathrm{X}]$ est-il principal ?

2. Soit A un anneau commutatif. À quelle condition $\mathrm{A}[\mathrm{X}]$ est-il principal ?

(École normale supérieure)

Solution.

1. Pour montrer la non-principalité, il suffit d'exhiber un idéal non principal. C'est le cas de l'idéal I engendré par 2 et X. En effet, supposons qu'il existe $P \in \mathbb{Z}[X]$ tel que $I = (P)$. Comme $2 \in I$, P doit être constant et diviser 2. Donc $P = \pm 1$ ou $P = \pm 2$. Mais comme 2 ne divise pas X dans $\mathbb{Z}[X]$, on a $P = \pm 1$. L'idéal $I = (2) + (X)$ contient alors 1, et on peut écrire $1 = 2U + XV$, avec U et V dans $\mathbb{Z}[X]$. On obtient, en considérant les valeurs en 0 des polynômes, $1 = 2U(0)$, ce qui est absurde, puisque $U(0) \in \mathbb{Z}$.

2. Nous savons que si A est un corps, A[X] est principal. Montrons que c'est une condition nécessaire. On raisonne par contraposition, en supposant que A n'est pas un corps. Il possède donc un élément non inversible a. Comme dans la première question, on considère l'idéal engendré par a et X. Supposant qu'il est principal, on trouve de nouveau qu'il est engendré par l'élément unité de A, que celui-ci s'écrit $1 = aU + XV$ et qu'enfin $1 = aU(0)$, ce qui contredit la non-inversibilité de a.

Conclusion. A[X] est principal si et seulement si A est un corps. ◁

L'arithmétique de l'anneau $\mathbb{Z}[X]$ est tout de même assez simple car il est factoriel, c'est-à-dire qu'un élément non nul se décompose de manière essentiellement unique en un produit d'irréductibles (d'après un théorème général de Gauss qui affirme que si A est un anneau factoriel, A[X] l'est aussi). Pour la définition précise d'un anneau factoriel voir l'exercice suivant, qui démontre que tout anneau principal est factoriel.

3.10. Anneaux factoriels

Soit A un anneau intègre. Un élément $p \in A^*$ est dit irréductible s'il n'est pas inversible et si, pour toute écriture $p = uv$, avec u et v dans A, on a u ou v inversible. Si $(a, b) \in A^2$, a et b sont dits associés si a s'écrit $a = ub$, avec u inversible. «Être associés» est une relation d'équivalence sur A.

A est dit factoriel si tout $a \in A^*$ peut s'écrire $a = up_1^{\alpha_1} \dots p_r^{\alpha_r}$ avec u inversible, les p_i irréductibles deux à deux non associés, et les $\alpha_i \in \mathbb{N}^*$. De plus cette écriture est unique au sens suivant : si $a = vq_1^{\beta_1} \dots q_s^{\beta_s}$ avec v inversible, les q_i irréductibles deux à deux non associés, les $\beta_i \in \mathbb{N}^*$, on a $r = s$ et quitte à renuméroter les q_i, p_i et q_i sont associés et $\alpha_i = \beta_i$ pour tout $1 \leqslant i \leqslant r$.

Montrer qu'un anneau principal est factoriel.

(École normale supérieure)

▷ **Solution.**

• Existence de l'écriture : dans $\mathbb{Z}$, l'existence de la décomposition de n s'obtient par récurrence sur n, dans K[X] où K est un corps commutatif, la décomposition de P s'obtient par récurrence sur deg P. Dans notre cas de figure, une démonstration par récurrence s'avère impossible car on ne voit pas sur quel entier elle se ferait. On va raisonner par l'absurde et supposer qu'il existe $a \in A^*$ qui n'admet pas une telle décomposition. Alors a n'est ni inversible, ni irréductible et par conséquent, il s'écrit $a = uv$ avec u et v dans A^* non inversibles. Si u et v admettaient une décomposition, le produit $a = uv$ en admettrait une aussi, ce qui est exclu par hypothèse. Supposons par exemple que u n'admet pas de décomposition. On pose $a_1 = u$. On a donc trouvé a_1 n'admettant de décomposition, divisant a et non associé à a puisque v est non inversible.

En réitérant ce raisonnement, on construit une suite $(a_n)_{n\in\mathbb{N}}$, avec $a_0 = a$ et pour tout $n \in \mathbb{N}$, a_{n+1} divise a_n, n'est pas associé à a_n et n'admet pas de décomposition.

Considérons les idéaux $I_n = a_nA$ pour tout $n \in \mathbb{N}$. Comme a_{n+1} divise a_n, $I_n \subset I_{n+1}$. L'inégalité est stricte. En effet, si elle ne l'était pas, on aurait $a_n | a_{n+1}$ et il existerait u et v dans A tels que $a_n = ua_{n+1}$ et $a_{n+1} = va_n$. Mais alors $a_n = uva_n$ et comme a_n est non nul et A intègre, $uv = 1$. Il en résulterait que u serait inversible et a_n et a_{n+1} associés, ce qui est exclu.

Considérons $I = \bigcup_{n\in\mathbb{N}} I_n$. Montrons que I est un idéal. Il est non vide. Soit $\alpha \in A$ et $(x, y) \in I^2$. Il existe $(n, p) \in \mathbb{N}^2$ tel que $x \in I_n$ et $y \in I_p$. On pose $m = \max(n, p)$. Alors x et y sont dans I_m puisque la suite $(I_n)_{n\in\mathbb{N}}$ est croissante. On a donc $x + y \in I_m \subset I$ et $\alpha x \in I_m \subset I$.

Comme A est un anneau principal, il existe donc $b \in I$ tel que $I = bA$. Par définition de I, il existe $n_0 \in \mathbb{N}$ tel que $b \in I_{n_0}$. Mais alors si $n \geqslant n_0$, on a

$$bA \subset I_{n_0} \subset I_n \subset I = bA$$

et la suite $(I_n)_{n\in\mathbb{N}}$ est stationnaire à partir du rang n_0, ce qui contredit sa stricte croissante. L'hypothèse absurde était donc l'existence de a indécomposable. On en déduit qu'il existe pour tout $a \in A^*$ une décomposition en produit d'irréductibles[1].

• Prouvons maintenant l'unicité de l'écriture. Soit $a \in A^*$. On suppose que l'on a deux écritures :

$$a = up_1^{\alpha_1} \dots p_r^{\alpha_r} = vq_1^{\beta_1} \dots q_s^{\beta_s}$$

1. Notons que la preuve demeure valide si A a la propriété que toute suite croissante d'idéaux est stationnaire. Un anneau intègre vérifiant cette propriété est dit noethérien.

avec u et v inversibles, les p_i irréductibles deux à deux non associés, les q_j irréductibles deux à deux non associés, les α_i et β_j dans $\mathbb{N}^*$. Montrons par récurrence sur $\alpha_1 + \cdots + \alpha_r$ que $r = s$ et que, quitte à renuméroter les q_j, on a p_i et q_i associés et $\alpha_i = \beta_i$ pour tout $1 \leqslant i \leqslant r$.

$\star$ Si $\alpha_1 + \cdots + \alpha_r = 0$, $r = 0$, a est inversible donc nécessairement $s = 0$ (si $s \geqslant 1$, q_1 serait alors inversible).

$\star$ Supposons $\alpha_1 + \cdots + \alpha_r \geqslant 1$. Alors p_r divise a. Démontrons le lemme suivant qui peut encore s'appeler lemme d'Euclide :

Lemme. *Soit p irréductible divisant la produit ab avec a et b dans* A. *Alors p divise a ou p divise b.*

Démonstration.

Considérons l'idéal engendré par p et b : $\mathrm{I} = p\mathrm{A} + b\mathrm{A}$. Comme A est principal, il existe $c \in \mathrm{A}$ tel que $\mathrm{I} = c\mathrm{A}$. Puisque p est dans I, c divise p. Donc c est inversible ou c est associé à p puisque p est irréductible. Dans le premier cas, $\mathrm{I} = \mathrm{A}$ et 1 s'écrit $1 = up + vb$ avec $(u, v) \in \mathrm{A}^2$. Donc $a = upa + vab$ et comme p divise ab, il divise a.

Dans le second cas, c associé à p, $\mathrm{I} = c\mathrm{A} = p\mathrm{A}$ et comme $b \in \mathrm{I}$, p divise b. Le lemme est prouvé. $\diamondsuit$

Comme p_r est irréductible, diviseur de $a = vq_1^{\beta_1} \ldots q_s^{\beta_s}$, d'après le lemme d'Euclide étendu par récurrence à un nombre quelconque de facteurs, il divise l'un des facteurs. Il ne peut diviser v puisque sinon, p_r serait inversible. Il divise donc l'un des q_i. Comme q_i est irréductible, q_i et p_r sont nécessairement associés. Quitte à les numéroter et à changer v en un autre inversible, on peut supposer $q_s = p_r$. On divise alors a par p_r. Il vient

$$\frac{a}{p_r} = up_1^{\alpha_1} \ldots p_{r-1}^{\alpha_{r-1}} p_r^{\alpha_r - 1} = vq_1^{\beta_1} \ldots q_{s-1}^{\beta_{s-1}} p_r^{\beta_s - 1}$$

Si $\alpha_r - 1 > 0$, le raisonnement précédent prouve que, puisque p_r divise $\dfrac{a}{p_r}$, il divise l'un des q_i. Comme les q_i sont non associés deux à deux, p_r divise nécessairement le facteur $p_r^{\beta_s - 1} = q_s^{\beta_s - 1}$ et en particulier $\beta_s - 1 > 0$. On est en droit d'appliquer l'hypothèse de récurrence à $\dfrac{a}{p_r}$: on a $r = s$ et quitte à renuméroter les q_i, p_i et q_i sont associés et $\alpha_i = \beta_i$ pour $i < r$, $\alpha_r - 1 = \beta_r - 1$ ce qui donne bien $\alpha_r = \beta_r$.

Si $\alpha_r - 1 = 0$, alors nécessairement $\beta_s - 1 = 0$. En effet, dans le cas contraire $q_s = p_r$ diviserait $up_1^{\alpha_1} \ldots p_{r-1}^{\alpha_{r-1}}$ et donc d'après le lemme d'Euclide, il diviserait l'un des p_i avec $i < r$ ce qui est impossible puisque les p_i sont deux à deux non associés. On applique alors l'hypothèse de récurrence à

$$\frac{a}{p_r} = up_1^{\alpha_1} \ldots p_{r-1}^{\alpha_{r-1}} = vq_1^{\beta_1} \ldots q_{s-1}^{\beta_{s-1}}$$

et on obtient : $r - 1 = s - 1$; quitte à renuméroter les q_i, p_i et q_i sont associés et $\alpha_i = \beta_i$ pour $i < r$. Comme on avait déjà $p_r = q_r$ et $\alpha_r = 1 = \beta_r$, l'unicité de la décomposition est prouvée.

Conclusion. Un anneau principal est factoriel. $\lhd$

L'exercice suivant rappelle la définition d'un anneau euclidien, montre qu'un anneau euclidien est principal et s'intéresse aux anneaux euclidiens dans lesquels la division euclidienne est unique.

3.11. Anneaux euclidiens

A étant un anneau intègre, on dit que A est euclidien lorsqu'il existe une application $\varphi : \mathrm{A}\backslash\{0\} \longrightarrow \mathbb{N}$ telle que, pour $a \in \mathrm{A}$ et $b \in \mathrm{A} \setminus \{0\}$, il existe $(q, r) \in \mathrm{A}^2$ tel que

$$a = bq + r \text{ et } r = 0 \text{ ou } \varphi(r) < \varphi(b). \quad (*)$$

1. Donner des exemples d'anneaux euclidiens.

2. Montrer qu'un anneau euclidien est principal.

3. On suppose de plus que A n'est pas un corps et que, pour tout a et b le couple (q, r) défini par $(*)$ est unique. Montrer que A est isomorphe à l'anneau des polynômes sur un certain corps.

(École normale supérieure)

$\rhd$ **Solution.**

1. • On peut prendre $\mathrm{A} = \mathbb{Z}$ et $\varphi : x \longmapsto |x|$. En effet, soit $a \in \mathbb{Z}$, $b \in \mathbb{Z}\backslash\{0\}$. Si q et r désignent respectivement le quotient et le reste de la division euclidienne de a par $|b|$, on a bien

$$a = b\varepsilon q + r \text{ et } r = 0 \text{ ou } 0 \leqslant r < |b|,$$

avec $|b| = \varepsilon b$ et $\varepsilon = \pm 1$.

• L'autre exemple du cours est $\mathrm{K}[\mathrm{X}]$ où K est un corps commutatif : la division euclidienne donne le couple q et r et pour l'application φ, il suffit de prendre la fonction degré.

• L'exercice 3.12 montre que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est euclidien.

2. Soit A un anneau euclidien. Par définition, A est intègre. Considérons un idéal I de A et montrons que I est principal. C'est clair si I est nul. Si $\mathrm{I} \neq \{0\}$, considérons l'ensemble $\mathrm{F} = \{\varphi(a) \in \mathbb{N}, a \in \mathrm{I}, a \neq 0\}$. C'est une partie non vide de $\mathbb{N}$, qui admet donc un plus petit élément. Il existe donc un élément a_0 non nul de I tel que $\varphi(a_0) = \min \mathrm{F}$. On a, bien entendu, $a_0\mathrm{A} \subset \mathrm{I}$.

Réciproquement, si $a \in \mathrm{I}$, il existe $(q, r) \in \mathrm{A}^2$ tel que $a = qa_0 + r$ avec $r = 0$ ou $\varphi(r) < \varphi(a_0)$. On en déduit que $r = a - a_0 q$ est dans I, puisque I est un idéal. Si r n'est pas nul, on obtient $\varphi(r) < \varphi(a_0) = \min \mathrm{F}$, ce qui est impossible. On a donc nécessairement $r = 0$ et $a = a_0 q \in a_0\mathrm{A}$. On conclut que $\mathrm{I} = a_0\mathrm{A}$: l'idéal I est principal.

On note que les exemples d'anneaux principaux les plus importants du cours sont des anneaux euclidiens. Il est assez difficile d'exhiber des anneaux principaux non euclidiens mais cela existe[2].

3. Il s'agit de sortir de notre chapeau le corps K dont A serait l'anneau des polynômes. Or, dans K[X], le corps K est composé de 0 et des éléments de degré minimal (à savoir 0). Cela nous donne une piste pour définir K : il serait constitué, outre 0, des éléments x non nuls de A, pour lesquels $\varphi(x)$ est minimal.

• Avant d'entrer dans le détail, nous allons introduire plusieurs notations et faire quelques remarques simples. A^* désigne comme d'habitude $\mathrm{A} \setminus \{0\}$ et $\mathrm{A}^\times$ l'ensemble des éléments inversibles de A. Deux éléments a et b de A sont dits associés s'il existe u inversible dans A tel que $a = bu$ (être associés est une relation d'équivalence). Enfin, si dans A, $a = bq + r$ avec $b \neq 0$, $r = 0$ ou $\varphi(r) < \varphi(b)$, on dira qu'il s'agit d'une division euclidienne de a par b. Par hypothèse, une division de a par b est unique.

Lemme. *Si a et b appartiennent à A et si $a|b$, alors $\varphi(a) \leqslant \varphi(b)$.*
Si a et b sont associés dans A^*, $\varphi(a) = \varphi(b)$.

Démonstration. En effet, si $a|b$ et si $\varphi(a) > \varphi(b)$, on a deux divisions euclidiennes de b par a : $b = a \times c + 0$ et $b = a \times 0 + b$, où $c = \dfrac{b}{a}$, ce qui est contraire à l'hypothèse. Si a et b sont associés, on a $a|b$ et $b|a$, d'où résultent les relations $\varphi(a) \leqslant \varphi(b)$ et $\varphi(b) \leqslant \varphi(a)$ et l'égalité annoncée. ◇

• Pour tout $a \in \mathrm{A}^*$, 1 divise a ; on a donc $\varphi(1) \leqslant \varphi(a)$. Il s'ensuit que $m_0 = \varphi(1) = \min \varphi$. Puisque 1 est associé à tout inversible de A, on obtient

$$\mathrm{A}^\times \subset \{x \in \mathrm{A}^*,\ \varphi(x) = m_0\}$$

Réciproquement, si $x \in \mathrm{A}^*$ et $\varphi(x) = m_0$, x est inversible. En effet, il existe q et r dans A tels que $1 = xy + r$ avec $r = 0$ ou $\varphi(r) < \varphi(x)$. Comme $\varphi(x) = m_0 = \min \varphi$, cette seconde condition est impossible, et on a $1 = xy$ et $x \in \mathrm{A}^\times$. On conclut :

$$\mathrm{A}^\times = \{x \in \mathrm{A}^*, \varphi(x) = m_0\}$$

2. PERRIN (D.), *Cours d'algèbre*, Ellipses, 1996, p. 53-54.

• Tout nous pousse à poser $K = A^\times \cup \{0\}$. Montrons que K est un corps commutatif.

⋆ Comme $K^* = A^\times$, nous savons déjà que $(K^*, \times)$ est un groupe commutatif.

Montrons que K est un sous-anneau de A.

⋆ K^* et donc K sont stables par multiplication.

⋆ $1 \in K$ et si $a \in K$, alors $-a \in K$.

⋆ Il reste à montrer la stabilité par addition. Soit a et b dans K. Si a ou b est nul, il est clair que $a + b$ est dans K. Supposons $a \neq 0$ et $b \neq 0$. Étant donné que $a + b = a(1 + a^{-1}b)$ et que K est stable par multiplication, il suffit de prouver le résultat suivant : si $u \in K^*$, alors $1 + u \in K$.

Raisonnons par l'absurde et supposons que $1 + u \notin K$. Alors, $1 + u$ est non nul, $\varphi(1 + u) > m_0 = \varphi(1) = \varphi(-u^{-1})$ et on peut écrire

$$1 = (1 + u) \times 0 + 1, \text{ mais aussi } 1 = (1 + u) \times u^{-1} + (-u^{-1}).$$

On a donc deux divisions euclidiennes de 1 par $1+u$, ce qui est contraire à l'hypothèse.

Établissons un bilan provisoire : K est corps commutatif, sous-anneau de A. Comme A n'est par un corps, $K \subsetneq A$.

• Dans $K[X]$, X est un polynôme de degré 1, *i.e.* de degré minimal parmi les polynômes non constants. Il est donc naturel de considérer ici un élément de $A \setminus K$, où φ est minimale. L'entier $m_1 = \min_{x \in A \setminus K} \varphi(x)$ est bien défini (car $A \setminus K \neq \emptyset$) et il existe $X_0 \in A \setminus K$ tel que $\varphi(X_0) = m_1$. Introduisons la fonction

$$\Psi : \begin{array}{ccc} K[X] & \longrightarrow & A \\ P & \longmapsto & P(X_0) \end{array}$$

Il s'agit d'un morphisme de K-algèbres. Montrons que Ψ est un isomorphisme.

• Prouvons l'injectivité de Ψ : montrons par récurrence sur $n \in \mathbb{N}$, que si $\deg P \leqslant n$ et $P(X_0) = 0$, alors $P = 0$.

⋆ C'est bon si $P = 0$ ou $\deg P = 0$ (car alors $P(X_0) = P \in K$).

⋆ Supposons $n \geqslant 1$ et la propriété vraie jusqu'au rang $n - 1$. Soit $P \in K[X]$ tel que $P(X_0) = 0$. En écrivant $P = a_n X^n + \cdots + a_1 X + a_0$, on obtient

$$0 = P(X_0) = (a_n X_0^{n-1} + \cdots + a_1)X_0 + a_0$$

On reconnaît là une division euclidienne de 0 par X_0. En effet soit $a_0 = 0$, soit $a_0 \in A^\times$ et $\varphi(a_0) = m_0 < \varphi(X_0) = m_1$. Puisque $0 = 0 \times X_0 + 0$, on obtient par unicité $a_0 = 0$ et $Q(X_0) = 0$ avec $Q = a_n X^{n-1} + \cdots + a_1$.

Comme $\deg Q \leqslant n-1$, par l'hypothèse de récurrence, on obtient $Q = 0$. Il en résulte que $P = 0$.

• La surjectivité est plus délicate. On veut montrer que les éléments de A sont dans $K[X_0] = \operatorname{Im}\Psi$. C'est vrai pour les éléments $x \in A^*$ tels que $\varphi(x) = m_0$: ils sont dans K. On va tenter une récurrence sur « $\varphi(x)$» que l'on pourrait diminuer par une division euclidienne par X_0. Plus précisément, montrons par récurrence sur $n \in \mathbb{N}$ que si $x \in A^*$ et $\varphi(x) \leqslant n$, alors $x \in K[X_0]$.

C'est vrai si $n \leqslant m_0$.

Supposons $n > m_0$, et la propriété vérifiée jusqu'à l'entier $n-1$. Prenons $x \in A^*$ avec $\varphi(x) \leqslant n$. On peut supposer $\varphi(x) > m_0$ *i.e.* $x \notin K$. Divisons x par X_0 : il existe q et r dans A tels que $x = X_0 q + r$ avec $r = 0$ ou $\varphi(r) < \varphi(X_0)$. Par conséquent, r appartient à K. Pour montrer que x est dans $K[X]$, il suffit de montrer que q est dans $K[X_0]$. D'après l'hypothèse de récurrence, c'est vrai si $\varphi(q) \leqslant n-1$. Or, on a $\varphi(X_0 q) = \varphi(x-r)$. Puisque $\varphi(x) \leqslant n$, l'inégalité $\varphi(q) \leqslant n-1$ va résulter des deux inégalités suivantes : $\varphi(x-r) = \varphi(x)$ et $\varphi(q) < \varphi(X_0 q)$ (ce qui est le cas lorsque φ est la fonction degré dans $K[X]$). On les déduit de deux lemmes.

Lemme. *Si $x \notin K$ et $a \in K$, alors $\varphi(x+a) = \varphi(x)$.*

Démonstration. C'est évident si $a = 0$. Sinon, a est inversible, $a + x$ est associé à $1 + a^{-1}x$ et x à $a^{-1}x$. On en déduit que

$$\varphi(a+x) = \varphi(1+a^{-1}x) \quad \text{et} \quad \varphi(a^{-1}x) = \varphi(x).$$

On peut donc se ramener à montrer que si $u \notin K$, alors $\varphi(1+u) = \varphi(u)$. On remarque que $1+u$ n'est pas dans K, sinon u y serait (K est un corps et contient 1). On a donc $1+u \neq 0$ et

$$1 = (1+u) \times 1 - u = (1+u) \times 0 + 1.$$

Comme $\varphi(1+u) > \varphi(1)$, on a nécessairement, par unicité de la division, $\varphi(u) \geqslant \varphi(1+u)$. En remplaçant u par $-(1+u)$, qui lui aussi n'est pas dans K, on obtient de même $\varphi(-(1+u)) \geqslant \varphi(1-(1+u))$. On a donc $\varphi(1+u) = \varphi(-(1+u)) \geqslant \varphi(-u) = \varphi(u)$. On conclut que $\varphi(1+u) = \varphi(u)$. Le lemme est prouvé. ◇

Lemme. *Si $x \neq 0$, $\varphi(xX_0) > \varphi(x)$.*

Démonstration. Raisonnons par l'absurde et supposons $\varphi(xX_0) \leqslant \varphi(x)$. Comme x divise xX_0, on a $\varphi(xX_0) \geqslant \varphi(x)$ et donc $\varphi(xX_0) = \varphi(x)$. Divisons x par $X_0 x$: il existe q et r dans A tels que

$$x = xX_0 q + r \quad \text{et} \quad r = 0 \text{ ou } \varphi(r) < \varphi(xX_0) = \varphi(x).$$

On remarque que x divise r, ce qui implique, si $r \neq 0$, que $\varphi(x) \leqslant \varphi(r)$. Cette inégalité n'est pas vérifiée. On a donc $r = 0$. On obtient alors $x = xX_0q$ et, par intégrité, $1 = X_0q$, ce qui montre que X_0 est inversible, donc dans K. C'est faux, par hypothèse. $\diamondsuit$

Résumons : $\varphi(q) < \varphi(X_0q) = \varphi(x)$ et donc $\varphi(q) \leqslant n-1$. D'après l'hypothèse de récurrence, $q \in K[X_0]$ et finalement $x \in K[X_0]$. $\lhd$

Conclusion. L'anneau $A = K[X_0]$ est isomorphe à l'anneau des polynômes $K[X]$.

On retiendra des exercices précédents la chaîne d'implications : pour un anneau commutatif et intègre A,

$$\text{A } \textit{euclidien} \Longrightarrow \text{A } \textit{principal} \Longrightarrow \text{A } \textit{factoriel}.$$

Nous allons, dans les deux exercices qui suivent, nous intéresser aux entiers de Gauss, exemple historiquement important, qui donne le coup d'envoi de la théorie algébrique des nombres. Le premier démontre que $\mathbb{Z}[i]$ est euclidien (donc principal et factoriel), ce qui conduit à une arithmétique proche de celle de $\mathbb{Z}$. Le lecteur aura intérêt, avant de l'aborder, à affermir ses connaissances sur les anneaux factoriels en traitant l'exercice 3.10.

3.12. Anneau des entiers de Gauss (1)

On considère l'anneau $\mathbb{Z}[i] = \{u + iv \in \mathbb{C},\ (u,v) \in \mathbb{Z}^2\}$ et l'application $\varphi : a \in \mathbb{Z}[i] \longmapsto a\overline{a} \in \mathbb{N}$.

1. Déterminer le groupe multiplicatif des éléments inversibles de $\mathbb{Z}[i]$.

2. Montrer que $\mathbb{Z}[i]$ est euclidien pour φ, c'est-à-dire que pour tout $(a,b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$, il existe $(q,r) \in \mathbb{Z}[i]^2$ tel que $a = bq + r$ avec $\varphi(r) < \varphi(b)$.

3. En déduire que $\mathbb{Z}[i]$ est factoriel.

4. Montrer que si $\varphi(a)$ est premier, alors a est irréductible dans $\mathbb{Z}[i]$.

5. Soit p un nombre premier. Montrer l'équivalence entre les propriétés suivantes :

(*i*) p est irréductible dans $\mathbb{Z}[i]$;

(*ii*) $p \equiv 3 \pmod 4$;

(*iii*) il n'existe pas $a \in \mathbb{Z}[i]$ tel que $p = \varphi(a)$.

On admettra que -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p n'est pas congru à 3 modulo 4.

6. En déduire tous les irréductibles de $\mathbb{Z}[i]$.

(École normale supérieure)

I · **Solution.**

1. Soit a un élément inversible de $\mathbb{Z}[i]$. Il existe b dans $\mathbb{Z}[i]$ tel que $ab = 1$. Comme φ est multiplicative, il vient $\varphi(a)\varphi(b) = 1$. L'entier naturel $\varphi(a)$ est inversible dans $\mathbb{Z}$ et donc égal à 1. Réciproquement si $\varphi(a) = 1$, alors $a\overline{a} = 1$ et $\overline{a}$, qui appartient à $\mathbb{Z}[i]$, est l'inverse de a.

Un élément $a \in \mathbb{Z}[i]$ est donc inversible si et seulement si $\varphi(a) = 1$. En posant $a = u + iv$, avec $(u, v) \in \mathbb{Z}^2$, on obtient $u^2 + v^2 = 1$. Les éléments inversibles de $\mathbb{Z}[i]$ sont donc $1, -1, i$ et $-i$: il s'agit du groupe des racines quatrième de l'unité.

2. Soit $(a, b) \in \mathbb{Z}[i] \times \mathbb{Z}[i]^*$. Considérons le nombre complexe $\dfrac{a}{b}$ qui s'écrit $\dfrac{a}{b} = x + iy$, avec $(x, y) \in \mathbb{R}^2$, u (resp. v) l'entier le plus proche de x (resp. y) et posons $q = u + iv$.

On a alors

$$\left|\frac{a}{b} - q\right|^2 = (u - x)^2 + (v - y)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

On en déduit $|a - bq|^2 < |b|^2$. Posons $r = a - bq$; a, b, q appartenant à $\mathbb{Z}[i]$, r appartient également à $\mathbb{Z}[i]$ et on a $|r|^2 < |b|^2$, c'est-à-dire $\varphi(r) < \varphi(b)$.

Nous avons déterminé $(q, r) \in \mathbb{Z}[i]^2$ tel que $a = bq + r$ et $\varphi(r) < \varphi(b)$.

Conclusion. L'anneau $\mathbb{Z}[i]$ est un anneau euclidien.

3. D'après l'exercice 3.11, $\mathbb{Z}[i]$ est un anneau principal et d'après l'exercice 3.10, il est alors factoriel.

4. Soit $a \in \mathbb{Z}[i]$ tel que $\varphi(a)$ soit premier. Supposons que a s'écrive $a = bc$, avec b et c dans $\mathbb{Z}[i]$. On a alors $\varphi(a) = \varphi(b)\varphi(c)$. L'entier $\varphi(a)$ étant premier, on en déduit que $\varphi(b) = 1$ ou $\varphi(c) = 1$, c'est-à-dire que b ou c est inversible. Donc a est irréductible.

5. Supposons (i) et montrons (ii) en raisonnant par l'absurde. Si p n'est pas congru à 3 modulo 4, alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et il existe $x \in \mathbb{Z}$ tel que $-1 \equiv x^2 \pmod{p}$. On obtient alors que p divise $x^2 + 1 = (x + i)(x - i)$ dans $\mathbb{Z}$ et donc dans $\mathbb{Z}[i]$. Puisque p est irréductible, il divise $x + i$ ou $x - i$. Mais ceci est impossible, car ni $\dfrac{x}{p} + \dfrac{i}{p}$, ni $\dfrac{x}{p} - \dfrac{i}{p}$ ne sont des éléments de $\mathbb{Z}[i]$.

Supposons (ii) et montrons (iii), toujours par l'absurde. Si $p = \varphi(a)$, alors $p = u^2 + v^2$, où u et v sont deux entiers tels que $a = u + iv$. Mais un carré étant toujours congru à 0 ou 1 (mod 4), p ne peut être congru qu'à $0, 1$ ou 2 (mod 4), ce qui contredit (ii).

Supposons (iii) et démontrons (i). Soit a et b dans $\mathbb{Z}[i]$ tels que $p = ab$. On a $p^2 = \varphi(p) = \varphi(a)\varphi(b)$. Si ni a, ni b ne sont inversibles, on a $\varphi(a)$ et $\varphi(b)$ différents de 1. On obtient, puisque p est premier, $\varphi(a) = \varphi(b) = p$, ce qui contredit l'hypothèse. On conclut que a ou b est inversible : p est irréductible.

6. D'après les questions précédentes, les entiers premiers congrus à 3 modulo 4 et les éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a)$ soit premier sont irréductibles. Montrons que ce sont les seuls, à multiplication par un inversible près.

Soit a un élément irréductible de $\mathbb{Z}[i]$. On remarque que a divise $\varphi(a) > 1$. L'entier $\varphi(a)$ est un produit d'entiers premiers. Puisque a est irréductible, il divise (dans $\mathbb{Z}[i]$) un de ces entiers premiers, p. Il existe $b \in \mathbb{Z}[i]$ tel que $p = ab$ et donc $p^2 = \varphi(a)\varphi(b)$. Si b est inversible, a est associé à p et nécessairement p est congru à 3 modulo 4, d'après la question 5. Sinon, on a, puisque $\varphi(a) > 1$, $\varphi(a) = p$ et a est un irréductible du type étudié dans la question 4. $\lhd$

On remarque que la condition (iii) de la question 5 de l'exercice équivaut à dire que p n'est pas somme de deux carrés. On obtient donc qu'un entier premier est somme de deux carrés si et seulement s'il n'est pas congru à 3 modulo 4. On trouvera dans le chapitre 4 (arithmétique) deux autres preuves de ce résultat (cf. 4.34 et 4.35).

L'exercice 3.13, qui étudie certaines sommes d'entiers de Gauss, suppose connus les résultats de l'exercice 3.12.

3.13. Anneau des entiers de Gauss (2)

Soit $k \in \mathbb{N}^*$ et $n \in \mathbb{N}$. On pose $s_n = \dfrac{1}{4} \displaystyle\sum_{\substack{a \in \mathbb{Z}[i] \\ a\overline{a}=n}} a^k$.

1. Montrer que $s_n \in \mathbb{Z}$ et que, si k n'est pas un multiple de 4, on a $s_n = 0$.

2. Calculer s_5, s_{13} et s_{65} pour $k = 4$. Que constate t-on ?

3. Généraliser le résultat de la question précédente.

(**École normale supérieure**)

$\rhd$ **Solution.**

1. Si $n = 0$, alors $s_n = 0$ pour tout k. Dans la suite, nous supposerons donc $n \neq 0$.

Comme dans l'exercice précédent, on note, pour $a \in \mathbb{Z}[i]$, $\varphi(a) = a\overline{a}$. On rappelle que deux éléments a et b de $\mathbb{Z}[i]$ sont associés s'il existe c, élément inversible de $\mathbb{Z}[i]$, tel que $b = ac$ et que la relation «être associés» est une relation d'équivalence. Il a été démontré dans l'exercice précédent, que les inversibles de $\mathbb{Z}[i]$ sont les éléments a tels que $\varphi(a) = 1$, c'est-à-dire $-1, 1, i, -i$. Si a est non nul, la classe de a contient donc quatre éléments distincts $a, -a, ia, -ia$.

On remarque que si a et b sont associés, alors $\varphi(a) = \varphi(b)$. L'ensemble des éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a) = n$ se compose donc

d'une réunion de classes d'équivalence (pour la relation «être associés») $\omega_1, \omega_2, \ldots, \omega_\ell$. On choisit, pour tout $j \in [\![1, \ell]\!]$, $a_j \in \omega_j$. On obtient alors $\sum_{a \in \omega_j} a^k = a_j^k(1^k + (-1)^k + i^k + (-i)^k)$. La valeur de la somme $u_k = 1^k + (-1)^k + i^k + (-i)^k$ ne dépend que du reste de k modulo 4. On trouve $u_0 = 4$, $u_1 = u_2 = u_3 = 0$. On en déduit que si k n'est pas divisible par 4, on a, pour tout $j \in [\![1, \ell]\!]$, $\sum_{a \in \omega_j} a^k = 0$ et donc $s_n = 0$.

Si k est divisible par 4, alors $\sum_{a \in \omega_j} a^k = 4a_j^k$, $s_n = \sum_{j=1}^{\ell} a_j^k$ et donc $s_n \in \mathbb{Z}[i]$. Par ailleurs, de l'égalité $\varphi(\overline{a}) = \varphi(a)$ pour tout $a \in \mathbb{Z}[i]$, on déduit que

$$\overline{s_n} = \frac{1}{4} \sum_{\varphi(a)=n} \overline{a}^k = \frac{1}{4} \sum_{\varphi(\overline{a})=n} \overline{a}^k = s_n.$$

Ceci montre que la partie imaginaire de s_n est nulle et donc que $s_n \in \mathbb{Z}$.

2. Pour calculer s_n, on détermine les solutions dans $\mathbb{Z}$ de $u^2 + v^2 = n$. Pour les valeurs données de n, c'est aisé : on considère les entiers u tels que $u^2 \leqslant n$ et on cherche ceux pour lesquels $n - u^2$ est un carré parfait.

Pour $n = 5$, on trouve $\{|u|, |v|\} = \{1, 2\}$. Les éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a) = 5$ sont $\pm 1 \pm 2i$ et $\pm 2 \pm i$. Il y en a huit qui se répartissent en deux classes : $2 + i$ et ses associés, $2 - i$ et les siens. La question précédente montre que

$$s_5 = (2+i)^4 + (2-i)^4 = (3+4i)^2 + (3-4i)^2 = -14.$$

De même, pour $n = 13$, on trouve $\{|u|, |v|\} = \{3, 2\}$. Les éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a) = 5$ sont $\pm 3 \pm 2i$ et $\pm 2 \pm 3i$. On en déduit

$$s_{13} = (3+2i)^4 + (3-2i)^4 = (5+12i)^2 + (5-12i)^2 = -238.$$

Dans le cas $n = 65$, on trouve $\{|u|, |v|\} = \{1, 8\}$ ou $\{4, 7\}$. Il y a seize éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a) = 65$. Ils forment quatre classes, celles de $8 + i$, $8 - i$, $7 + 4i$ et $7 - 4i$. On obtient donc

$$\begin{aligned} s_{65} &= (8+i)^4 + (8-i)^4 + (7+4i)^4 + (7-4i)^4 \\ &= (63+16i)^2 + (63-16i)^2 + (33+56i)^2 + (33-56i)^2 \\ &= 2(63^2 - 16^2 + 33^2 - 56^2) = 3332. \end{aligned}$$

On remarque que $(-14)(-238) = 3332$, c'est-à-dire que

$$\boxed{s_5 s_{13} = s_{65}}.$$

Essayons d'expliquer ce résultat. D'après l'exercice précédent, $\mathbb{Z}[i]$ est un anneau factoriel et a est irréductible dès que $\varphi(a)$ est un entier premier.

Considérons $a \in \mathbb{Z}[i]$ tel que $\varphi(a) = 65$. On peut écrire

$$a\overline{a} = 65 = 13 \times 5 = 13(2+i)(2-i).$$

On en déduit que $2+i$ divise $a\overline{a}$ et donc, $2+i$ étant irréductible puisque 5 est premier, que $2+i$ divise a ou $\overline{a}$. Il existe donc $b \in \mathbb{Z}[i]$ tel que $a = (2+i)b$ ou $\overline{a} = (2+i)b$. Dans le second cas, on a $a = (2-i)\overline{b}$. Remarquons que

$$\varphi(b) = \frac{\varphi(a)}{\varphi(2+i)} = \frac{65}{5} = 13,$$

dans le premier cas et de même $\varphi(\overline{b}) = 13$, dans le second. Ainsi, nous avons démontré que tout $a \in \mathbb{Z}[i]$ tel que $\varphi(a) = 65$ s'écrit $a = bc$ avec $\varphi(b) = 13$ et $\varphi(c) = 5$. De plus, b et c sont irréductibles, car 5 et 13 sont premiers. Réciproquement, tout $a \in \mathbb{Z}[i]$ qui s'écrit $a = bc$ avec $\varphi(b) = 13$ et $\varphi(c) = 5$ vérifie $\varphi(a) = 65$. Une telle écriture de a en produits de facteurs irréductibles est unique, à multiplication par des inversibles près. On peut donc écrire a de quatre manières différentes sous la forme $a = bc$ avec $\varphi(b) = 13$ et $\varphi(c) = 5$. Si (b, c) est un couple solution, les autres sont $(-b, -c)$, $(ib, -ic)$ et $(-ib, ic)$.

De tout cela on déduit que, pour tout $k \in \mathbb{N}$,

$$s_5 s_{13} = \frac{1}{16} \sum_{\varphi(b)=5} b^k \sum_{\varphi(c)=13} c^k = \frac{1}{16} \sum_{\substack{\varphi(b)=5 \\ \varphi(c)=13}} (bc)^k = \frac{1}{16}\, 4 \sum_{\varphi(a)=65} a^k = s_{65}.$$

3. Montrons, plus généralement que, si m et n sont premiers entre eux, on a $s_{mn} = s_m s_n$. Il faut démontrer, comme précédemment, que si $a \in \mathbb{Z}[i]$ vérifie $\varphi(a) = mn$, alors il existe $(b, c) \in (\mathbb{Z}[i])^2$ tel que $a = bc$, $\varphi(b) = m$ et $\varphi(c) = n$ et que de plus, à a correspondent quatre telles décompositions $a = bc$, b pouvant être multiplié par un inversible quelconque. Le résultat s'obtient à partir de la décomposition de a en facteurs irréductibles.

D'après l'exercice précédent les irréductibles de $\mathbb{Z}[i]$ sont les entiers premiers congrus à 3 (mod 4) et les éléments a tels que $\varphi(a)$ soit un entier premier (non congru à 3 (mod 4)). La décomposition de a en facteurs irréductibles peut s'écrire

$$a = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{j=1}^{s} a_j^{\beta_j},$$

où ε est inversible, r et s sont des entiers naturels, $p_1, \ldots, p_r$ des entiers premiers congrus à 3 (mod 4), $a_1, \ldots, a_s$ sont des éléments de $\mathbb{Z}[i]$ tels que $\varphi(a_1), \ldots, \varphi(a_s)$ soient des entiers premiers, non congrus à 3 (mod 4), $\alpha_1, \ldots, \alpha_r$, $\beta_1, \ldots, \beta_s$ des entiers naturels non nuls. On en déduit que

$$mn = \varphi(a) = \prod_{i=1}^{r} p_i^{2\alpha_i} \prod_{j=1}^{s} \varphi(a_j)^{\beta_j}.$$

On observe que cette écriture est la décomposition de mn en facteurs premiers. Les entiers m et n étant premiers entre eux, ils n'ont aucun diviseur premier commun. Quitte à renuméroter les irréductibles qui divisent a, on peut supposer qu'il existe des entiers naturels r' et s' tels que $r' \leqslant r$, $s' \leqslant s$ et

$$m = \prod_{i=1}^{r'} p_i^{2\alpha_i} \prod_{j=1}^{s'} \varphi(a_j)^{\beta_j} \quad \text{et} \quad n = \prod_{i=r'+1}^{r} p_i^{2\alpha_i} \prod_{j=s'+1}^{s} \varphi(a_j)^{\beta_j}.$$

Si b et c sont deux éléments de $\mathbb{Z}[i]$ tels que $a = bc$, $m = \varphi(b)$ et $n = \varphi(c)$, il résulte du calcul de $\varphi(a)$ à partir de a et de l'expression de m et n, que les irréductibles qui divisent b sont $p_1, \ldots, p_{r'}$ et $a_1, \ldots, a_{s'}$ et que ceux qui divisent c sont $p_{r'+1}, \ldots, p_r$ et $a_{s'+1}, \ldots, a_s$. Puisque $a = bc$, il existe ε' inversible tel que

$$b = \varepsilon' \prod_{i=1}^{r'} p_i^{\alpha_i} \prod_{j=1}^{s'} a_j^{\beta_j} \quad \text{et} \quad c = \varepsilon(\varepsilon')^{-1} \prod_{i=r'+1}^{r} p_i^{\alpha_i} \prod_{j=s'+1}^{s} a_j^{\beta_j}.$$

Il est clair que b et c ainsi définis ont toutes les propriétés voulues.

On obtient donc, pour tout a tel que $\varphi(a) = mn$, quatre décompositions sous la forme $a = bc$, avec $m = \varphi(b)$ et $n = \varphi(c)$, correspondant aux quatre valeurs de ε'. De la même manière que dans la question précédente, on conclut que $s_m s_n = s_{mn}$. $\lhd$

Une écriture d'un entier n sous la forme $n = \varphi(a)$ correspond (bijectivement) à une décomposition de n en somme de deux carrés $n = u^2 + v^2$, où u et v sont deux entiers tels que $a = u + iv$. Pour tout entier $n \geqslant 1$, notons $r(n)$ le nombre de couples $(u, v) \in \mathbb{Z}^2$ tels que $n = u^2 + v^2$, c'est-à-dire le nombre d'éléments a de $\mathbb{Z}[i]$ tels que $\varphi(a) = n$. La dernière question de l'exercice montre que si m et n sont premiers entre eux, on a $r(m)r(n) = 4r(mn)$. Si on pose $\delta(n) = \dfrac{r(n)}{4}$, on obtient $\delta(mn) = \delta(m)\delta(n)$: la fonction δ est donc multiplicative. Pour quelques remarques sur les fonctions arithmétiques multiplicatives, on se reportera aux exercices 4.28 à 4.33 du chapitre 4 (arithmétique).

L'exercice suivant étudie un anneau dont les éléments sont de la forme $\mathrm{P} + \varepsilon\mathrm{Q}$, où ε vérifie $\varepsilon^2 = \mathrm{X}^2 - 1$. On rapprochera cet anneau de l'anneau $\mathbb{Z}[i]$, obtenu de même à partir de $\mathbb{Z}$ en rajoutant un élément de carré -1 (cf. exercice 3.12). En particulier l'application N qu'on y définit joue le rôle de l'application φ de $\mathbb{Z}[i]$ dans la détermination des éléments inversibles.

3.14. Une extension quadratique de $\mathbb{C}[X]$

On considère le sous-ensemble A de $\mathcal{F}(]1,+\infty[,\mathbb{C})$ défini par

$$A = \left\{x \longmapsto P(x) + Q(x)\sqrt{x^2-1},\quad (P,Q) \in \mathbb{C}[X]^2\right\}$$

1. Montrer que A est un anneau. Vérifier que tout $z \in A$ s'écrit de manière unique sous la forme $z = P + \varepsilon Q$ avec P et Q dans $\mathbb{C}[X]$, où ε désigne l'application $x \longmapsto \sqrt{x^2-1}$.

2. Montrer que $z = P + \varepsilon Q$ est une unité de A si, et seulement si, $N(z) = P^2 - (X^2-1)Q^2 \in \mathbb{C}^*$.

3. Montrer qu'il existe $z_0 \in A$ tel que

$$U_0 = \{z \in A,\ N(z) = 1\} = \{\pm z_0^n,\ n \in \mathbb{Z}\}.$$

4. Expliciter les couples de polynômes $(P,Q) \in \mathbb{C}[X]^2$ qui vérifient $P^2 - (X^2-1)Q^2 = 1$.

(École polytechnique)

▷ **Solution.**

1. Il est clair que A contient l'application nulle ainsi que l'application constante égale à 1, et qu'il est stable pour la somme et l'opposé. Soit $(P_1,Q_1,P_2,Q_2) \in \mathbb{C}[X]^4$. On a

$$(P_1+\varepsilon Q_1)(P_2+\varepsilon Q_2) = P_1P_2 + \varepsilon^2 Q_1Q_2 + \varepsilon(P_1Q_2 + P_2Q_1) \in A,$$

car ε^2 est la fonction polynôme $x \longmapsto x^2-1$. Il en résulte que A est un sous-anneau de l'anneau $\mathcal{F}(]1,+\infty[,\mathbb{C})$.

L'application $\psi : \mathbb{C}[X]^2 \to A$ qui au couple (P,Q) associe $z = P + \varepsilon Q$ est clairement un morphisme de groupes additifs. Il est surjectif par définition de A. Enfin, il est injectif car si $P \in \operatorname{Ker}\psi$ *i.e.* $P + \varepsilon Q = 0$, on obtient $P^2 = (X^2-1)Q^2$, ce qui impose $P = Q = 0$ (car sinon la multiplicité de la racine 1 est paire dans le membre de gauche et impaire dans celui de droite). Il en résulte que tout $z \in A$ s'écrit de manière unique sous la forme $z = P + \varepsilon Q$. En particulier on peut identifier $\mathbb{C}[X]$ à un sous-anneau de A, ce qu'on fera dans la suite.

2. Si $z = P + \varepsilon Q$ est un élément de A, on pose $\overline{z} = P - \varepsilon Q$ et on parle du conjugué de z. Il est clair que l'application $z \longmapsto \overline{z}$ est un automorphisme d'anneau de A.

On a $N(z) = z\overline{z} = P^2 - (X^2-1)Q^2 \in \mathbb{C}[X]$.

• Soit $z \in A$ inversible et $z' \in A$ tel que $zz' = 1$. On a alors

$$1 = N(1) = N(zz') = zz'\overline{zz'} = z\overline{z}z'\overline{z'} = N(z)N(z'),$$

d'où il résulte que $N(z)$ est inversible dans $\mathbb{C}[X]$ et appartient donc à $\mathbb{C}^*$.

• Réciproquement, si $N(z) = \lambda \in \mathbb{C}^*$, alors $\frac{1}{\lambda}\overline{z} \in A$ est l'inverse de z dans A.

3. Notons U le groupe des unités de A. Comme N est un morphisme de groupes de U dans $\mathbb{C}^*$, $U_0 = \operatorname{Ker} N$ est un sous-groupe de U.

Posons $z_0 = X + \varepsilon$. On a $N(z_0) = X^2 - (X^2 - 1) = 1$, donc z_0 est dans U_0. On va montrer que z_0 répond à la question. Il est déjà clair que $\{\pm z_0^n,\ n \in \mathbb{Z}\} \subset U_0$. Soit $z = P + \varepsilon Q \in U_0$. On considère un entier $m \in \mathbb{Z}$ tel que $z' = z_0^{-m} z$ s'écrive $z' = A + \varepsilon B$, avec un polynôme B de degré minimal. Alors z' appartient à U_0, car U_0 est un groupe multiplicatif. On va montrer que $B = 0$. Il s'ensuivra que $A = \pm 1$, puisque $z' \in U_0$, soit encore $z = \pm z_0^m$.

Supposons par l'absurde que $B \neq 0$. On a $A^2 - (X^2 - 1)B^2 = 1$, puisque $z' \in U_0$, ce qui peut s'écrire $(A - XB)(A + XB) = 1 - B^2$. On doit nécessairement avoir $\deg A = 1 + \deg B$. Il en résulte que l'un des deux polynômes $A - XB$ ou $A + XB$ a un degré strictement inférieur à $\deg B$ (car sinon $\deg(A - XB) = \deg(A + XB) = \deg B$, d'où l'on déduit $\deg A = \deg(2A) \leqslant \deg B$, ce qui est faux). Or on a

$$\begin{aligned} z_0 z' &= (X + \varepsilon)(A + \varepsilon B) = XA + (X^2 - 1)B + \varepsilon(XB + A) \\ z_0^{-1} z' &= (X - \varepsilon)(A + \varepsilon B) = XA - (X^2 - 1)B + \varepsilon(XB - A) \end{aligned}$$

et l'une des deux égalités est contredit la minimalité du degré de B.

4. Posons pour $n \in \mathbb{N}$, $z_0^n = (X + \varepsilon)^n = P_n + \varepsilon Q_n$. On obtient alors $z_0^{-n} = \overline{z_0}^n = P_n - \varepsilon Q_n$. D'après la question précédente, les solutions de l'équation $P^2 - (X^2 - 1)Q^2 = 1$ sont donc les couples $(\pm P_n, \pm Q_n)$, où n décrit $\mathbb{N}$. À l'aide de la formule du binôme on obtient

$$\begin{aligned} P_n &= \sum_{0 \leqslant 2k \leqslant n} C_n^{2k} (X^2 - 1)^k X^{n-2k} \\ Q_n &= \sum_{0 \leqslant 2k+1 \leqslant n} C_n^{2k+1} (X^2 - 1)^k X^{n-2k-1}. \end{aligned}$$

On peut reconnaître ici les polynômes de Tchebychev de première et de seconde espèce T_n et U_{n-1} qui sont définis par $\cos n\theta = T_n(\cos\theta)$ et $\sin n\theta = \sin\theta U_{n-1}(\cos\theta)$. Cela s'explique très bien. Soit f l'application de A dans l'anneau des polynômes trigonométriques complexes qui a $z = P + \varepsilon Q$ associe, $P(\cos\theta) + i\sin\theta Q(\cos\theta)$. On vérifie facilement que f est un morphisme d'anneaux et qu'il est injectif. On en déduit que $f(z_0^n) = P_n(\cos\theta) + i\sin\theta Q_n(\cos\theta)$ et, grâce à la formule de Moivre,

$$\begin{aligned} f(z_0^n) = f(z_0)^n &= (\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta \\ &= T_n(\cos\theta) + i\sin\theta U_{n-1}(\cos\theta). \end{aligned}$$

On obtient donc donc $P_n = T_n$ et $Q_n = U_{n-1}$. $\lhd$

Une autre démonstration, élémentaire, de la dernière question est donnée dans l'exercice 5.7.

Les trois exercices suivants étudient des exemples assez simples de corps. Le premier fait la transition avec les anneaux.

3.15. Anneau sans idéal non premier

Soit A un anneau commutatif dont tout idéal I est premier c'est-à-dire vérifie, pour tout $(x, y) \in A^2$,

$$xy \in I \Longrightarrow x \in I \text{ ou } y \in I.$$

Montrer que A est un corps.

(École normale supérieure)

▷ **Solution.**

Dire que l'idéal nul est premier signifie que A est intègre. Soit x dans A, non nul. On souhaite prouver que x est inversible. Comme l'idéal principal (x^2) est premier, on a $x \in (x^2)$. Il existe donc $a \in A$ tel que $x = ax^2$. Comme A est intègre et x non nul, on a $ax = 1$ et x est inversible. On conclut que A est un corps. ◁

Les corps étudiés maintenant sont des corps de nombres algébriques, dont on peut donner la définition suivante : soit θ un élément de $\mathbb{C}$, racine d'un polynôme non nul P de $\mathbb{Q}[X]$ qui est irréductible sur $\mathbb{Q}$. Alors l'ensemble des nombres complexes de la forme $\Phi(\theta)$, où $\Phi \in \mathbb{Q}[X]$, est un corps noté $\mathbb{Q}(\theta)$, isomorphe au quotient $\mathbb{Q}[X]/P\mathbb{Q}[X]$. De plus $\mathbb{Q}(\theta)$ est un espace vectoriel de dimension $n = \deg P$ sur $\mathbb{Q}$. Pour un exemple plus complexe, le lecteur se reportera à l'exercice 5.17 qui étudie $\mathbb{Q}(e^{i\frac{2\pi}{p}})$, où p est premier.

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

Soit $E = \{a + b\sqrt{2} \in \mathbb{C}^2, (a, b) \in \mathbb{Q}^2\}$. Montrer que E est un sous-corps de $\mathbb{C}$ et en déterminer tous les automorphismes.

(École polytechnique)

▷ **Solution.**

• $\mathbb{C}$ est une $\mathbb{Q}$-algèbre. L'application

$$\varphi : \begin{array}{ccc} \mathbb{Q}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & P(\sqrt{2}) \end{array}$$

est un morphisme d'algèbres. Son image est donc une sous-algèbre de $\mathbb{C}$, qui contient clairement E.

Pour montrer l'inclusion inverse, on observe que, si $n \geqslant 0$, on a $\varphi(X^n) = (\sqrt{2})^n = 2^p(\sqrt{2})^r \in E$, où $n = 2p + r$, avec $r = 0$ ou 1 et $p \in \mathbb{N}$. On en déduit que $\operatorname{Im}\varphi = E$. Par conséquent, E est un sous-anneau de $\mathbb{C}$.

• Soit $x \in E$ non nul, qui s'écrit $x = a + b\sqrt{2}$ avec $(a, b) \in \mathbb{Q}^2$. On a alors $a - b\sqrt{2} \neq 0$ (car $\sqrt{2} \notin \mathbb{Q}$) et donc

$$x^{-1} = \frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2} \in E.$$

On en déduit que E est un sous-corps de $\mathbb{C}$.

• Si f un automorphisme de E, alors f laisse invariants tous les éléments de $\mathbb{Q}$. En effet, on a, pour $x \in \mathbb{Q}$ et $n \in \mathbb{N}$,

$$f(nx) = f(x + \cdots + x) = f(x) + \cdots + f(x) = nf(x) = nf(x),$$

et donc $f(n) = n$, car $f(1) = 1$. On a ensuite $f(-n) + f(n) = f(0) = 0$ et donc $f(-n) = -f(n) = -n$. Enfin si $q \in \mathbb{N}^*$ et $p \in \mathbb{Z}$, on obtient

$$qf\left(\frac{p}{q}\right) = f\left(q\frac{p}{q}\right) = f(p) = p \quad \text{et} \quad f\left(\frac{p}{q}\right) = \frac{p}{q}.$$

On détermine ensuite $f(\sqrt{2})$. De $f(\sqrt{2})^2 = f(\sqrt{2}^2) = f(2) = 2$ résulte $f(\sqrt{2}) = \varepsilon\sqrt{2}$ avec $\varepsilon = \pm 1$. On a donc, pour tout $(a, b) \in \mathbb{Q}^2$,

$$f(a + b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a + \varepsilon b\sqrt{2}.$$

Réciproquement, les deux applications ainsi définies (pour $\varepsilon = -1$ et 1) sont des automorphismes de corps de E. Il n'existe qu'un seul automorphisme de E qui ne soit pas l'identité. $\lhd$

L'exercice suivant est l'occasion de découvrir les propriétés fondamentales de la théorie algébrique des corps et notamment la formule de multiplicativité des degrés.

3.17. Nombres algébriques

On considère un corps commutatif M et $K \subset L$ deux sous-corps de M.

1. Démontrer l'équivalence des deux conditions suivantes :

(i) M est un K-espace vectoriel de dimension finie m ;

(ii) M est un L-espace vectoriel de dimension finie n et L un K-espace vectoriel de dimension finie p.

Vérifier que dans ces conditions $m = np$.

2. On suppose que $a \in \mathrm{M}$ est *algébrique sur* K : il existe P non nul dans $\mathbb{K}[\mathrm{X}]$ tel que $\mathrm{P}(a) = 0$. Démontrer l'existence d'un unique polynôme unitaire μ de $\mathrm{K}[\mathrm{X}]$ tel que, pour tout polynôme P de $\mathrm{K}[\mathrm{X}]$,

$$\mathrm{P}(a) = 0 \iff \mu | \mathrm{P}.$$

Vérifier que μ est irréductible (μ est appelé le *polynôme minimal de a sur* K) et que l'ensemble $\mathrm{K}(a) = \{\mathrm{Q}(a),\ \mathrm{Q} \in \mathrm{K}[\mathrm{X}]\}$ est à la fois un K-espace vectoriel de dimension $\deg \mu$ et un sous-corps de M.

3. On dit que $a \in \mathbb{C}$ est *algébrique* si a est algébrique sur le corps $\mathbb{Q}$. Démontrer que $a = \sqrt[2]{2} + \sqrt[3]{2}$ est algébrique et déterminer son polynôme minimal.

(École Polytechnique)

▷ **Solution.**

1. Supposons (ii). On se donne $(e_1, \ldots, e_p)$ une base du K-espace vectoriel L et $(f_1, \ldots, f_n)$ une base du L-espace vectoriel M. Montrons que la famille $(e_j f_i)_{(i,j) \in [\![1,n]\!] \times [\![1,p]\!]}$ est une base du K-espace vectoriel M.

Soit $x \in \mathrm{M}$. On écrit $x = \lambda_1 f_1 + \cdots + \lambda_n f_n$ avec $\lambda_i \in \mathrm{L}$. Chaque λ_i s'écrit $\lambda_i = \sum\limits_{j=1}^{p} \mu_{i,j} e_j$ avec $\mu_{i,j} \in \mathrm{K}$. Par associativité, on obtient

$$x = \sum_{(i,j) \in [\![1,n]\!] \times [\![1,p[\![} \mu_{i,j} e_j f_i,$$

ce qui prouve que la famille $(e_j f_i)_{(i,j) \in [\![1,n]\!] \times [\![1,p]\!]}$ est génératrice du K-espace vectoriel M.

Vérifions qu'elle est libre : soit $\mu_{i,j} \in \mathrm{K}$ pour $(i,j) \in [\![1,n]\!] \times [\![1,p]\!]$ tels que

$$0 = \sum_{(i,j) \in [\![1,n]\!] \times [\![1,p]\!]} \mu_{i,j} e_j f_i.$$

Par associativité, on peut écrire

$$0 = \sum_{i=1}^{n} \underbrace{\left(\sum_{j=1}^{p} \mu_{i,j} e_j \right)}_{\in \mathrm{L}} f_i$$

ce qui impose que pour tout i, $\sum\limits_{j=1}^{p} \mu_{i,j} e_j = 0$ puisque $(f_1, \ldots, f_n)$ est libre dans le L-espace M. Comme $(e_1, \ldots, e_p)$ est libre dans le K-espace L, il vient que tous les $\mu_{i,j}$ sont nuls. On conclut que la famille $(e_j f_i)_{(i,j) \in [\![1,n[\![\times [\![1,p[\![}$ est une base du K-espace vectoriel M et que $m = np$.

Supposons (i). Comme L est un sous-espace du K-espace vectoriel M, L est de dimension finie sur K. D'autre part, si $(\varepsilon_1, \ldots, \varepsilon_m)$ constitue une base du K-espace M, c'est clairement un système générateur de M en tant que L-espace vectoriel. Donc M est un L-espace vectoriel de dimension finie.

On dit dans ces conditions que L *est une extension de* K *et* M *est une extension de* L. *La dimension de* L *comme* K*-espace vectoriel est notée* $[\mathrm{L} : \mathrm{K}]$ *: c'est le degré de l'extension* L *sur le corps* K. *Nous venons de démontrer que*

$$[\mathrm{K} : \mathrm{M}] = [\mathrm{K} : \mathrm{L}][\mathrm{L} : \mathrm{M}].$$

Cette identité est la relation de multiplicativité des degrés.

2. Le corps M est une K-algèbre. Considérons le morphisme de K-algèbres

$$\Phi : \begin{array}{ccc} \mathrm{K}[\mathrm{X}] & \longrightarrow & \mathrm{M} \\ \mathrm{P} & \longmapsto & \mathrm{P}(a) \end{array}.$$

L'ensemble $\mathrm{K}(a)$, qui est l'image de Φ, est une sous-algèbre de M. Le noyau $\operatorname{Ker}\Phi = \{\mathrm{P} \in \mathbb{Q}[\mathrm{X}],\ \mathrm{P}(a) = 0\}$ forme un idéal de $\mathrm{K}[\mathrm{X}]$. Par hypothèse, a est algébrique donc $\mathrm{I} \neq \{0\}$. Dans ces conditions, comme I est un idéal principal, on sait qu'il existe un unique polynôme μ unitaire de degré supérieur ou égal à 1 dans $\mathrm{K}[\mathrm{X}]$ tel que $\mathrm{I} = \mu\mathrm{K}[\mathrm{X}]$. On a l'équivalence

$$\forall \mathrm{P} \in \mathrm{K}[\mathrm{X}],\ \ \mu|\mathrm{P} \iff \mathrm{P}(a) = 0.$$

Si le polynôme μ' unitaire de $\mathrm{K}[\mathrm{X}]$ vérifie la même équivalence, alors $\mu'|\mu$ et $\mu|\mu'$ donc $\mu = \mu'$: μ est unique.

Montrons que le polynôme μ est irréductible. Si $\mu = \mathrm{AB}$ avec A et B dans $\mathrm{K}[\mathrm{X}]$, on a

$$0 = \mu(a) = \mathrm{A}(a)\mathrm{B}(a)$$

et donc $\mathrm{A}(a) = 0$ ou $\mathrm{B}(a) = 0$, ce qui implique $\mu|\mathrm{A}$ ou $\mu|\mathrm{B}$ et donc A ou B constant : le polynôme μ est irréductible. Remarquons que si P est irréductible unitaire avec $\mathrm{P}(a) = 0$, alors $\mathrm{P} = \mu$ puisque $\mu|\mathrm{P}$.

Montrons ensuite que $\mathrm{K}(a)$ est de dimension $r = \deg\mu$ comme K-espace vectoriel. Pour cela, vérifions que $(1, a, \ldots, a^{r-1})$ est une base de $\mathrm{K}(a)$. Le fait que μ soit un polynôme non nul de degré minimal annulant a garantit la liberté de la famille $(1, a, \ldots, a^{r-1})$. D'autre part, si $x \in \mathrm{K}(a)$, il s'écrit $x = \mathrm{A}(a)$ avec $\mathrm{A} \in \mathrm{K}[\mathrm{X}]$ et en notant R le reste de la division euclidienne de A par μ, on obtient $x = \mathrm{R}(a) \in \mathrm{Vect}(1, a, \ldots, a^{r-1})$.

Montrons enfin que $\mathrm{K}(a)$ est un sous-corps de M : c'est déjà un sous-anneau de M. Si x est non nul dans $\mathrm{K}(a)$, il s'écrit $x = \mathrm{A}(a)$ avec A non divisible par μ. Dans ces conditions, μ étant irréductible, il est premier avec A. D'après le théorème de Bezout, il existe U et V dans

K[X] tels que $1 = UA + V\mu$ et en évaluant en a, il vient $1 = U(a)x$ et donc $x^{-1} = U(a) \in K(a)$.

3. Il s'agit de trouver un polynôme non nul de $\mathbb{Q}[X]$ qui admet a comme racine. On a $(a - \sqrt{2})^3 = 2$ ce qui donne en développant

$$a^3 + 6a - 2 = \sqrt{2}(3a^2 + 2),$$

et en élevant au carré

$$a^6 - 6a^4 - 4a^3 + 12a^2 - 24a - 4 = 0.$$

Le polynôme $P = X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4 \in \mathbb{Q}[X]$ annule donc a, qui est un nombre algébrique.

Notons μ le polynôme minimal de a ; c'est un diviseur de P. On va prouver que $P = \mu$ en considérant la dimension du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}(a)$. En fait, la relation $a^3 + 6a - 2 = \sqrt{2}(3a^2 + 2)$ prouve que $\sqrt{2}$ est dans $\mathbb{Q}(a)$ puisque $3a^2 + 2 > 0$, $\sqrt{2} = (a^3 + 6a - 2)(3a^2 + 2)^{-1}$ et $\mathbb{Q}(a)$ est un corps. On a également $\sqrt[3]{2} = a - \sqrt{2} \in \mathbb{Q}(a)$. Comme $\mathbb{Q}(a)$ est une $\mathbb{Q}$-algèbre, pour tout $Q \in K[X]$, $Q(\sqrt{2})$ et $Q(\sqrt[3]{2})$ sont dans $Q(a)$. Il s'ensuit les inclusions

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(a) \quad \text{et} \quad \mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{Q}(a).$$

Or le polynôme minimal de $\sqrt{2}$ sur $\mathbb{Q}$ est $X^2 - 2$ et celui de $\sqrt[3]{2}$ est $X^3 - 2$ (ils sont bien irréductibles car de degré 2 ou 3 sans racine rationnelle). On en déduit que la dimension de $\mathbb{Q}(\sqrt{2})$ (resp. $\mathbb{Q}(\sqrt[3]{2})$) sur $\mathbb{Q}$ est 2 (resp. 3). D'après la première question et la multiplicativité des degrés des extensions, 2 et 3 divisent la dimension de $\mathbb{Q}(a)$ sur $\mathbb{Q}$. Donc, cette dimension est supérieure ou égale à 6. On a donc $\deg \mu \geqslant 6$. Comme μ divise P, ces polynômes unitaires sont égaux :

$$\boxed{\mu = X^6 - 6X^4 - 4X^3 + 12X^2 - 24X - 4}. \lhd$$

L'exercice suivant détermine toutes les valuations sur $\mathbb{Q}$.

3.18. Valuations sur $\mathbb{Q}$

On appelle valuation sur un anneau A toute application ν de A dans $\mathbb{R} \cup \{+\infty\}$ telle que, pour tout $(x, y) \in A^2$:

(*i*) $\nu(xy) = \nu(x) + \nu(y)$;
(*ii*) $\nu(x+y) \geqslant \min(\nu(x), \nu(y))$;
(*iii*) $\nu(x) = +\infty \Longleftrightarrow x = 0$.

1. Donner des exemples de valuation sur $\mathbb{Z}$, sur $\mathbb{Q}$.

2. Déterminer toutes les valuations sur $\mathbb{Q}$.

(**École normale supérieure**)

Solution.

1. Le cours fournit l'exemple des valuations p-adiques sur $\mathbb{Z}$: pour tout nombre premier p et tout entier non nul n, $\nu_p(n)$ est le plus grand entier naturel α tel que p^α divise n. On pose $\nu_p(0) = +\infty$ et il est aisé de vérifier les propriétés (*i*) et (*ii*). Ces valuations se prolongent à $\mathbb{Q}$: si x est un nombre rationnel non nul admettant comme représentant $\dfrac{a}{b}$, on pose $\nu_p(x) = \nu_p(a) - \nu_p(b)$; $\nu_p(x)$ ne dépend que de x et pas du représentant choisi et ν_p est encore une valuation sur $\mathbb{Q}$.

On va montrer dans la seconde question que les seules valuations sur $\mathbb{Q}$ sont la valuation triviale (*i.e.* nulle sur $\mathbb{Q}^*$) et les applications $\lambda\nu_p$, où λ est un réel strictement positif arbitraire et p un nombre premier.

2. Soit ν une valuation sur $\mathbb{Q}$, que l'on suppose non triviale.

• On a $\nu(1) = \nu(1^2) = \nu(1) + \nu(1)$, de sorte que $\nu(1) = 0$, mais aussi $2\nu(-1) = \nu(1) = 0$ et donc $\nu(-1) = 0$. On en déduit que, pour tout $x \in \mathbb{Q}^*$, $\nu(-x) = \nu(x) + \nu(-1) = \nu(x)$: ν est paire. On a par la propriété (*ii*), $\nu(2) \geqslant 0$ et par une récurrence évidente, $\nu(n) \geqslant 0$ pour tout entier $n \in \mathbb{N}$. Observons enfin que $\nu(x^n) = n\nu(x)$ pour tout $n \in \mathbb{N}$ et tout $x \in \mathbb{Q}$.

• L'ensemble $\mathrm{E} = \{n \in \mathbb{N}^*,\ \nu(n) > 0\}$ est non vide, car sinon ν serait triviale. Soit p le plus petit élément de E. Nécessairement, p est premier : en effet, si $p = ab$ avec $1 < a, b < p$, $\nu(p) = \nu(a) + \nu(b) = 0 + 0 = 0$, d'après la propriété (*i*), ce qui est absurde.

Soit q un nombre premier distinct de p. Comme $\mathrm{pgcd}(p, q) = 1$, on peut trouver $(u, v) \in \mathbb{Z}^2$ tel que $up + vq = 1$ par le théorème de Bezout. Par (*ii*) on obtient

$$0 \geqslant \min(\nu(up), \nu(vq)) = \min(\nu(u)+\nu(p), \nu(v)+\nu(q)) \geqslant \min(\nu(p), \nu(q)).$$

On ne peut donc pas avoir $\nu(q) > 0$ et donc $\nu(q) = 0$.

Il résulte alors du théorème de décomposition en facteurs premiers et du point (*i*) que, pour tout $n \in \mathbb{Z}^*$, $\nu(n) = \lambda\nu_p(n)$ où $\lambda = \nu(p) > 0$. Et toujours en vertu de (*i*) (qui implique que $\nu\left(\dfrac{x}{y}\right) = \nu(x) - \nu(y)$, pour tout $(x, y) \in \mathbb{Q} \times \mathbb{Q}^*$), cette égalité s'étend à $\mathbb{Q}$ tout entier. ◁

Les valuations sur $\mathbb{Q}$ résultent toutes d'un prolongement de celles de $\mathbb{Z}$. C'est vrai pour le corps des fractions d'un anneau intègre quelconque.

Chaque valuation de $\mathbb{Z}$ ou $\mathbb{Q}$, ν_p est associée à un nombre premier p. Il y a correspondance entre irréductibles et valuations prenant des valeurs positives ou nulles sur l'anneau A, *dans tous les anneaux* A *principaux et même dans des anneaux plus généraux, les anneaux de Dedekind (anneaux intègres dans lesquels tout idéal est produit d'idéaux premiers), à condition de remplacer les nombres premiers par les idéaux premiers.*

L'exercice suivant détermine les valeurs absolues non-archimédiennes sur $\mathbb{C}(X)$. Une valeur absolue sur un corps K *de caractéristique nulle est non-archimédienne si $\mathbb{N}^*$, considéré comme sous-anneau de* K, *est borné par* 1. *Elles s'opposent donc à la valeur absolue usuelle sur $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$, que nous savons être archimédienne.*

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

Soit K un corps commutatif de caractéristique nulle. On appelle valeur absolue de K toute application $|\ |$: K $\longrightarrow \mathbb{R}_+$ telle que, pour tout $(x, y) \in K^2$:

(*i*) $|x| = 0 \Longleftrightarrow x = 0$;

(*ii*) $|xy| = |x|\,|y|$;

(*iii*) $|x + y| \leqslant |x| + |y|$.

1. Soit $|\ |$ une valeur absolue de K telle que $|n| \leqslant 1$ pour $n \in \mathbb{N}^*$. Montrer que $|\ |$ vérifie l'inégalité *ultra-métrique* : pour tout couple $(x, y) \in K^2$,

$$|x + y| \leqslant \max(|x|, |y|).$$

2. Soit ν une valeur absolue de $\mathbb{C}(X)$ telle que $\nu(x) = 1$ pour tout $x \in \mathbb{C}^*$. Montrer que ν est de l'un des types suivants :

(*i*) $\nu(F) = 1$ pour toute fraction F non nulle ;

(*ii*) $\nu(F) = a^{\deg F}$, avec $a > 1$, pour F non nulle ;

(*iii*) $\nu(F) = a^{\mathrm{val}(F)}$, avec $0 < a < 1$, pour F non nulle, où l'on précisera ce qu'est val(F).

(École normale supérieure)

▷ **Solution.**

1. Ici, n désigne $n \cdot 1$, somme de n termes égaux à l'élément neutre pour la multiplication de K. Soit $(x, y) \in K^2$. Supposons, par exemple, que $|y| \leqslant |x|$. Pour tout entier naturel n, on a le développement du binôme $(x + y)^n = \sum_{k=0}^{n} C_n^k x^k y^{n-k}$. En prenant la valeur absolue, il vient

$$|x+y|^n \leqslant \sum_{k=0}^{n} |C_n^k x^k y^{n-k}| \leqslant \sum_{k=0}^{n} |C_n^k \cdot 1||x^k y^{n-k}| \leqslant \sum_{k=0}^{n} |x|^k |y|^{n-k}$$
$$\leqslant \sum_{k=0}^{n} |x|^n = (n+1)|x|^n.$$

Il en résulte que pour tout entier n, $|x+y| \leqslant (n+1)^{1/n}|x|$. Le résultat suit, en faisant tendre n vers l'infini.

Une valeur absolue telle que $\mathbb{N}^*$ *soit bornée par* 1 *est dite* non-archimédienne. *Elle vérifie l'inégalité ultra-métrique, qui est plus forte que l'inégalité triangulaire* (*iii*). *Observons que la réciproque est vraie :* (*i*) *et* (*ii*) *impliquent* $|1| = 1$, *puis* $|-1| = 1$ *; on en déduit que, pour toute valeur absolue qui vérifie l'inégalité ultra-métrique,* $\mathbb{Z}$ *est borné par* 1.

2. La valeur absolue ν est non-archimédienne et donc vérifie l'inégalité ultra-métrique.

• Observons pour commencer que, pour tout $(F, G) \in (\mathbb{C}(X))^2$ tel que $\nu(F) < \nu(G)$, on a $\nu(F+G) = \nu(G)$. En effet, on sait, d'après l'inégalité ultra-métrique, que $\nu(F+G) \leqslant \nu(G)$, mais comme $G = (F+G) + (-F)$, on a aussi $\nu(G) \leqslant \max(\nu(F), \nu(F+G)) = \nu(F+G)$, d'où l'égalité.

Posons $a = \nu(X)$.

• Supposons que $a > 1$. Tout polynôme non nul P de $\mathbb{C}[X]$ s'écrit $P = \sum_{k=0}^{n} a_k X^k$, avec $n = \deg(P)$. Comme pour tout k, $\nu(a_k X^k) = a^k$, on a

$$\nu(a_0) = 1 < \nu(a_1 X) < \nu(a_2 X^2) < \cdots < \nu(a_n X^n) = a^n.$$

Ceci permet d'affirmer que $\nu(P) = \nu(a_n X^n) = a^n = a^{\deg(P)}$. Grâce à la propriété (*ii*) de la valeur absolue, on conclut que, pour toute fraction rationnelle non nulle $F = \dfrac{P}{Q}$, on a

$$\nu(F) = \nu(P) - \nu(Q) = \frac{a^{\deg(P)}}{a^{\deg(G)}} = a^{\deg(F)}.$$

• Le cas $a < 1$ se traite de la même façon. On a $\nu(a_k X^k) = a^k$ si $a_k \neq 0$ et on trouve cette fois, $\nu(P) = a^{\mathrm{val}(P)}$ pour tout polynôme non nul P, où $\mathrm{val}(P)$ est la valuation en X de P, c'est-à-dire le plus petit indice k tel que $a_k \neq 0$. Si $F = \dfrac{P}{Q}$ est une fraction non nulle, la quantité $\mathrm{val}(P) - \mathrm{val}(Q)$ ne dépend que de F et pas du représentant choisi. Cette quantité étant notée $\mathrm{val}(F)$, on a $\nu(F) = a^{\mathrm{val}\,F}$.

• Supposons enfin $a = 1$. Dans ce cas, on a $\nu(X^k) = 1$, pour tout k et $\nu(P) \leqslant 1$, pour tout polynôme P. Distinguons deux cas.

⋆ Si $\nu(P) = 1$ pour tout polynôme non nul P, alors ν est triviale : elle vaut 1 sur toutes les fractions non nulles.

$\star$ Dans le cas contraire, notons Q un polynôme de degré minimal tel que $\nu(\mathrm{Q}) < 1$. Ce polynôme Q est irréductible car, si $\mathrm{Q} = \mathrm{AB}$ avec $\deg \mathrm{A} < \deg \mathrm{Q}$ et $\deg \mathrm{B} < \deg \mathrm{Q}$, on a $\nu(\mathrm{A}) = \nu(\mathrm{B}) = 1$ et donc $\nu(\mathrm{Q}) = 1$, ce qui est absurde. On peut bien entendu choisir Q unitaire, donc de la forme $\mathrm{Q} = \mathrm{X} - \alpha$, $\alpha \in \mathbb{C}$. Posons alors $b = \nu(\mathrm{X} - \alpha) < 1$. On fait le même travail que dans le cas $a < 1$, en remplaçant X par $\mathrm{X} - \alpha$ (tout polynôme P s'écrit $\mathrm{P} = \sum_{k=0}^{n} b_k(\mathrm{X} - \alpha)^k$, d'après la formule de Taylor). On a alors, pour tout polynôme non nul P, $\nu(\mathrm{P}) = b^{\nu_{\mathrm{X}-\alpha}(\mathrm{P})}$, où $\nu_{\mathrm{X}-\alpha}(\mathrm{P})$ est la valuation de P en $\mathrm{X} - \alpha$ c'est-à-dire, si l'on préfère, l'ordre de multiplicité de la racine α dans P. Ici aussi, cette valuation s'étend au corps des fractions $\mathbb{C}(\mathrm{X})$ et $\nu(\mathrm{F}) = b^{\nu_{\mathrm{X}-\alpha}(\mathrm{F})}$ pour toute fraction non nulle F. $\lhd$

Si $|\ |$ est une valeur absolue non-archimédienne sur le corps K, l'application $\nu : \mathrm{K} \longmapsto \mathbb{R}$, définie par $\nu(x) = -\lambda \ln(|x|)$ si $x \neq 0$ et $\nu(0) = +\infty$, où λ appartient à $\mathbb{R}_+^*$, est une valuation. Réciproquement, toute valuation ν sur K définit une valeur absolue non-archimédienne par la formule $|x| = e^{-\mu\nu(x)}$ si $x \neq 0$, où $\mu \in \mathbb{R}_+^*$.

Il résulte de l'exercice précédent que les seules valeurs absolues non-archimédiennes sur $\mathbb{Q}$ sont, outre la valeur absolue triviale ($|x| = 1$ si $x \neq 0$), les applications définies pour $x \neq 0$ par $|x| = e^{-\lambda\nu_p(x)}$, avec $\lambda > 0$ et p premier. Le théorème d'Ostrowski affirme d'autre part que les seules valeurs absolues archimédiennes sur $\mathbb{Q}$ sont les applications $x \longmapsto |x|^s$, où $|\ |$ est la valeur absolue usuelle et $0 < s \leqslant 1$. Elle définissent la même topologie que la valeur absolue usuelle.

L'exercice suivant montre que n boules quelconques, de rayon $\varepsilon > 0$ dans $\mathbb{Q}$, correspondant à n valeurs absolues deux à deux non équivalentes ont toujours une intersection non vide.

3.20. Indépendance des valeurs absolues sur $\mathbb{Q}$

Soit $p_1, \ldots, p_n$ des nombres premiers deux à deux distincts, $q_0, q_1, \ldots, q_n$ dans $\mathbb{Q}$ et $\varepsilon > 0$. Prouver qu'il existe $q \in \mathbb{Q}$ tel que $|q - q_0| < \varepsilon$ et $|q - q_i|_{p_i} < \varepsilon$ pour tout $i \in [\![1, n]\!]$ (pour p premier, $|x|_p = p^{-\nu_p(x)}$ désigne la valeur absolue p-adique du rationnel x).

(École normale supérieure)

$\rhd$ **Solution.**

• Nous chercherons q sous la forme $\sum_{i=0}^{n} \alpha_i q_i$, avec $\alpha_0, \ldots, \alpha_n$ nombres rationnels dépendant d'un entier k à déterminer.

$\star$ On aura alors, $q - q_0 = \sum_{i=1}^{n} \alpha_i q_i + (\alpha_0 - 1)q_0$. Cette quantité devra être rendue assez petite. Pour cela, nous imposerons que les α_i, pour $i \geqslant 1$ et $\alpha_0 - 1$ tendent vers 0 avec k.

$\star$ Si $i \in [\![1, n]\!]$, $q - q_i = \sum_{\substack{0 \leqslant j \leqslant n \\ j \neq i}}^{n} \alpha_j q_j + (\alpha_i - 1)q_i$. Il faudra rendre la valeur absolue p_i-adique de cette quantité assez petite, c'est-à-dire sa valuation p_i-adique assez grande. Nous choisirons les α_i pour que, pour $j \in [\![0, n]\!], j \neq i$, on ait $\nu_{p_i}(\alpha_j) = k$ et $\nu_{p_i}(\alpha_i - 1) = k$.

• Soit $k \in \mathbb{N}$ et p un nombre premier distinct de $p_1, \ldots, p_n$. Posons, pour tout $j \in [\![1, n]\!]$,

$$\alpha_j = \frac{(p_1 \ldots \widehat{p_j} \ldots p_n)^k}{p^k p_j^k + (p_1 \ldots \widehat{p_j} \ldots p_n)^k} \text{ et } \alpha_0 = \frac{(p_1 \ldots p_n)^k}{(p_1 \ldots p_n)^k + 1}$$

et montrons qu'ils conviennent. Soit $\varepsilon > 0$.

$\star$ Choisissons p tel que $p > p_1 p_2 \ldots p_n$. On a alors $\lim_{k \to +\infty} \alpha_i = 0$ pour tout i de $[\![1, n]\!]$ et, d'autre part, $\lim_{k \to +\infty} \alpha_0 = 1$. On en déduit que $\lim_{k \to +\infty} q = q_0$, et donc, pour k assez grand, $|q - q_0| < \varepsilon$.

$\star$ Soit $i \in [\![1, n]\!]$. Pour $j \in [\![0, n]\!], j \neq i$, le numérateur de α_j est divisible par p_i^k et son dénominateur est premier avec p_i. On en déduit que $\nu_{p_i}(\alpha_j) = k$. On obtient également $\nu_{p_i}(\alpha_i - 1) = k$.

En posant $m = \min_{\substack{0 \leqslant j \leqslant n \\ 1 \leqslant i \leqslant n}} \nu_{p_i}(q_j)$, on a alors

$$\begin{aligned} &\nu_{p_i}(\alpha_j q_j) = \nu_{p_i}(\alpha_j) + \nu_{p_i}(q_j) \geqslant k + m, \text{ pour } j \neq i, \\ &\nu_{p_i}((\alpha_i - 1)q_i) \geqslant \nu_{p_i}(\alpha_i - 1) + \nu_{p_i}(q_i) \geqslant k + m. \end{aligned}$$

Sachant que, pour tout $(x, y) \in \mathbb{Q}^2$, $\nu_{p_i}(x + y) \geqslant \min(\nu_{p_i}(x), \nu_{p_i}(y))$, on en déduit que, pour $i \geqslant 1$,

$$\nu_{p_i}(q - q_i) \geqslant k + m \text{ et donc } |q - q_i|_{p_i} \leqslant {p_i}^{-(k+m)}.$$

On a alors, pour k assez grand,

$$|q - q_i|_{p_i} \leqslant \varepsilon, \text{ pour tout } i \geqslant 1.$$

Pour k assez grand, q a donc toutes les propriétés voulues. $\lhd$

Chapitre 4

Arithmétique

Les nombres entiers ont toujours exercé sur les esprits une sorte de fascination. Il n'est pas étonnant que ce soit au sein de l'école pythagoricienne, éprise de mysticisme que débute l'étude de leurs propriétés : avec les catégories de pair et d'impair commencent les premières réflexions sur la divisibilité. Celles-ci aboutissent deux siècles plus tard, dans les Éléments *d'Euclide dont le chapitre VII s'ouvre par une série de définitions : nombre premier et composé, nombre parfait, diviseur et multiple, même si le langage est très différent du langage moderne. On trouve exposés entre autres l'algorithme de détermination du* pgcd *de deux nombres (algorithme d'Euclide) et la démonstration de l'infinité des nombres premiers (lemme d'Euclide).*

Aux pythagoriciens remontent les premiers exemples d'équations diophantiennes, notamment la résolution de l'équation $x^2 + y^2 = z^2$ en nombres entiers. Diophante, au IIIe *siècle de notre ère, va s'intéresser à un grand nombre d'équations analogues. Sa grande œuvre,* les Arithmétiques *rompt avec la Mathématique grecque, centrée jusqu'alors sur les problèmes géométriques, et se rapproche des méthodes algébriques hautement élaborées des Babyloniens, mais contrairement à ceux-ci, il s'intéresse uniquement aux solutions exactes. Il s'évertue à donner des règles simples de calcul algébrique comme les règles sur les produits de puissance ou une première idée de la règle des signes dans un produit. Il est le premier à utiliser un symbole littéral pour désigner les inconnues et peut être vu comme le père de l'algèbre. Il résout des équations à coefficients entiers du premier degré ($ax + by = c$) et du second degré (cas particuliers d'équations de Pell telles que $x^2 = 1 + 30y^2$). Il s'intéresse à l'écriture d'un nombre comme somme de deux carrés (il sait qu'un entier de la forme $8n + 7$ ne peut pas s'écrire comme somme de deux carrés). Il énonce l'identité de Lagrange.*

Aux VIIe *et* VIIIe *siècles, les savants arabes, notamment à Bagdad, assimilent l'héritage hellénique et oriental à travers la traduction des ouvrages de l'Antiquité (Euclide, Archimède, Diophante...). Mais leurs théories mathématiques propres sont plus orientées vers l'Algèbre que vers l'Arithmétique proprement dite.*

En Occident, le réveil de la théorie des nombres doit attendre Pierre de Fermat (1601-1665) dont les premiers travaux s'appuient sur la récente traduction des textes grecs de Diophante par Bachet de Méziriac (1621). Il s'intéresse particulièrement à la divisibilité et aux nombres

premiers. Il aborde de nombreux problèmes et formule des conjectures qui pour la plupart seront prouvées au siècle suivant : citons le petit théorème de Fermat, l'équation de Pell-Fermat ($x^2 - dy^2 = 1$ a, pour tout entier positif non carré parfait d, une infinité de solutions entières), les nombres de Fermat et le grand théorème de Fermat dont nous parlerons un peu plus loin. Il développe la première méthode générale d'attaque des équations diophantiennes : la descente infinie. Au XVIIIe *siècle, Euler et Lagrange s'inspirent de ses méthodes et prouvent la plupart de ses résultats.*

En 1801, Gauss publie Disquisitiones arithmeticae *qui contribue à unifier de nombreux résultats et à développer des méthodes et des techniques nouvelles qui marquent le début de l'Arithmétique moderne : il fixe la terminologie et les notations de la théorie des congruences, réfléchit à la notion de divisibilité et de décomposition en facteurs premiers et l'étend au cas de nombres algébriques (comme les entiers de Gauss $\mathbb{Z}+i\mathbb{Z}$), élabore la théorie des formes quadratiques à coefficients entiers, énonce le théorème des nombres premiers.*

Les premiers exercices de ce chapitre s'appuient sur la notion élémentaire de divisibilité et les théorèmes fondamentaux que constituent le lemme d'Euclide et le théorème de Gauss.

4.1. Étude de l'irréductibilité d'une fraction

1. Montrer que pour tout $n \in \mathbb{N}$, la fraction $\dfrac{5^{n+1}+6^{n+1}}{5^n+6^n}$ est irréductible.

2. Trouver une condition nécessaire et suffisante sur $(\lambda, \mu, \alpha, \beta) \in \mathbb{N}^4$ pour que la fraction $\dfrac{\lambda\alpha^{n+1}+\mu\beta^{n+1}}{\lambda\alpha^n+\mu\beta^n}$ soit irréductible pour tout $n \in \mathbb{N}^*$.

(École polytechnique)

▷ **Solution.**

1. Soit $n \in \mathbb{N}$. Raisonnons par l'absurde et supposons qu'il existe p premier divisant à la fois $5^n + 6^n$ et $5^{n+1} + 6^{n+1}$. Alors modulo p, $5^n \equiv -6^n$ et $6.5^n \equiv -6^{n+1} \equiv 5^{n+1}$, d'où p divise $5^n(6-5) = 5^n$, ce qui entraîne $p = 5$. Or clairement, le numérateur et dénominateur ne sont pas congrus à 0 modulo 5 mais à 1. La fraction considérée est donc irréductible.

2. • Pour que la fraction considérée soit irréductible, il est nécessaire que λ soit premier avec μ et β et que α soit premier avec μ et β. Supposons ces conditions réalisées dans la suite.

• Supposons qu'il existe $n \geqslant 1$ tel que $F_n = \dfrac{\lambda\alpha^{n+1} + \mu\beta^{n+1}}{\lambda\alpha^n + \mu\beta^n}$ ne soit pas irréductible. Il existe p nombre premier divisant à la fois le numérateur et le dénominateur de F_n. Modulo p, on obtient

$$\lambda\alpha^n \equiv -\mu\beta^n \quad \text{et} \quad \lambda\alpha^{n+1} \equiv -\mu\beta^{n+1}$$

Si p divise α, p divise $\mu\beta^n$ et d'après le lemme d'Euclide, il divise μ ou β. On aboutit une contradiction puisque α est premier avec μ et β. On en déduit que p ne divise pas α. On montre de même que p ne divise pas λ, μ et β. Les classes modulo p de ces entiers ne sont pas nulles dans le corps $\mathbb{Z}/p\mathbb{Z}$. On en déduit

$$\overline{\lambda} = -\overline{\mu}\left(\frac{\overline{\beta}}{\overline{\alpha}}\right)^n = -\overline{\mu}\left(\frac{\overline{\beta}}{\overline{\alpha}}\right)^{n+1}$$

et finalement $\dfrac{\overline{\beta}}{\overline{\alpha}} = 1$ après simplification (justifiée puisque les classes sont non nulles). Donc modulo p, $\alpha \equiv \beta$ et $\lambda \equiv -\mu$. En particulier, p divise $\alpha - \beta$ et $\lambda + \mu$. Nous avons donc

$$\operatorname{pgcd}(\alpha - \beta, \lambda + \mu) \neq 1.$$

• Réciproquement, supposons $\operatorname{pgcd}(\alpha - \beta, \lambda + \mu) \neq 1$. Il existe un nombre premier p divisant à la fois $\alpha - \beta$ et $\lambda + \mu$. Le système de congruences :

$$\lambda\alpha^n \equiv -\mu\beta^n \quad \text{et} \quad \lambda\alpha^{n+1} \equiv -\mu\beta^{n+1}$$

est vérifié pour tout $n \in \mathbb{N}^*$ et F_n n'est donc pas irréductible.

Conclusion. Pour que F_n soit irréductible pour tout $n \in \mathbb{N}^*$, il faut et il suffit que

$$\begin{aligned} \operatorname{pgcd}(\lambda, \mu) &= \operatorname{pgcd}(\lambda, \beta) = \operatorname{pgcd}(\alpha, \mu) = \operatorname{pgcd}(\alpha, \beta) \\ &= \operatorname{pgcd}(\alpha - \beta, \lambda + \mu) = 1. \lhd \end{aligned}$$

4.2. Équation $a^b = b^a$ dans $\mathbb{N}$

Trouver les couples (a, b) d'entiers strictement positifs tels que $a \neq b$ et $a^b = b^a$.

(École polytechnique)

▷ **Solution.**

• L'examinateur attendait sans doute une preuve arithmétique mais on constate qu'une simple étude de fonctions permet de répondre à la question. Un couple $(a,b) \in (\mathbb{N}^*)^2$, tel que $a < b$, est solution de l'équation si et seulement si $f(a) = f(b)$, où f est la fonction

$$f : x \in \mathbb{R}_+^* \longmapsto \frac{\ln x}{x}.$$

Cette fonction est strictement croissante sur $]0,e]$, allant de $-\infty$ à $\frac{1}{e}$, puis strictement décroissante sur $[e,+\infty[$, allant de $\frac{1}{e}$ à 0. On a donc nécessairement $a \leqslant e$. Comme $a = 1$ est visiblement exclu, on obtient $a = 2$. On remarque que $f(2) = f(4)$; le couple $(2,4)$ est donc solution de l'équation et c'est la seule (si $a < b$), étant données les variations de la fonction f.

• Donnons maintenant une preuve arithmétique. Si $(a,b) \in \mathbb{N}^{*2}$ est un couple solution avec $a < b$, on pose $d = \operatorname{pgcd}(a,b)$, $a = da'$ et $b = db'$. Les entiers a' et b' sont premiers entre eux et $a' < b'$. L'équation devient alors $d^{b'-a'}a'^{b'} = b'^{a'}$. L'entier a' divise $b'^{a'}$, avec qui il est premier. On a donc $a' = 1$, $b' > 1$ et $d^{b'-1} = b'$; on en déduit que $d > 1$. Si $b' \geqslant 3$, on a $d^{b'-1} > b'$; en effet, on peut écrire

$$d^{b'-1} \geqslant (1+1)^{b'-1} > 1 + \mathrm{C}_{b'-1}^1 = b'.$$

On conclut que $b' = 2$ et $d = 2$, d'où l'on tire $a = 2$ et $b = 4$. Réciproquement, on constate que le couple $(2,4)$ est solution.

Vus les rôles symétriques joués par a et b, on conclut : les couples $(2,4)$ et $(4,2)$ sont les seuls couples solutions de l'équation $a^b = b^a$ avec $a \neq b$ dans $\mathbb{N}$. ◁

4.3. Divisibilité

> Soit a, b dans $\mathbb{N}$ avec $b \geqslant a \geqslant 2$. On suppose que $a^n - 1$ divise $b^n - 1$ pour tout $n \in \mathbb{N}^*$. Montrer qu'il existe $p \in \mathbb{N}^*$ tel que $b = a^p$.
> **(École normale supérieure)**

▷ **Solution.**

Notons tout d'abord que la réciproque est vraie et facile à démontrer. En effet, si $b = a^p$ pour un certain entier $p \geqslant 1$, alors, modulo $a^n - 1$, on a $a^n \equiv 1$ et donc $(a^n)^p \equiv 1^p \equiv 1$ c'est-à-dire $b^n \equiv 1$. Donc $a^n - 1$ divise $b^n - 1$ et cela pour tout $n \geqslant 1$. On va prouver par l'absurde que les entiers qui ne sont pas des puissances de a ne conviennent pas.

On fait donc l'hypothèse que $u_n = \dfrac{b^n - 1}{a^n - 1}$ est entier pour tout $n \geqslant 1$ et que b n'est pas une puissance de a. La suite u_n tend vers $+\infty$ et de plus $u_n \sim \left(\dfrac{b}{a}\right)^n$. L'idée est d'aboutir à une contradiction de nature asymptotique en considérant une combinaison linéaire à coefficients entiers des termes de la suite u. Comme $u_{n+1} \sim \left(\dfrac{b}{a}\right)^{n+1}$ il est naturel de poser

$$v_n = au_{n+1} - bu_n.$$

Cette suite (v_n) est toujours une suite d'entiers et elle va être plus petite que la suite (u_n). En effet, un petit calcul donne

$$v_n = \frac{(1-a)b^{n+1} + (b-1)a^{n+1} - b + a}{(a^n - 1)(a^{n+1} - 1)} \sim \frac{(1-a)b^{n+1}}{a^{2n+1}} = \frac{(1-a)b}{a}\left(\frac{b}{a^2}\right)^n.$$

Supposons alors pour commencer que $a < b < a^2$. L'équivalent obtenu montre que (v_n) tend vers 0 en étant non nulle à partir d'un certain rang : mais c'est absurde puisqu'il s'agit d'une suite d'entiers !

Avant de traiter le cas général, regardons encore ce qui se passe si on suppose que $a^2 < b < a^3$. Notre suite (v_n) diverge vers $+\infty$. Étant donné l'équivalent trouvé plus haut, il est naturel de recommencer et de poser

$$w_n = a^2 v_{n+1} - bv_n.$$

Le calcul exact de w_n est un peu long et on peut le confier à un logiciel de calcul formel. On obtient comme équivalent

$$w_n \sim \frac{(1-a^2)(1-a)b^2}{a^3}\left(\frac{b}{a^3}\right)^n$$

et cela conduit à la même contradiction que précédemment : w_n est une suite d'entiers non nuls à partir d'un certain rang qui converge vers 0.

Traitons maintenant le cas général et notons p l'unique entier naturel tel que $a^p < b < a^{p+1}$. L'étude des cas précédents nous invite à considérer les opérateurs $\mathrm{T}_k : (x_n)_{n\geqslant 0} \mapsto (a^k x_{n+1} - bx_n)_{n\geqslant 0}$ sur l'espace des suites réelles. Il est clair que l'image par T_k d'une suite à coefficients dans $\mathbb{Z}$ est encore une suite à coefficients dans $\mathbb{Z}$. On considère alors la suite $(\mathrm{T}_p \circ \cdots \circ \mathrm{T}_2 \circ \mathrm{T}_1)(u)$ et on va montrer qu'elle tend vers 0 en étant non nulle à partir d'un certain rang, ce qui fournira la contradiction cherchée. Le calcul exact de cette suite étant inextricable on va se contenter de travailler sur des développements asymptotiques. On a

$$u_n = \frac{b^n}{a^n} + \frac{b^n}{a^{2n}} + \cdots + \frac{b^n}{a^{pn}} + \frac{b^n}{a^{(p+1)n}} + o\left(\frac{b^n}{a^{(p+1)n}}\right)$$

car $\dfrac{1}{a^n}$ est négligeable devant $\dfrac{b^n}{a^{(p+1)n}}$ étant donné que $\dfrac{1}{a} < \dfrac{b}{a^{p+1}}$ par hypothèse. On a bien entendu poussé le développement de u_n jusqu'à

un terme qui tend vers 0. On a alors le développement de u_{n+1} dans la même échelle :

$$u_{n+1} = \frac{b}{a}\frac{b^n}{a^n} + \frac{b}{a^2}\frac{b^n}{a^{2n}} + \cdots + \frac{b}{a^p}\frac{b^n}{a^{pn}} + \frac{b}{a^{p+1}}\frac{b^n}{a^{(p+1)n}} + o\left(\frac{b^n}{a^{(p+1)n}}\right).$$

On en déduit que

$$v_n = \mathrm{T}_1(u)_n = b\left(\frac{1}{a} - 1\right)\frac{b^n}{a^{2n}} + \cdots + b\left(\frac{1}{a^p} - 1\right)\frac{b^n}{a^{(p+1)n}} + o\left(\frac{b^n}{a^{(p+1)n}}\right).$$

L'opérateur T_1 a annulé le premier coefficient du développement asymptotique (on retrouve notamment l'équivalent ci-dessus). En itérant de même on voit que $w_n = (\mathrm{T}_2 \circ \mathrm{T}_1)(u)_n$ a pour développement

$$b^2\left(\frac{1}{a^2} - 1\right)\left(\frac{1}{a} - 1\right)\frac{b^n}{a^{3n}} + \cdots$$
$$+ b^2\left(\frac{1}{a^p} - 1\right)\left(\frac{1}{a^{p-1}} - 1\right)\frac{b^n}{a^{(p+1)n}} + o\left(\frac{b^n}{a^{(p+1)n}}\right).$$

Une récurrence finie facile permet de voir que

$$(\mathrm{T}_p \circ \cdots \circ \mathrm{T}_2 \circ \mathrm{T}_1)(u)_n \sim b^p\left(\frac{1}{a^p} - 1\right)\cdots\left(\frac{1}{a} - 1\right)\frac{b^n}{a^{(p+1)n}}$$

ce qui permet de conclure car le coefficient est bien non nul. $\lhd$

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

Soit $\mathrm{P} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ et $\mathrm{Q} = (b_1, \ldots, b_n) \in \mathbb{Z}^n$.

1. Montrer l'équivalence des deux conditions suivantes :

(*i*) les $b_i - a_i$ sont premiers entre eux dans leur ensemble ;

(*ii*) il n'existe pas de points de $\mathbb{Z}^n$ sur le segment $]\mathrm{P}, \mathrm{Q}[\subset \mathbb{R}^n$ (si cette condition est réalisée, on dit que Q est visible depuis P).

2. On prend $n = 2$. Montrer que pour tout $r \in \mathbb{N}^*$, il existe un carré de $\mathbb{Z}^2$ de côté r (*i.e.* une partie du type $[\![a+1, a+r]\!] \times [\![b+1, b+r]\!]$ avec $(a, b) \in \mathbb{Z}^2$), dont tous les points sont invisibles de l'origine.

(**École polytechnique**)

$\rhd$ **Solution.**

1. Quitte à faire une translation de vecteur $(a_1, \ldots, a_n) \in \mathbb{Z}^n$, on peut se ramener au cas où $\mathrm{P} = (0, \ldots, 0)$.

• Supposons que $]\mathrm{P}, \mathrm{Q}[$ admette un point $(\ell_1, \ldots, \ell_n) \in \mathbb{Z}^n$. Alors il existe $\lambda \in]0, 1[$ tel que $\ell_i = \lambda b_i$ pour tout $1 \leqslant i \leqslant n$. Nécessairement, λ est un rationnel qui s'écrit $\frac{p}{q}$, avec $(p, q) \in \mathbb{N}^{*2}$ et $p < q$. Ainsi, pour

tout $1 \leqslant i \leqslant n$, on a $pb_i = q\ell_i$ et donc

$$p\,\mathrm{pgcd}(b_1, \ldots, b_n) = q\,\mathrm{pgcd}(\ell_1, \ldots, \ell_n),$$
$$\mathrm{pgcd}(b_1, \ldots, b_n) = \frac{q}{p}\,\mathrm{pgcd}(\ell_1, \ldots, \ell_n) > 1.$$

Les b_i ne sont donc pas premiers entre eux dans leur ensemble.

• Réciproquement, supposons que les b_i ne sont pas premiers entre eux. Soit donc $k \in \mathbb{N}$, $k > 1$, un diviseur commun à tous les b_i. Alors le point $\left(\frac{b_1}{k}, \frac{b_2}{k}, \ldots, \frac{b_n}{k}\right)$ est dans $\mathbb{Z}^n$ et il se situe sur le segment $]\mathrm{P}, \mathrm{Q}[$ puisque $0 < \frac{1}{k} < 1$. L'équivalence est prouvée.

2. D'après ce qui précède, il suffit de trouver deux entiers a et b tels que pour tout couple $(i, j) \in [\![1, r]\!]^2$, $a + i$ et $b + j$ ne soient pas premiers entre eux. En particulier l'entier $a + i$ doit avoir un facteur premier en commun avec $b + j$. On se donne donc une famille $(p_{ij})_{1 \leqslant i, j \leqslant r}$ de nombres premiers, deux à deux distincts. Le théorème chinois, assure l'existence d'un entier a vérifiant pour tout $(i, j) \in [\![1, r]\!]^2$, $a \equiv -i\ [p_{ij}]$. De même, il existe un entier b tel que $b \equiv -j\ [p_{ij}]$ pour tout couple (i, j). On a alors la propriété désirée, puisque $a + i$ et $b + j$ ont le nombre premier p_{ij} comme diviseur commun. ◁

4.5. Produits d'entiers consécutifs

Soit $\mathrm{N}_1, \ldots, \mathrm{N}_q$ des entiers non nuls, deux à deux distincts. On pose $\mathrm{P}_k = \prod_{i=1}^{q} (\mathrm{N}_i + k)$, pour $k \in \mathbb{Z}$ et on suppose que pour tout $k \in \mathbb{Z}$, P_0 divise P_k.

1. Montrer qu'il existe $i \in [\![1, q]\!]$ tel que $|\mathrm{N}_i| = 1$.

2. On suppose de plus que, pour tout $1 \leqslant i \leqslant q$, on a $\mathrm{N}_i \geqslant 1$. Montrer que $\mathrm{N}_1, \ldots, \mathrm{N}_q$ sont les q premiers entiers naturels non nuls.

(École polytechnique)

Solution.

Rappelons que pour N *et* d *dans* $\mathbb{N}$, *si* $d|\mathrm{N}$ *et* $d > \mathrm{N}$ *alors* $\mathrm{N} = 0$.

1. On a

$$\mathrm{P}_0 = \mathrm{N}_1\mathrm{N}_2 \ldots \mathrm{N}_q,\ \mathrm{P}_1 = (\mathrm{N}_1 + 1) \ldots (\mathrm{N}_q + 1),\ \mathrm{P}_{-1} = (\mathrm{N}_1 - 1) \ldots (\mathrm{N}_q - 1).$$

Comme P_0 divise P_1 et P_{-1}, P_0^2 divise $\mathrm{P}_1\mathrm{P}_{-1}$. Puisque

$$0 \leqslant \mathrm{P}_1\mathrm{P}_{-1} = (\mathrm{N}_1^2 - 1) \ldots (\mathrm{N}_q^2 - 1) < \mathrm{N}_1^2 \ldots \mathrm{N}_q^2 = \mathrm{P}_0^2,$$

on a nécessairement $\mathrm{P}_1\mathrm{P}_{-1} = 0$ et il existe un indice i tel que $\mathrm{N}_i^2 = 1$, c'est-à-dire $|\mathrm{N}_i| = 1$.

2. On peut supposer $1 \leqslant N_1 < N_2 < \cdots < N_q$, quitte à renuméroter les N_i. Montrons, par récurrence sur k compris entre 1 et q, que $N_k = k$.

• Le cas $k = 1$ résulte de la question précédente.

• Supposons $k \geqslant 2$. On a, d'après l'hypothèse de récurrence,

$$\begin{aligned} P_0 &= 1 \cdot 2 \ldots (k-1) N_k \ldots N_q = (k-1)! N_k \ldots N_q \quad \text{et} \\ P_{-k} &= (-k+1)(-k+2) \ldots (-2)(-1)(N_k - k) \ldots (N_q - k) \\ &= (-1)^{k-1}(k-1)!(N_k - k) \ldots (N_q - k). \end{aligned}$$

De P_0 divise P_{-k}, on déduit que $N_k \ldots N_q$ divise $(N_k - k) \ldots (N_q - k)$. Or si $\ell \in [\![k, q]\!]$, on a $N_\ell > N_{k-1} = k - 1$, c'est-à-dire $N_\ell \geqslant k$. On obtient donc

$$0 \leqslant (N_k - k) \ldots (N_q - k) < N_k \ldots N_q.$$

Il en résulte que $(N_k - k) \ldots (N_q - k) = 0$. Il existe $\ell \in [\![k, q]\!]$ tel que $N_\ell = k$. Comme $k \leqslant N_k \leqslant N_\ell$, on a, puisque les N_i sont deux à deux distincts, $\ell = k$ et $N_k = k$. $\lhd$

L'exercice suivant exploite le théorème de Bezout : des entiers $a_1, \ldots, a_n$ sont premiers entre eux, si et seulement si il existe une combinaison linéaire des a_k à coefficients entiers égale à 1. Ce résultat fut démontré par Bachet de Méziriac (1621), puis généralisé par Bezout (1730-1752) pour des polynômes à coefficients réels.

4.6. Parties de $\mathbb{N}$ additivement stables

Soit P une partie de $\mathbb{N}$ stable par addition. Montrer qu'il existe $(n, k) \in \mathbb{N}^2$ tel que $P \cap [\![n, +\infty[\![= k\mathbb{N} \cap [\![n, +\infty[\![$.

(École normale supérieure)

$\rhd$ **Solution.**

Supposons $P \neq \{0\}$, le cas $P = \{0\}$ étant trivial. Soit d le pgcd de tous les éléments de P ; d appartient à $\mathbb{N}^*$.

• Traitons, pour commencer, le cas où que $d = 1$ et montrons qu'alors $k = 1$ convient. On fait l'hypothèse supplémentaire que P contient 0, l'y rajouter ne changeant rien à la propriété à démontrer. La remarque fondamentale est que si P est additivement stable et contient 0, alors toute combinaison linéaire d'éléments de P à coefficients entiers naturels appartient à P.

$\star$ Montrons qu'il existe $m \in \mathbb{N}$ tel que m et $m + 1$ soient dans P.

L'ensemble P est infini car si $x \in P \setminus \{0\}$, alors $x\mathbb{N} \subset P$. Soit $(a_i)_{i \in \mathbb{N}}$ la suite des éléments de P, rangés par ordre croissant. Pour tout entier naturel i, posons $d_i = \text{pgcd}(a_0, \ldots, a_i)$. Alors (d_i) est une suite décroissante

d'entiers naturels, donc stationnaire : il existe des entiers naturels δ et i_0 tels que $d_i = \delta$ pour $i \geqslant i_0$. Comme δ divise tous les éléments de P, on a $\delta = 1$ et en particulier, $\mathrm{pgcd}(a_0, \ldots, a_{i_0}) = 1$.

D'après le théorème de Bezout, il existe $(u_0, \ldots, u_{i_0}) \in \mathbb{Z}^{i_0+1}$ tel que $\sum_{i=0}^{i_0} u_i a_i = 1$. Soit I (resp. J) l'ensemble des indices i tels que $u_i > 0$ (resp. $u_i \leqslant 0$). On peut écrire

$$1 = \sum_{i \in \mathrm{I}} u_i a_i - \sum_{i \in \mathrm{J}} |u_i| a_i.$$

D'après la remarque initiale, on a

$$m = \sum_{i \in \mathrm{J}} |u_i| a_i \in \mathrm{P} \quad \text{et} \quad m + 1 = \sum_{i \in \mathrm{I}} u_i a_i \in \mathrm{P}.$$

⋆ La même remarque justifie le fait que P contient tous les entiers naturels de la forme $a(m+1) + bm$, avec $(a, b) \in \mathbb{N}^2$. Montrons que tout entier naturel supérieur ou égal à $m(m-1)$ peut s'écrire ainsi. Si $\mathrm{N} \geqslant m(m-1)$, on effectue la division euclidienne de N par m. On obtient $\mathrm{N} = qm + r$, avec $0 \leqslant r \leqslant m-1$ et $q \geqslant m-1$ car $\mathrm{N} \geqslant m(m-1)$ (en effet, si $q \leqslant m-2$, $qm + r \leqslant m(m-2) + m - 1 = m(m-1) - 1$). On peut alors écrire

$$\mathrm{N} = qm + r(m + 1 - m) = (q - r)m + r(m + 1),$$

avec r et $q - r$ positifs. C'est la décomposition cherchée, qui montre que P contient tous les entiers supérieurs ou égaux à $m(m-1)$. On a donc bien $1\mathbb{N} \cap [\![m(m-1), +\infty[\![= \mathrm{P} \cap [\![m(m-1), +\infty[\![$.

• Passons au cas général, $d \geqslant 2$. En posant $\mathrm{P} = d\mathrm{P}'$, on obtient une partie P' additivement stable de $\mathbb{N}$, telle que le pgcd de tous ses éléments soit 1. Il existe donc, d'après ce qui précède, $n \in \mathbb{N}$ tel que $\mathrm{P}' \cap [\![n, +\infty[\![= [\![n, +\infty[\![$ et donc $\mathrm{P} \cap [\![dn, +\infty[\![= d\mathbb{N} \cap [\![dn, +\infty[\![$, ce qui montre la propriété pour P. ◁

L'exercice suivant montre l'intérêt qu'on peut avoir à réduire certains problèmes modulo n pour un entier n bien choisi. Il commence une série d'exercices consacrés aux congruences et aux anneaux $\mathbb{Z}/n\mathbb{Z}$.

4.7. Un exercice pour les années impaires

Montrer qu'il n'existe pas d'application $f : \mathbb{N} \to \mathrm{N}$ telle que pour tout $n \in \mathbb{N}$, $f(f(n)) = n + 2007$.

(École normale supérieure)

▷ **Solution.**

Supposons l'existence d'une telle application f et soit $n \in \mathbb{N}$. On a

$$f(n+2007) = f(f(f(n))) = (f \circ f)(f(n)) = f(n) + 2007.$$

Par une récurrence immédiate, on en déduit que, pour tout $k \in \mathbb{N}$,

$$f(n+2007k) = f(n) + 2007k.$$

Il en résulte que le résidu de $f(n)$ modulo 2007 ne dépend que du résidu de n modulo 2007. Ainsi, f induit une application $\overline{f}$ de $\mathbb{Z}/2007\mathbb{Z}$ dans lui-même, définie par $\overline{f}(\overline{n}) = \overline{f(n)}$, où $\overline{k}$ désigne le projeté de l'entier k dans $\mathbb{Z}/2007\mathbb{Z}$. La propriété vérifiée par f implique que $\overline{f} \circ \overline{f} = \mathrm{Id}$. Or, le cardinal de $\mathbb{Z}/2007\mathbb{Z}$ est impair et toute involution d'un ensemble fini de cardinal impair admet au moins un point fixe (en effet, la permutation f est d'ordre 2 et se décompose donc en produit de transpositions à supports disjoints ; il y a donc une orbite réduite à un singleton). Il existe donc un entier $a \in \mathbb{N}$ (que l'on peut même prendre dans $[\![0, 2006]\!]$) et $k \in \mathbb{N}$ tels que $f(a) = a + 2007k$. On obtient alors

$$f(f(a)) = a + 2007 = f(a + 2007k) = f(a) + 2007k = a + 2 \cdot 2007k.$$

D'où l'on tire $2k = 1$, ce qui est impossible dans $\mathbb{Z}$ et fournit la contradiction souhaitée. ◁

4.8. Équation du second degré dans $\mathbb{Z}/p\mathbb{Z}$

> Montrer que pour tout nombre premier p, il existe un entier naturel n tel que $6n^2 + 5n + 1 \equiv 0\ [p]$.
>
> **(École polytechnique)**

▷ **Solution.**

Pour $p = 2$ ou 3, $n = 1$ est solution. Supposons $p \geqslant 5$ premier. Alors $\mathbb{Z}/p\mathbb{Z}$ est alors un corps commutatif de caractéristique distincte de 2. Comme $\overline{6}$ est non nul dans $\mathbb{Z}/p\mathbb{Z}$, l'équation $6x^2+5x+1$ est une équation du second degré. On calcule son discriminant $\Delta = 25 - 24 = 1 = 1^2$. C'est un carré. Donc l'équation admet deux racines distinctes dans $\mathbb{Z}/p\mathbb{Z}$, ce qui assure l'existence de $n \in \mathbb{N}$ tel que $6n^2 + 5n + 1 \equiv 0\ [p]$. ◁

Lorsque p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et réciproquement. Dans ces conditions, $(\mathbb{Z}/p\mathbb{Z})^*$ est un groupe multiplicatif de cardinal $p-1$ et le théorème de Lagrange impose alors que si p ne divise pas a, on ait

$a^{p-1} \equiv 1 \pmod p$ *: c'est le petit théorème de Fermat qui est souvent utilisé dans les calculs de congruences.*

4.9. Un problème de congruence

> Montrer que pour tout $n \in \mathbb{N}^*$, $10^{10^n} \equiv 4 \pmod 7$.
> **(École polytechnique)**

Solution.

Posons $A = 10^{10^n}$. On a $A \equiv 3^{10^n} \pmod 7$ et, puisque 7 est un nombre premier ne divisant pas 3, d'après le petit théorème de Fermat, $3^6 \equiv 1 \pmod 7$. Recherchons donc le reste de 10^n modulo 6, c'est-à-dire le reste de 4^n modulo 6. On obtient $4^2 \equiv 4 \pmod 6$, puis, pour tout entier $n \geqslant 2$,

$$4^n \equiv 4^2 4^{n-2} \equiv 4 \cdot 4^{n-2} = 4^{n-1} \pmod 6.$$

On a donc, pour $n \geqslant 1$, $4^n \equiv 4 \pmod 6$ et $A \equiv 3^4 = 81 \equiv 4 \pmod 7$. ◁

4.10. Un multiple de 1996 qui ne s'écrit qu'avec des 4

> Montrer qu'il existe un multiple de 1996 dont l'écriture décimale ne comporte que le chiffre 4.
> **(École normale supérieure)**

Solution.

Notons $u_n = 444\ldots4 = \sum_{k=0}^{n-1} 4.10^k = \frac{4}{9}(10^n - 1)$ l'entier dont l'écriture décimale est composée du chiffre 4 répété n fois. On a $1996 = 4 \times 499$ et 499 est un nombre premier. On en déduit, d'après le petit théorème de Fermat, $10^{498} \equiv 1$ [499]. Comme 9 est premier avec 499, 499 divise aussi l'entier $\frac{10^{498} - 1}{9}$. En multipliant par 4 on en déduit donc que 1996 divise u_{498}. ◁

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

> Soit p un nombre premier et $k \in \mathbb{N}^*$. Montrer que $\sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$ est égal à 0 ou -1. Préciser à quelle condition on obtient 0 ou -1.
> **(École polytechnique)**

▷ **Solution.**

Posons $S_k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} x^k$. Soit y un élément non nul de $\mathbb{Z}/p\mathbb{Z}$. L'application $x \longmapsto yx$ est une bijection de $\mathbb{Z}/p\mathbb{Z}$. Il en résulte que :

$$y^k S_k = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (yx)^k = \sum_{z \in \mathbb{Z}/p\mathbb{Z}} z^k = S_k.$$

De deux choses l'une :

- soit il existe y non nul tel que $y^k \neq 1$ et alors $S_k = 0$;
- soit $y^k = 1$ pour tout y non nul et dans ce cas, $S_k = \overline{p-1} = -1$.

On sait déjà par le petit théorème de Fermat que, si k est un multiple de $p-1$, alors c'est la deuxième éventualité qui se produit. Montrons réciproquement que si $p-1$ ne divise pas k, alors $S_k = 0$. Pour cela, posons $d = \text{pgcd}(p-1, k)$. On a par hypothèse $d < p-1$. Supposons alors par l'absurde que $y^k = 1$ pour tout $y \in (\mathbb{Z}/p\mathbb{Z})^*$. Dans ce cas l'ordre de tout y non nul de $(\mathbb{Z}/p\mathbb{Z})^*$ divise k (par hypothèse) et $p-1$ (par le théorème de Lagrange) donc divise d. Comme le polynôme $X^d - 1$ ne peut pas avoir $p-1$ racines distinctes, c'est absurde.

Ainsi, $S_k = 0$ si et seulement si $p-1$ divise k. ◁

4.12. Théorème de Wilson (1759)

Soit $p \in \mathbb{N}^*$, $p \geqslant 2$. Montrer l'équivalence :

$$(p-1)! \equiv -1 \pmod{p} \iff p \text{ premier.}$$

(École polytechnique)

▷ **Solution.**

- Supposons p premier. Nous pouvons écrire $\overline{(p-1)!} = \prod_{x \in (\mathbb{Z}/p\mathbb{Z})^*} x$.

Comme p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et dans ce produit, on peut associer par paires chaque élément x et son inverse x^{-1}, lorsque $x \neq x^{-1}$, *i.e.* $x^2 \neq 1$ ou encore $x \neq \pm\overline{1}$. Le produit de x par x^{-1} fait 1 et il reste donc

$$\overline{(p-1)!} = \overline{1} \times (-\overline{1}) = -\overline{1}.$$

- Réciproquement, supposons que p divise $1 + (p-1)!$. On a donc $\overline{(p-1)!} = -\overline{1}$ dans $\mathbb{Z}/p\mathbb{Z}$. On en déduit que si $1 \leqslant k \leqslant p-1$, $\overline{k}$ est inversible (d'inverse $-\prod_{\substack{1 \leqslant \ell \leqslant p-1 \\ \ell \neq k}} \overline{\ell}$). Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps et p est premier. ◁

Bien entendu ce critère de primalité est inutilisable en pratique. Il semblerait que le résultat était déjà connu de Leibniz. On peut en déduire que si p est un nombre premier congru à 1 modulo 4, alors -1 est un

carré modulo p (regrouper chaque facteur de $(p-1)!$ avec son opposé pour obtenir $-1 \equiv \left(\frac{p-1}{2}!\right)^2$; on pourra aussi se reporter à l'exercice 4.34).

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

Soit p un nombre premier.

1. Soit q un nombre premier qui divise $p-1$. Établir l'existence d'un élément de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre multiplicatif q.

2. Soit q un nombre premier et $\alpha \in \mathbb{N}^*$ tels que q^α divise $p-1$. Montrer l'existence d'un élément de $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ d'ordre q^α.

3. En déduire que $((\mathbb{Z}/p\mathbb{Z})^*, \times)$ est cyclique.

(École normale supérieure)

▷ **Solution.**

1. L'entier p étant premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps et $(\mathbb{Z}/p\mathbb{Z})^*$ est son groupe multiplicatif. Pour tout x dans $(\mathbb{Z}/p\mathbb{Z})^*$, notons $y_x = x^{\frac{p-1}{q}}$. On a alors $(y_x)^q = x^{p-1} = 1$, d'après le petit théorème de Fermat. L'ordre de y_x divise donc q et puisque q est premier, il est donc égal à q ou à 1. Dire que l'ordre de y_x est 1, c'est dire que $y_x = 1$. Imaginons que cela soit le cas pour tout x dans $(\mathbb{Z}/p\mathbb{Z})^*$. Le polynôme $X^{\frac{p-1}{q}} - 1$ aurait au moins $p-1$ racines distinctes. Comme son degré $\frac{p-1}{q}$ est strictement inférieur à $p-1$, c'est absurde. Il existe donc $x \in (\mathbb{Z}/p\mathbb{Z})^*$ pour lequel $y_x \neq 1$. Cet élément y_x est d'ordre q.

Le résultat de cette question est un cas particulier du lemme de Cauchy démontré dans l'exercice 2.10.

2. Inspirons-nous de ce qui précède : pour tout x dans $(\mathbb{Z}/p\mathbb{Z})^*$, on pose $y_x = x^{\frac{p-1}{q^\alpha}}$. On a alors $(y_x)^{q^\alpha} = x^{p-1} = 1$. L'ordre de y_x divise donc q^α ; il est de la forme q^{r_x} avec $r_x \leqslant \alpha$. On considère le plus grand des entiers r_x pour x décrivant l'ensemble fini $(\mathbb{Z}/p\mathbb{Z})^*$; on le note r. On a $r \leqslant \alpha$. On obtient $x^{\frac{p-1}{q^\alpha}q^r} = (y_x)^{q^r} = \left((y_x)^{q^{r_x}}\right)^{q^{r-r_x}} = 1$, pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^*$. Le polynôme $X^{\frac{p-1}{q^{\alpha-r}}} - 1$ a au moins $p-1$ racines distinctes. Ce polynôme n'étant manifestement pas le polynôme nul, son degré doit être supérieur ou égal à $p-1$. On a donc $\frac{p-1}{q^{\alpha-r}} = p-1$ et $\alpha = r$. Étant donnée la définition de r, il existe donc dans $(\mathbb{Z}/p\mathbb{Z})^*$ un élément d'ordre q^α.

3. Il a été démontré dans le chapitre 2 sur les groupes (exercice 2.8) que si G est un groupe abélien et x et y sont deux éléments de G d'ordre

p et q respectivement, p et q étant premiers entre eux, alors l'ordre de xy dans G est pq.

Bien évidemment, on établit par récurrence que si $x_1, \ldots, x_r$ sont d'ordres respectifs $p_1, \ldots, p_r$, les p_i étant deux à deux premiers entre eux, l'ordre de leur produit $x_1 \ldots x_r$ est $p_1 \ldots p_r$.

Décomposons donc $p-1$ en produit de facteurs premier $q_1^{\alpha_1} \ldots q_r^{\alpha_r}$, les q_i étant des entiers premiers et distincts deux à deux et les α_i des entiers naturels non nuls. D'après la question 2, il existe, pour tout $1 \leqslant i \leqslant r$, un élément x_i de $(\mathbb{Z}/p\mathbb{Z})^*$ d'ordre $q_i^{\alpha_i}$. Ainsi, le produit $x_1 \ldots x_r$ est d'ordre $q_1^{\alpha_1} \ldots q_r^{\alpha_r} = p-1$. Le groupe $(\mathbb{Z}/p\mathbb{Z})^*$ a donc un élément d'ordre $p-1$. Il est cyclique. $\lhd$

On pourra également consulter l'exercice 2.8 qui établit un résultat plus général, à savoir : tout sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

Dans le cas où on ne suppose plus n premier, on peut considérer le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$, habituellement noté $(\mathbb{Z}/n\mathbb{Z})^\times$. Son cardinal est le nombre d'entiers k compris entre 1 et n, premiers avec n. Il est noté $\varphi(n)$, où φ est appelée indicatrice d'Euler. *Si $a \in \mathbb{Z}$ est premier avec n, il vérifie, d'après le théorème de Lagrange, $a^{\varphi(n)} \equiv 1 \pmod{n}$: c'est un théorème d'Euler qui généralise le petit théorème de Fermat.*

4.14. Critères de primalité

Soit a et p des entiers de $\mathbb{N}^*$ tels que $a^{p-1} \equiv 1 \pmod{p}$.

1. On suppose que pour tout diviseur d de $p-1$ autre que $p-1$, l'entier $a^d - 1$ est premier avec p. Montrer que p est premier.

2. On suppose que $p-1$ se décompose en $p-1 = rs$ avec $r \geqslant s$ et que, pour tout diviseur t de r autre que 1, l'entier $a^{\frac{p-1}{t}} - 1$ est premier avec p. Montrer que p est premier.

(**École normale supérieure**)

$\rhd$ **Solution.**

1. Considérons le groupe multiplicatif des inversibles de $\mathbb{Z}/p\mathbb{Z}$ que nous noterons $(\mathbb{Z}/p\mathbb{Z})^\times$. L'entier p est premier si et seulement si $\mathbb{Z}/p\mathbb{Z}$ est un corps, c'est-à-dire si et seulement si tout élément de $(\mathbb{Z}/p\mathbb{Z})^*$ est inversible, soit encore si et seulement si $\varphi(p) = \mathrm{Card}(\mathbb{Z}/p\mathbb{Z})^\times = p-1$. On a, dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^{p-1} = 1$; $\overline{a}$ est donc inversible et son ordre dans $(\mathbb{Z}/p\mathbb{Z})^\times$ divise $p-1$. On sait par hypothèse que, pour tout diviseur d de $p-1$, $a^d - 1$ est premier avec p et en particulier $\overline{a}^d \neq 1$. L'ordre de $\overline{a}$ est donc $p-1$. Il en résulte que $\varphi(p) \geqslant p-1$ et donc $\varphi(p) = p-1$. Cela montre que p est premier.

2. Raisonnons par l'absurde et supposons p non premier. Il admet alors un diviseur premier $q \leqslant \sqrt{p}$. On a *a fortiori* $a^{p-1} \equiv 1 \pmod{q}$. Dans l'anneau $\mathbb{Z}/q\mathbb{Z}$, on obtient donc $\overline{a}^{p-1} = 1$, soit $(\overline{a}^s)^r = 1$; $\overline{a}^s$ est donc un inversible de $\mathbb{Z}/q\mathbb{Z}$ dont l'ordre divise r. Traduisons l'hypothèse : pour tout diviseur $t \neq 1$ de r, $a^{\frac{p-1}{t}} - 1$ n'est pas divisible par q, c'est-à-dire $\overline{a}^{\frac{p-1}{t}} \neq 1$. Or nous avons

$$\overline{a}^{\frac{p-1}{t}} = \overline{a}^{\frac{sr}{t}} = (\overline{a}^s)^{\frac{r}{t}}.$$

Puisque $\dfrac{r}{t}$ décrit les diviseurs stricts de r, lorsque t décrit les diviseurs de r autre que 1, l'ordre de $\overline{a}^s$ est r. On en déduit que $r \leqslant q-1$. D'autre part, comme r et s ne peuvent être tous deux inférieurs strictement à $\sqrt{p-1}$ et comme $r \geqslant s$, on a $r \geqslant \sqrt{p-1}$. Il en résulte $\sqrt{p-1} \leqslant q-1 \leqslant \sqrt{p}-1$. En élevant au carré, il vient $p-1 \leqslant p+1-2\sqrt{p}$ et $\sqrt{p} \leqslant 1$, ce qui est exclu.

Conclusion. p est un nombre premier. $\lhd$

Les critères de primalité de ce type sont dus à Lehmer. Le lecteur intéressé par ces questions pourra consulter l'excellent cours d'algèbre de Michel Demazure[1].

4.15. Diviseurs premiers communs aux termes d'une suite arithmétique

1. Soit a et r deux entiers relatifs premiers entre eux. Montrer qu'il existe $k \in \mathbb{N}^*$ tel que $a^k \equiv 1 \pmod{r}$.

2. Soit a et r deux entiers avec $a > r \geqslant 2$. Montrer que la progression arithmétique de premier terme a et de raison r contient une infinité de termes ayant tous les mêmes diviseurs premiers.

(École polytechnique)

$\rhd$ **Solution.**

1. Comme a est premier avec r, sa classe $\overline{a}$ est inversible dans $\mathbb{Z}/r\mathbb{Z}$. L'ensemble des éléments inversibles de $\mathbb{Z}/r\mathbb{Z}$ est un groupe fini. Si $k \geqslant 1$ est l'ordre de $\overline{a}$ dans ce groupe, on a $\overline{a}^k = \overline{1}$, c'est-à-dire $a^k \equiv 1 \pmod{r}$.

2. Si $\operatorname{pgcd}(a,r) = d$, on pose $a = \alpha d$ et $r = \rho d$, avec $\operatorname{pgcd}(\alpha,\rho) = 1$ et $\alpha > \rho \geqslant 1$. Pour tout $n \in \mathbb{N}$, on a $a + nr = d(\alpha + n\rho)$. L'ensemble des diviseurs premiers de $a + nr$ étant la réunion de ceux de d et de $\alpha + n\rho$, il suffit donc de démontrer le résultat pour α et ρ. Autrement dit, on peut supposer a et r premiers entre eux et $a \geqslant 2$.

Reprenons les notations de la première question. Pour tout $n \in \mathbb{N}$, on a $a^{nk} \equiv 1 \pmod{r}$ et donc $a^{nk+1} \equiv a \pmod{r}$. Autrement dit, il

1. DEMAZURE (M.), *Cours d'algèbre*, Cassini, 1997, p 71-83.

existe $\ell_n \in \mathbb{Z}$ tel que $a^{nk+1} = \ell_n r + a$. Alors la suite (ℓ_n) est strictement croissante (puisque $k > 0$) et les entiers $\ell_n r + a$ ont bien les mêmes facteurs premiers que a. $\lhd$

Pierre de Fermat est issu d'une famille de commerçants et exerce le métier de conseiller au Parlement de Toulouse. Pour lui, les mathématiques sont un hobby, ce qui n'a pas empêché ses travaux, dont peu furent publiés de son vivant, d'être à l'origine de développements féconds. Il s'intéresse particulièrement aux nombres premiers.

4.16. Nombres de Fermat

1. Déterminer une condition nécessaire sur $m \in \mathbb{N}$ pour que le nombre $2^m + 1$ soit premier.

On pose pour tout $n \in \mathbb{N}$, $F_n = 2^{2^n} + 1$: F_n est le n-ième nombre de Fermat.

2. Vérifier que F_0, F_1, F_2, F_3 et F_4 sont des nombres premiers. Montrer que F_5 est divisible par 641 (pour cela, on observera que $641 = 5^4 + 2^4 = 1 + 5 \times 2^7$).

3. Prouver que si $n \neq m$, alors F_n et F_m sont premiers entre eux. Retrouver ainsi le théorème d'Euclide : il existe une infinité de nombres premiers.

4. Si p est un diviseur premier de F_n, établir que $p \equiv 1\ [2^{n+1}]$. Expliquer pourquoi on en vient naturellement à essayer 641 comme diviseur de F_5.

(École normale snpérieure)

$\rhd$ **Solution.**

1. Il est nécessaire que m soit une puissance de 2. En effet, si ce n'est pas le cas on peut écrire $m = 2^\alpha k$ avec $k \geqslant 3$ impair et on a la factorisation suivante :

$$2^m + 1 = 2^{2^\alpha k} + 1 = (2^{2^\alpha})^k + 1 = (2^{2^\alpha} + 1)\left(\sum_{i=1}^{k-1} (2^{2^\alpha})^{k-i}(-1)^{i-1}\right)$$

de sorte que $2^n + 1 = (2^{2^\alpha})^m + 1$ est divisible par $2^{2^\alpha} + 1$ et n'est donc pas premier.

2. On observe que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ sont bien des nombres premiers. On va montrer que F_5 est divisible par 641, donc non premier. Le très joli calcul qui suit est dû à Euler. On a $641 = 2^4 + 5^4 = 1 + 5 \times 2^7$ de sorte que $5 \times 2^7 \equiv -1\ [641]$. Élevons cette congruence à la puissance 4 : $5^4 \times 2^{28} \equiv 1\ [641]$. Comme, $641 = 5^4 + 2^4$ on a $5^4 \equiv -2^4\ [641]$ et donc $2^{32} \equiv -1\ [641]$. C'est le résultat voulu.

On a, plus précisément, $F_5 = 641 \times 6700417$.

3. Sans perte de généralité, on peut poser $m = n + k$ avec $k \geqslant 1$. On remarque alors que F_n divise $F_m - 2 = (2^{2^n})^{2^k} - 1$. Si p est un diviseur premier commun à F_n et F_m il en résulte que p doit diviser 2, *i.e.* être égal à 2. Or les nombres de Fermat sont impairs. Ils sont donc premiers entre eux deux à deux. Comme chaque F_n a au moins un diviseur premier, on en déduit qu'il existe une infinité de nombres premiers.

4. Soit p un diviseur premier de F_n. On se place dans $G = (\mathbb{Z}/p\mathbb{Z})^*$, groupe multiplicatif de cardinal $p - 1$. Comme p est impair, $\overline{2} \in G$. On a : $\overline{2}^{2^n} = -\overline{1}$. En élevant cette égalité au carré, il vient : $\overline{2}^{2^{n+1}} = \overline{1}$. L'ordre de $\overline{2}$ dans G est donc un diviseur de 2^{n+1}, *i.e.* une puissance de 2. Cependant, si cet ordre valait 2^k avec $k < n + 1$ on aurait : $\overline{2}^{2^n} = \overline{1}$. Ce qui n'est pas ! Donc l'ordre de $\overline{2}$ est exactement 2^{n+1}. Cet ordre est un diviseur du cardinal de G, c'est-à-dire de $p-1$. Le résultat en découle. Pour $n = 5$ on doit avoir $p \equiv 1$ [64]. On teste donc les nombres premiers parmi 65, 129, 193, 257, 321, 385, 449, 513, 577, 641,... Après 193, 257, 449 et 577, on en vient très vite à essayer 641. $\lhd$

Le résultat de la question 4 est du à Lucas. Fermat avait conjecturé la primalité de F_n *pour tout* n*, conjecture invalidée par Euler. En fait, on ne connaît pas d'autres* F_n *premiers que ceux vus ci-dessus. A l'heure actuelle (2007) on sait que* F_n *est composé pour* $5 \leqslant n \leqslant 30$ *et on connaît sa factorisation pour* $5 \leqslant n \leqslant 11$*. En revanche on ne dispose d'aucun facteur premier pour* F_{14}*,* F_{20}*,* F_{22} *et* F_{24}*. On conjecture actuellement qu'il n'y a qu'un nombre fini de* F_n *premiers.*

À la suite de Pierre de Fermat, la communauté mathématique montre un fort intérêt pour les nombres premiers. Euclide savait déjà qu'il y en a une infinité (sa preuve est celle proposée dans l'exercice suivant). Le XIXe *siècle aura été marqué par une concentration des efforts des mathématiciens en vue de démontrer le théorème des nombres premiers, conjecturé par Gauss : si* $\pi(n)$ *désigne le nombre d'entiers premiers inférieurs ou égaux à* n*, alors*

$$\pi(n) \underset{n\to+\infty}{\sim} \frac{n}{\ln n}.$$

On notera la raréfaction des nombres premiers à l'infini puisque $\lim\limits_{n\to\infty} \dfrac{\pi(n)}{n} = 0$*. Si les travaux de Tchebychev et Riemann furent déterminants, c'est seulement en 1896 que de la Vallée-Poussin et Hadamard de manière séparée viennent à bout de la conjecture.*

Trouver des nombres premiers nouveaux est une activité qui n'intéresse pas seulement les mathématiciens. Les grands nombres premiers

sont utilisés dans certains algorithmes de cryptage des données. Beaucoup de grands nombres premiers connus sont des nombres de Mersenne $M_p = 2^p - 1$ *où p est premier (si $a^n - 1$ est premier, $a = 2$ et n est premier). En 1644, Mersenne affirma que M_p était premier pour $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ et composé pour les autres valeurs de p premier inférieures à 257. Mais en 1806, Pervasin et Seelhoff démontrèrent que M_{61} était premier. En 1876, Lucas établit un méthode efficace pour tester la primalité des M_p (et prouva ainsi que M_{127} était premier). En septembre 2006 le 44-ième nombre de Mersenne premier a été découvert : il s'agit de $M_{32582657}$ et il possède* 9808358 *chiffres.*

4.17. Infinité des nombres premiers congrus à 3 modulo 4

Montrer que l'ensemble $\mathcal{P}$ des nombres premiers est infini. Montrer qu'il en est de même de l'ensemble des nombres premiers congrus à 3 modulo 4.

(École polytechnique)

▷ **Solution.**

• Raisonnons par l'absurde et supposons qu'il n'existe qu'un nombre fini de nombres premiers. Notons-les $p_1, p_2, \ldots, p_n$. Considérons l'entier $N = p_1 p_2 \ldots p_n + 1$. Comme N est strictement supérieur à 1, il possède un diviseur premier p_k. Dans ces conditions, p_k divise $N - p_1 p_2 \ldots p_n = 1$, ce qui est impossible. Donc $\mathcal{P}$ est infini.

• Pour montrer qu'il existe une infinité de nombres premiers congrus à 3 modulo 4, raisonnons de nouveau par l'absurde et supposons qu'il n'en existe qu'un nombre fini n. Notons-les $p_1, p_2, \ldots, p_n$. Considérons cette fois l'entier $N = 4p_1 p_2 \ldots p_n - 1 \geqslant 2$.

Aucun des p_k ne divise N, sinon il diviserait 1. Comme N est impair, tout diviseur premier de N ($N > 1$) est impair et n'est pas congru à 3 modulo 4 d'après ce qui précède ; il est donc congru à 1 modulo 4 et N est donc lui-même congru à 1 modulo 4. Or, manifestement, N est congru à 3 modulo 4. C'est la contradiction cherchée.

Conclusion. L'ensemble des nombres premiers congrus à 3 modulo 4 est infini. ◁

Ce dernier résultat est en fait un cas particulier du théorème de la progression arithmétique de Dirichlet qui affirme l'existence d'une infinité de nombres premiers de la forme $an + b$ lorsque a et b sont premiers entre eux. La preuve de ce théorème a fait l'objet du problème de six heures posé en 1993 aux ENS. L'exercice suivant traite le cas où $b = 1$.

4.18. Version faible du théorème de la progression arithmétique de Dirichlet (1837)

On note $\Phi_1 = X - 1$ et pour $n \geqslant 2$, $\Phi_n = \prod_{\substack{1 \leqslant k \leqslant n \\ \mathrm{pgcd}(k,n)=1}} \left(X - e^{\frac{2ik\pi}{n}}\right)$, le n-ième polynôme cyclotomique.

1. Montrer que Φ_n est à coefficients entiers pour tout $n \in \mathbb{N}^*$.

2. Que peut-on dire d'un nombre premier p qui divise $\Phi_n(a)$, où $a \in \mathbb{Z}$, mais aucun des $\Phi_d(a)$, où d décrit l'ensemble des diviseurs stricts de n ?

3. En déduire que pour $n \geqslant 1$ fixé, il existe une infinité de nombres premiers de la forme $\lambda n + 1$ avec λ entier.

(École normale supérieure)

▷ **Solution.**

1. • Montrons que $X^n - 1 = \prod_{d|n} \Phi_d$. On sait que $X^n - 1 = \prod_{\ell=1}^{n} \left(X - e^{\frac{2i\ell\pi}{n}}\right)$. Notons pour $d \geqslant 1$, P_d l'ensemble des racines primitives d-ièmes de l'unité et U_d l'ensemble des racines d-ièmes de l'unité. On a, par définition, $\Phi_n = \prod_{\xi \in P_n} (X - \xi)$. Si $\xi \in U_n$, l'ordre de ξ est un diviseur d de n et alors $\xi \in P_d$. Par conséquent, U_n est réunion disjointe des P_d pour d divisant n. D'où il résulte

$$X^n - 1 = \prod_{\xi \in U_n} (X - \xi) = \prod_{d|n} \left(\prod_{\xi \in P_d} (X - \xi) \right) = \prod_{d|n} \Phi_d.$$

On obtient le résultat voulu

$$\boxed{X^n - 1 = \prod_{d|n} \Phi_d}.$$

On retrouve ainsi un résultat classique sur l'indicatrice d'Euler φ : pour tout entier $n \geqslant 1$, $\varphi(n)$ est le degré de Φ_n i.e. le nombre d'entiers k compris entre 1 et n, premiers avec n. En considérant les degrés, l'identité précédente donne

$$\boxed{n = \sum_{d|n} \varphi(d)}.$$

• Nous allons établir que Φ_n est à coefficients entiers par récurrence sur $n \geqslant 1$ en utilisant le résultat suivant :

Lemme. *Soit* A *et* B *deux polynômes à coefficients entiers,* B *étant non nul unitaire. Alors* Q *et* R, *le quotient et le reste de la division euclidienne de* A *par* B *dans* $\mathbb{C}[X]$ *sont aussi à coefficients entiers.*

Démonstration. Le détail de la démonstration est laissé au lecteur ; on peut l'obtenir par une récurrence sur le degré de A (comme pour la division dans $K[X]$ avec K corps) ou bien en constatant que dans les opérations de l'algorithme de division euclidienne, seuls des entiers interviennent.

Établissons maintenant par récurrence sur n que Φ_n est à coefficients entiers.

$*$ C'est vrai, par définition, si $n = 1$.

$*$ Si $n \geqslant 2$, Φ_n est le quotient dans $\mathbb{C}[X]$ de $X^n - 1$ par B, où B est égal au produit des Φ_d, où d est un diviseur strict de n. Si on suppose la propriété vraie pour les entiers $\leqslant n-1$, chacun de ces Φ_d est à coefficients entiers et unitaires par définition, donc B est aussi à coefficients entiers et unitaire. En vertu du lemme, Φ_n est à coefficients entiers.

2. Soit p premier vérifiant l'hypothèse. Comme p divise $\Phi_n(a)$, il divise aussi a^n-1. Ainsi, l'ordre de $\overline{a}$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ divise n. Montrons que cet ordre est exactement n. Si d divise n, $d < n$, on a dans $\mathbb{Z}/p\mathbb{Z}$

$$\overline{a}^d - 1 = \prod_{d'|d} \overline{\Phi_{d'}(a)}.$$

Or si d' divise d, d' divise aussi n et par hypothèse, $\overline{\Phi_{d'}(a)} \neq 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, le produit de ces éléments non nuls est également non nul, si bien que $\overline{a}^d \neq 1$. L'ordre de $\overline{a}$ est donc n. Comme cet ordre divise $p-1$ d'après le théorème de Lagrange, p est de la forme $\lambda n + 1$ avec λ entier.

3. Raisonnons par l'absurde et supposons qu'il n'existe qu'un nombre fini d'entiers premiers congrus à 1 modulo n, soit $p_1, \ldots, p_q$. La question précédente, si on arrive à trouver a et p vérifiant les hypothèses, assure que p est congru à 1 modulo n. Ce sera insuffisant pour aboutir à une contradiction, p pouvant être alors un des p_i. Pour éviter cela, on va changer n en $N = np_1p_2\ldots p_q$. Si p est congru à 1 (mod N), p ne peut être un des p_i et pourtant, il est congru à 1 (mod n).

Il faut donc trouver $a \in \mathbb{Z}$ et p premier, tels que p divise $\Phi_N(a)$, mais aucun des $\Phi_d(a)$ pour $d|N$, $d < N$. On note $B = \prod_{d|, d<N} \Phi_d$. Le problème est donc de trouver $a \in \mathbb{Z}$ et p premier tels que p divise $\Phi_N(a)$ et ne divise pas $B(a)$.

Le polynôme B est premier avec Φ_N dans $\mathbb{C}[X]$ (en effet, ils sont scindés sur $\mathbb{C}$ et n'ont aucune racine commune), donc dans $\mathbb{Q}[X]$, puisque

ces polynômes sont à coefficients rationnels et que le pgcd est invariant par extension de corps (l'algorithme d'Euclide s'écrit de la même manière dans $\mathbb{C}[X]$ et dans $\mathbb{Q}[X]$).

D'après le théorème de Bezout, il existe donc $(U, V) \in \mathbb{Q}[X]^2$ tel que $1 = U\Phi_N + VB$. Il existe $a \in \mathbb{Z}$ tel que $U' = aU$ et $V' = aV$ appartiennent à $\mathbb{Z}[X]$ (il suffit de prendre un multiple du ppcm des dénominateurs des coefficients qui apparaissent dans U et V). Comme $\Phi_N \neq 0$ et $\Phi_N \neq \pm 1$, on peut même choisir a tel que $\Phi_N(a) \neq 0$ et $\Phi_N(a) \neq \pm 1$, étant donnée l'infinité de $a \in \mathbb{Z}$ vérifiant $aU \in \mathbb{Z}[X]$ et $aV \in \mathbb{Z}[X]$ (ceci en vue d'avoir des nombres premiers qui divisent $\Phi_N(a)$). On a donc

$$a = U'\Phi_N + V'B \quad \text{et en particulier} \quad a = U'(a)\Phi_N(a) + V'(a)B(a). \quad (*)$$

Soit p un nombre premier divisant $\Phi_N(a)$. Alors p divise $a^N - 1$, car Φ_N divise $X^N - 1$ dans $\mathbb{Z}[X]$. Dans $\mathbb{Z}/p\mathbb{Z}$, $\overline{a}^N = 1$ et donc $\overline{a}$ est inversible, ce qui signifie que a est premier avec p. Si p divisait $B(a)$, il diviserait a, d'après $(*)$, ce qui est exclu.

On est donc dans les hypothèses de la question précédente : p est congru à 1 modulo N, et donc modulo n, avec p forcément distinct des p_i, pour $1 \leqslant i \leqslant q$. C'est la contradiction voulue. $\lhd$

4.19. Plus petit nombre premier ne divisant pas n

1. Montrer que tout entier $n > 6$ s'écrit comme somme de deux entiers premiers entre eux, strictement supérieurs à 1.

2. Soit $(p_n)_{n \geqslant 1}$ la suite strictement croissante des nombres premiers. Montrer que pour tout $k > 2$, on a $p_{k+1} + p_{k+2} \leqslant p_1 p_2 \cdots p_k$.

3. Pour $n \in \mathbb{N}^*$, on note q_n le plus petit nombre premier ne divisant pas n. Montrer que la suite $\dfrac{q_n}{n}$ tend vers 0.

(École normale supérieure)

$\rhd$ **Solution.**

1. Si n est impair, on peut écrire $n = 2 + (n-2)$ et $\text{pgcd}(2, n-2) = 1$.

Si $n \equiv 0 \pmod 4$, il s'écrit $n = 4k$ avec $k \geqslant 2$. Alors la décomposition $n = (2k-1) + (2k+1)$ convient.

Enfin, si $n \equiv 2 \pmod 4$, il s'écrit $n = 4k + 2$ avec $k \geqslant 2$. Alors la décomposition $n = (2k+3) + (2k-1)$ est aussi du type souhaité (si p premier divise $2k+3$ et $2k-1$ il divise la différence c'est-à-dire 4, ce qui est impossible, car les entiers sont impairs).

Par contre, $6 = 2 + 4 = 3 + 3$ n'a pas de décomposition de ce type.

2. Pour $k = 3$ on a $p_1 p_2 p_3 = 2 \times 3 \times 5 = 30$ et $p_4 + p_5 = 7 + 11 = 18$.

Posons, pour $k \geqslant 3$, $n = p_1 p_2 \ldots p_k$. Comme $n > 6$, on peut l'écrire sous la forme $n = a + b$, $a > 1$, $b > 1$, $a \wedge b = 1$. Aucun des nombres p_i,

où $1 \leqslant i \leqslant k$, ne peut diviser a (car il diviserait aussi b). Les facteurs premiers de a sont donc supérieurs ou égaux à p_{k+1}. De même pour b. Or, a et b sont premiers entre eux et n'ont donc aucun diviseur premier commun. Il en résulte que $n = a + b \geqslant p_{k+1} + p_{k+2}$.

3. Pour $n \geqslant 2$, on note k_n l'unique entier tel que

$$p_1 p_2 \cdots p_{k_n} \leqslant n < p_1 p_2 \cdots p_{k_n+1}.$$

Il est alors évident que $q_n \leqslant p_{k_n+1}$. Ainsi, on a pour $n \geqslant 2 \cdot 3 \cdot 5 \cdot 7 = 210$,

$$\frac{q_n}{n} \leqslant \frac{p_{k_n+1}}{p_1 p_2 \cdots p_{k_n}} \leqslant \frac{1}{p_{k_n}},$$

la dernière inégalité résultant de la question 2 :

$$p_{k+1} < p_{k_n+1} + p_{k_n} \leqslant p_1 \cdots p_{k_n-1}$$

pour $k_n \geqslant 4$, c'est-à-dire pour $n \geqslant 210$. Comme k_n tend vers l'infini lorsque n tend vers l'infini, le résultat est prouvé. $\lhd$

Les exercices suivants sont centrés sur la factorialité de $\mathbb{Z}$: tout entier $n \geqslant 2$ s'écrit de manière unique (à l'ordre des facteurs près) sous la forme $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ où $p_1, \ldots, p_k$ sont des nombres premiers deux à deux distincts et $\alpha_1, \ldots, \alpha_k$ des entiers naturels non nuls.

4.20. Théorème de Kurschak (1918)

Pour quelles valeurs entières $n \geqslant m$ a-t-on $\sum_{i=m}^{n} \frac{1}{i} \in \mathbb{N}$?

(École normale supérieure)

$\rhd$ **Solution.**

On obtient un entier pour $n = m = 1$ et on va voir que c'est le seul cas. Supposons $n \geqslant 2$. L'idée consiste à regarder la valuation 2-adique des entiers entre m et n. On peut supposer $m < n$ car $\frac{1}{n}$ n'est pas entier pour $n \geqslant 2$. Soit $\alpha = \max\{\nu_2(k),\ m \leqslant k \leqslant n\}$. On a $\alpha \geqslant 1$, car il y a au moins un entier pair entre m et n. En fait, le point essentiel est que la valuation 2-adique maximale α n'est atteinte qu'une et une seule fois. En effet, supposons qu'il existe deux entiers k, k' avec $m \leqslant k < k' \leqslant n$ et $k = 2^\alpha(2r+1)$, $k' = 2^\alpha(2s+1)$. Alors $2^\alpha(2r+2) = 2^{\alpha+1}(r+1)$ appartient à $[\![m, n]\!]$ et est de valuation 2-adique supérieure ou égale à $\alpha + 1$ ce qui contredit la définition de α. Il en résulte que le représentant irréductible de la somme $\sum_{i=m}^{n} \frac{1}{i}$ est de la forme $\frac{\mathrm{A}}{2^\alpha \mathrm{B}}$ où A, B sont impairs. Ce qui prouve que la somme en question n'est pas un entier. $\lhd$

Le résultat a d'abord été prouvé en 1915 par Taeisinger dans le cas $m = 1$ et généralisé en 1918 par Kurschak. En 1932, le célèbre Paul Erdös a prouvé que le résultat se généralise pour des entiers formant une progression arithmétique quelconque.

4.21. Théorème de Legendre (1808)

Soit n un entier supérieur à 2 et p un nombre premier. Montrer que la valuation p-adique de $n!$ est égale à $\sum_{k=1}^{+\infty} \mathrm{E}\left(\frac{n}{p^k}\right)$.

(École polytechnique)

▷ **Solution.**

Notons qu'en fait la somme considérée est finie. Parmi les entiers entre 1 à n, le nombre de multiples de p qui ne sont pas multiples de p^2 est $\mathrm{E}\left(\frac{n}{p}\right) - \mathrm{E}\left(\frac{n}{p^2}\right)$. Chacun de ces entiers amène une contribution de 1 dans la valuation p-adique de $n!$. Le nombre de multiples de p^2 non multiples de p^3 est $\mathrm{E}\left(\frac{n}{p^2}\right) - \mathrm{E}\left(\frac{n}{p^3}\right)$. Chacun amène une contribution de 2. On continue ... Si on note q le plus grand entier tel que $p^q \leqslant n$, la valuation p-adique de $n!$ est donc

$$\nu_p(n!) = \sum_{k=1}^{q} k\left(\mathrm{E}\left(\frac{n}{p^k}\right) - \mathrm{E}\left(\frac{n}{p^{k+1}}\right)\right) = \sum_{k=1}^{q} \mathrm{E}\left(\frac{n}{p^k}\right) = \sum_{k=1}^{+\infty} \mathrm{E}\left(\frac{n}{p^k}\right).$$

C'est le résultat demandé. ◁

Ce calcul permet par exemple de déterminer le nombre de zéros placés à droite de l'écriture décimale de $\mathrm{N} = 2007!$. *Il s'agit de trouver la plus grande puissance de* 10 *qui divise cet entier. Comme* $\nu_5(\mathrm{N}) \leqslant \nu_2(\mathrm{N})$ *le nombre cherché est égal à la valuation* 5*-adique de* 2007!. *Elle vaut*

$$\mathrm{E}\left(\frac{2007}{5}\right) + \mathrm{E}\left(\frac{2007}{25}\right) + \mathrm{E}\left(\frac{2007}{125}\right) + \mathrm{E}\left(\frac{2007}{625}\right) = 500.$$

4.22. Un produit de trois entiers consécutifs n'est jamais une puissance k-ième

Soit $k \geqslant 2$. Montrer que le produit de trois entiers naturels non nuls consécutifs ne peut pas être une puissance k-ième.

(École normale supérieure)

▷ **Solution.**

On cherche à montrer que l'équation $n(n+1)(n+2) = x^k$ n'a pas de solution non nulle. Mieux vaut écrire cette équation sous la forme plus symétrique $(n-1)n(n+1) = x^k$. Supposons par l'absurde qu'il existe une solution (x, n) avec $n \geqslant 2$. Les entiers n et $n^2 - 1$ sont premiers entre eux. Or on a le résultat essentiel suivant, conséquence de la factorialité de $\mathbb{Z}$:

Lemme. *Soit a et b deux entiers naturels non nuls premiers entre eux, $k \geqslant 2$. On suppose qu'il existe $c \in \mathbb{N}$ tel que $ab = c^k$. Alors a et b sont eux aussi des puissances k-ièmes.*

Démonstration.

Écrivons la décomposition de a, b et c en produit de facteurs premiers :

$$a = \prod_{p \text{ premier}} p^{\alpha_p}, \quad b = \prod_{p \text{ premier}} p^{\beta_p}, \quad c = \prod_{p \text{ premier}} p^{\gamma_p},$$

où les α_p, β_p et γ_p sont des familles d'entiers à support fini. Comme $ab = c^k$, on obtient, par unicité de la décomposition, $\alpha_p + \beta_p = k\gamma_p$ pour tout p premier. Puisque a et b sont premiers entre eux, on a $\alpha_p\beta_p = 0$ pour tout p. Il en résulte que pour tout p premier α_p et β_p sont divisibles par k. Ainsi a et b sont des puissances k-ièmes. ◇

Il existe d'après le lemme y et z dans $\mathbb{N}^*$ tels que $n = y^k$ et $n^2 - 1 = z^k$. D'où $y^{2k} - z^k = 1$. Or deux puissances k-ièmes non nulles consécutives diffèrent au moins de k puisque, pour $u \geqslant 1$, $(u+1)^k - u^k \geqslant ku \geqslant k \geqslant 2$. La relation $(y^2)^k - z^k = 1$ implique donc $z = 0$ et $y = 1$, d'où $n = 1$. Il n'y a donc pas de solution avec $n \geqslant 2$. ◁

Erdös et Selfridge ont démontré en 1975 une conjecture vieille de plus de 150 ans : pour tout $m \geqslant 2$, un produit de m entiers consécutifs n'est jamais une puissance k-ième[2].

4.23. Théorème de Palfy-Erdös

Pour tout $x \in \mathbb{Z}$ et tout premier p, on note x_p le résidu de x modulo p. Soit a et b deux entiers positifs tels que pour tout p premier, $a_p \leqslant b_p$.

1. Montrer que $a \leqslant b$.

2. ERDÖS (P.) & SELFRIDGE (J.L.), *The product of consecutive integers is never a power*, Illinois J. of Math. 19, 1975, p. 292-301.

On désire montrer que $a = b$. Raisonnons par l'absurde et supposons $a < b$. On note $A = 1 \cdot 2 \ldots (a-1)a$ et $B = (b-a+1) \ldots (b-1)b$. Pour p premier et $k \geqslant 1$, on note $r(p^k)$ (resp. $s(p^k)$) le nombre de facteurs de A (resp. B) divisibles par p^k.

2. Montrer que $s(p^k)$ est égal à $r(p^k)$ ou $r(p^k) + 1$.

3. Montrer en utilisant l'hypothèse que $r(p) = s(p)$. En déduire que si $p > a$, alors $r(p^k) = s(p^k) = 0$.

4. On note $t(p)$ le plus grand entier k tel que $s(p^k) > 0$. Prouver que $C_b^a = \dfrac{B}{A}$ divise $\prod\limits_{p \leqslant a} p^{t(p)-1}$ et en déduire que

$$\frac{(b-a+1)\ldots(b-1)b}{\prod\limits_{p \leqslant a} p^{t(p)}} \text{ divise } \frac{1.2\ldots(a-1)a}{\prod\limits_{p \leqslant a} p}.$$

5. On suppose de plus $a \leqslant \dfrac{b}{2}$. Aboutir à une contradiction.

6. Prouver, en utilisant 5, que l'on aboutit également à une contradiction si $\dfrac{b}{2} < a < b$.

(École normale supérieure)

1 · **Solution.**

1. Soit p premier, $p > a$ et $p > b$. Alors on a $a = a_p \leqslant b_p = b$.

2. L'entier $r(p^k)$ est le nombre d'entiers d vérifiant $1 \leqslant dp^k \leqslant a$. Il en résulte que $r(p^k) = E\left(\dfrac{a}{p^k}\right)$ et $\dfrac{a}{p^k} - 1 < r(p^k) \leqslant \dfrac{a}{p^k}$. On peut écrire, d'autre part,

$$s(p^k) = \text{Card}\{d \in \mathbb{N}, b - a < dp^k \leqslant b\} = \text{Card}\left\{d \in \mathbb{N}, \frac{b-a}{p^k} < d \leqslant \frac{b}{p^k}\right\}$$
$$= E\left(\frac{b}{p^k}\right) - E\left(\frac{b-a}{p^k}\right).$$

Encadrons $s(p^k)$:

$$\begin{aligned} \frac{b}{p^k} - 1 - \frac{b-a}{p^k} < \quad & s(p^k) \quad < \frac{b}{p^k} - \left(\frac{b-a}{p^k} - 1\right), \\ \frac{a}{p^k} - 1 < \quad & s(p^k) \quad < \frac{a}{p^k} + 1, \\ r(p^k) - 1 < \quad & s(p^k) \quad < r(p^k) + 2. \end{aligned}$$

Comme dans cette dernière inégalité, il ne figure que des entiers, $s(p^k)$ vaut $r(p^k)$ ou $r(p^k) + 1$.

3. Considérons maintenant les deux suites finies $S_1' = (a, a-1, \ldots, 1)$ et $S_2' = (b, b-1, \ldots, b-a+1)$. Le premier multiple de p dans S_1' est $a - a_p$ et le premier multiple de p dans S_2' est $b - b_p$. Donc, comme $a_p \leqslant b_p$, celui de S_1', qui est le (a_p+1)-ième terme de la suite S_1' arrive avant ou en même temps que celui de S_2', qui est le (b_p+1)-ième terme de la suite S_2'. Les deux suites étant de même longueur, cela entraîne $r(p) \geqslant s(p)$ et finalement $r(p) = s(p)$, en utilisant la question précédente.

Ainsi, si $p > a$, $r(p)$ est nul et donc $s(p)$ aussi. Donc aucun facteur de A et de B n'est divisible par p. Il s'ensuit que $r(p^k) = s(p^k) = 0$ pour tout $k \geqslant 1$.

4. On peut écrire

$$\mathrm{A} = \prod_{p \text{ premier}} p^{\sum_{k=1}^{\infty} r(p^k)} \quad \text{et } \mathrm{B} = \prod_{p \text{ premier}} p^{\sum_{k=1}^{\infty} s(p^k)}$$

et même, compte tenu de la question précédente,

$$\mathrm{A} = \prod_{p \leqslant a} p^{\sum_{k=1}^{\infty} r(p^k)} \quad \text{et } \mathrm{B} = \prod_{p \leqslant a} p^{\sum_{k=1}^{\infty} s(p^k)},$$

p en indice désignant toujours un nombre premier. On en déduit que

$$\mathrm{C}_b^a = \frac{\mathrm{B}}{\mathrm{A}} = \prod_{p \leqslant a} p^{\sum_{k=1}^{\infty} s(p^k) - r(p^k)}.$$

De la question 3, on déduit l'égalité

$$\sum_{k=1}^{\infty} s(p^k) - r(p^k) = \sum_{k=2}^{\infty} s(p^k) - r(p^k).$$

Si $k > t(p)$, on a $0 = s(p^k) \geqslant r(p^k)$ et $r(p^k) = 0$. La somme devient donc

$$\sum_{k=1}^{\infty} s(p^k) - r(p^k) = \sum_{k=2}^{t(p)} s(p^k) - r(p^k) \leqslant \sum_{k=2}^{t(p)} 1 = t(p) - 1,$$

la dernière inégalité résultant de la question 2. Par conséquent, l'entier $\dfrac{\mathrm{B}}{\mathrm{A}}$ divise $\prod_{p \leqslant a} p^{t(p)-1}$. Il existe donc $\lambda \in \mathbb{N}$ tel que

$$\lambda \frac{\mathrm{B}}{\mathrm{A}} = \prod_{p \leqslant a} p^{t(p)-1} \quad \text{c'est-à-dire } \lambda \left(\frac{\mathrm{B}}{\prod_{p \leqslant a} p^{t(p)}} \right) = \frac{\mathrm{A}}{\prod_{p \leqslant a} p}.$$

Mais $\dfrac{B}{\prod\limits_{p\leqslant a} p^{t(p)}}$ et $\dfrac{A}{\prod\limits_{p\leqslant a} p}$ sont des entiers (car $p^{t(p)}$ divise l'un des facteurs de B, pour tout p). On est donc en droit d'écrire que

$$\frac{(b-a+1)\dots(b-1)b}{\prod\limits_{p\leqslant a} p^{t(p)}} \text{ divise } \frac{1.2\dots(a-1)a}{\prod\limits_{p\leqslant a} p}.$$

5. On note $\pi(a)$ le nombre d'entiers premiers inférieurs ou égaux à a. Considérons le terme de droite dans la relation ci-dessus $\dfrac{1.2\dots(a-1)a}{\prod\limits_{p\leqslant a} p}$. Après simplification, on obtient un produit de $a-\pi(a)$ facteurs tous inférieurs ou égaux à a. De même, après simplification, le terme de gauche de la relation $\dfrac{(b-a+1)\dots(b-1)b}{\prod\limits_{p\leqslant a} p^{t(p)}}$ «contient» $a-\pi(a)$ facteurs supérieurs ou égaux à $b-a+1$ (tous les termes du numérateur qui ne sont pas divisible par un $p^{t(p)}$) avec, par hypothèse, $b-a+1 \geqslant 2a-a+1 > a$. On en déduit que

$$\frac{(b-a+1)\dots(b-1)b}{\prod\limits_{p\leqslant a} p^{t(p)}} > a^{a-\pi(a)} \geqslant \frac{1.2\dots(a-1)a}{\prod\limits_{p\leqslant a} p},$$

ce qui est manifestement contradictoire avec le résultat de la question 4.

6. Supposons $\dfrac{b}{2} < a < b$ et posons $c = b-a$. On a $0 < c < \dfrac{b}{2}$. On obtient, pour tout p premier, $c \equiv b_p - a_p\ [p]$ et $0 \leqslant b_p - a_p < p$ et donc $c_p = b_p - a_p \leqslant b_p$. Ceci est impossible d'après 5. On conclut donc que nécessairement $a = b$. $\lhd$

Les exercices suivants sont consacrés aux propriétés arithmétiques des coefficients binomiaux.

4.24. Valuation p-adique de $C_{p^n}^k$

> Soit p un nombre premier, $n \in \mathbb{N}^*$ et $k \in [\![1, p^n-1]\!]$. Quelle est la plus grande puissance de p qui divise $C_{p^n}^k$?
>
> **(École normale supérieure)**

1. **Solution.**

La question consiste à chercher la valuation p-adique de $C_{p^n}^k$. On écrit

$$k!C_{p^n}^k = p^n(p^n-1)(p^n-2)\dots(p^n-(k-1)).$$

On note ν_p la valuation p-adique. Pour tout entier $\lambda \in [\![1, k-1]\!]$, on a

$$\nu_p(p^n - \lambda) = \nu_p(\lambda),$$

car si $\lambda = p^\alpha u$ avec u non divisible par p et $\alpha < n$ (puisque $\lambda < p^n$), on a $p^n - \lambda = p^\alpha(p^{n-\alpha} - u)$ et $p^{n-\alpha} - u$ n'est pas divisible par p. En passant à la valuation dans l'égalité ci-dessus on obtient, puisque la valuation d'un produit est la somme des valuations des différents termes,

$$\nu_p(k!) + \nu_p(\mathrm{C}_{p^n}^k) = n + \nu_p((k-1)!)$$

et finalement

$$\boxed{\nu_p(\mathrm{C}_{p^n}^k) = n - \nu_p(k)}. \lhd$$

L'énoncé suivant regroupe trois exercices posés indépendamment.

4.25. Congruences de Lucas (1878)

Soit p un nombre premier et n, k des entiers naturels.

1. On suppose $n \geqslant 2$. Montrer l'équivalence entre les assertions suivantes :

(i) n est premier ;

(ii) $\forall i \in [\![1, n-1]\!]$, n divise C_n^i.

2. On écrit n et k en base p : $n = n_0 + n_1 p + \cdots + n_j p^j$ et $k = k_0 + k_1 p + \cdots + k_j p^j$ (avec le même indice j quitte à compléter avec des zéros). Établir le théorème de Lucas :

$$\mathrm{C}_n^k \equiv \mathrm{C}_{n_0}^{k_0} \mathrm{C}_{n_1}^{k_1} \ldots \mathrm{C}_{n_j}^{k_j} \pmod{p}.$$

(avec la convention habituelle que $\mathrm{C}_n^k = 0$ si $k > n$).

3. Montrer que le nombre d_n de coefficients binomiaux impairs sur la n-ième ligne du triangle de Pascal (c'est-à-dire parmi les C_n^k, $0 \leqslant k \leqslant n$) est une puissance de 2.

(École normale supérieure)

$\rhd$ **Solution.**

1. Supposons n premier. On a pour tout $i \in [\![1, n-1]\!]$, $i\mathrm{C}_n^i = n\mathrm{C}_{n-1}^{i-1}$. Il en résulte que n divise $i\mathrm{C}_n^i$. Par le lemme de Gauss, n divise i ou n divise C_n^i. Le premier cas étant visiblement exclu, l'assertion (ii) est prouvée.

Réciproquement, supposons que (ii) est vérifiée. Soit d un diviseur positif de n. On a comme ci-dessus, $\mathrm{C}_n^d = \dfrac{n}{d}\mathrm{C}_{n-1}^{d-1} \equiv 0 \pmod{n}$. Cela invite à regarder le résidu des C_{n-1}^i modulo n. On obtient, pour $i = 1$,

$C_{n-1}^{i} = n-1 \equiv -1 \pmod{n}$ et la formule de Pascal, $C_{n-1}^{i}+C_{n-1}^{i+1} = C_n^{i+1}$ pour $1 \leqslant i \leqslant n-2$, donne $C_{n-1}^{i+1} \equiv -C_{n-1}^{i} \pmod{n}$, compte-tenu de (*ii*). Il en résulte que pour tout $i \in [\![1, n-1]\!]$, on a $C_{n-1}^{i} \equiv (-1)^i \pmod{n}$ et donc $\dfrac{n}{d} C_{n-1}^{d-1} \equiv \dfrac{n}{d}(-1)^d \equiv 0 \pmod{n}$, ce qui n'est possible que si $d = 1$. L'entier n est donc premier.

2. Il résulte de la question 1 et de la formule du binôme de Newton que $(1+X)^p = 1 + X^p$ dans $(\mathbb{Z}/p\mathbb{Z})[X]$. Pour $a \in \mathbb{N}$, $a < p$, on a donc dans $(\mathbb{Z}/p\mathbb{Z})[X]$,

$$(1+X)^{np+a} = (1+X^p)^n(1+X)^a.$$

Si $b \in \mathbb{N}$, $b < p$, on obtient, en identifiant les coefficients de X^{kp+b} dans les deux expressions de ce polynôme, la congruence

$$C_{np+a}^{kp+b} \equiv C_n^k C_a^b \pmod{p},$$

ceci étant valable même si $k > n$ ou $b > a$, avec la convention indiquée dans l'énoncé. En opérant la division euclidienne de n (resp. k) par p, on peut écrire $n = n_0 + pq$ et $k = k_0 + pq'$ avec $(q, q') \in \mathbb{N}^*$. La formule précédente donne

$$C_n^k \equiv C_{n_0}^{k_0} C_q^{q'} \pmod{p}.$$

On réitère le même procédé en divisant q et q' par p, ce qui fait apparaître comme restes n_1 et k_1 et, de proche en proche, après j itérations, on obtient

$$C_n^k \equiv C_{n_0}^{k_0} C_{n_1}^{k_1} \dots C_{n_j}^{k_j} \pmod{p}.$$

3. Soit $k \in [\![0, n]\!]$. Écrivons n et k en base 2 : $n = n_0 + 2n_1 + \dots + 2^j n_j$ et $k = k_0 + 2k_1 + \dots + 2^j k_j$, où $n_i, k_j \in \{0, 1\}$ pour tout $0 \leqslant i \leqslant j$. Puisque, d'après la question 2, on a $C_n^k \equiv C_{n_0}^{k_0} C_{n_1}^{k_1} \dots C_{n_j}^{k_j} \pmod{2}$, pour que C_n^k soit impair, *i.e.* $C_n^k \equiv 1 \pmod{2}$, il faut et il suffit que $C_{n_i}^{k_i} \equiv 1 \pmod{2}$ pour tout i. C'est le cas si, et seulement si, $0 \leqslant k_i \leqslant n_i$ pour tout i.

On obtient donc $d_n = (n_0+1)(n_1+1)\dots(n_j+1) = 2^{c_n}$, où c_n est le nombre de chiffres 1 dans l'écriture binaire de n. Par exemple, si n est une puissance de 2, il n'y a que 2 coefficients binomiaux impairs sur la n-ième ligne du triangle de Pascal (les extrémités, évidemment). ◁

4.26. Un problème de congruence

Soit p premier. Montrer que $\displaystyle\sum_{k=0}^{p} C_p^k C_{p+k}^k \equiv 2^p + 1 \pmod{p^2}$.

(École polytechnique)

▷ **Solution.**

Posons $S_p = \sum_{k=0}^{p} C_p^k C_{p+k}^k$. Il est classique que $C_p^k \equiv 0 \pmod p$ pour tout $k \in [\![1, p-1]\!]$ (le lecteur trouvera ce résultat dans la question 1 de l'exercice précédent). Étudions le résidu modulo p de C_{p+k}^k. On a, pour tout $k \in [\![1, p-1]\!]$,

$$k!C_{p+k}^k = (p+k)(p+k-1)\dots(p+1) \equiv k! \pmod p.$$

Il en résulte que p divise $k!(C_{p+k}^k - 1)$ et comme $k!$ et p sont premiers entre eux, p divise $C_{p+k}^k - 1$. Ainsi p^2 divise $C_p^k(C_{p+k}^k - 1)$, ce qui équivaut à $C_p^k C_{p+k}^k \equiv C_p^k \pmod{p^2}$. On a donc

$$S_p \equiv 1 + C_{2p}^p + \sum_{k=1}^{p-1} C_p^k \equiv 1 + C_{2p}^p + 2^p - 2 \pmod{p^2},$$

la dernière congruence résultant de la formule du binôme de Newton.

Pour terminer, on est ramené à prouver que $C_{2p}^p \equiv 2 \pmod{p^2}$. Cela est vrai pour $p = 2$ puisque $C_4^2 = 6$. Dans la suite, on supposera que p est un nombre premier impair. On écrit

$$C_{2p}^p - 2 = \frac{(2p)(2p-1)\dots(p+1)}{p!} - 2 = \frac{2}{(p-1)!}\left(\prod_{k=1}^{p-1}(p+k) - (p-1)!\right)$$

Comme p est différent de 2 et est premier avec $(p-1)!$, il nous faut prouver que $\prod_{k=1}^{p-1}(p+k) - (p-1)! = Q(p) - (p-1)!$ (où $Q(X)$ est le polynôme $\prod_{k=1}^{p-1}(X+k) \in \mathbb{Z}[X]$) est divisible par p^2.

Si on écrit $Q(X) = X^{p-1} + a_{p-2}X^{p-2} + \dots + a_1X + a_0$, on a clairement $Q(p) \equiv a_0 + a_1 p \pmod{p^2}$. Comme $a_0 = (p-1)!$ il suffit donc de prouver que a_1 est nul modulo p. En notant $\overline{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$ la réduction modulo p de Q, on a

$$\overline{Q} = \prod_{k=1}^{p-1}(X + \overline{k}) = \prod_{k=1}^{p-1}(X - \overline{p-k}) = \prod_{k=1}^{p-1}(X - \overline{k}).$$

Les racines de $\overline{Q}$ sont donc exactement les éléments non nuls de $\mathbb{Z}/p\mathbb{Z}$ et ces racines sont simples. Le polynôme $X^{p-1} - \overline{1}$ a le même degré que $\overline{Q}$ et s'annule aussi en tout $\overline{k}$, pour $1 \leqslant k \leqslant p-1$, d'après le petit théorème de Fermat. Il est donc égal à $\overline{Q}$.

De l'égalité $\overline{Q} = X^{p-1} + \overline{a}_{p-2}X^{p-2} + \dots + \overline{a}_1 X + \overline{a_0} = X^{p-1} - \overline{1}$, on déduit $\overline{a}_1 = 0$, *i.e.* p divise a_1. ◁

4.27. Le problème de Ducci

Pour tout $n \in \mathbb{N}$, on écrit $n = \sum_{q=0}^{+\infty} \varepsilon_q(n) 2^q$ où pour tout $q \geqslant 0$, $\varepsilon_q(n) \in \{0,1\}$ et $\varepsilon_q(n)$ nul pour q assez grand : il s'agit de l'écriture de n en numération binaire.

1. Pour $n \geqslant 1$, on note $s(n) = \sum_{q=0}^{+\infty} \varepsilon_q(n)$ et $\nu(n)$ le plus petit entier q tel que $\varepsilon_q(n) = 1$. Montrer que $\nu(n) = 1 + s(n-1) - s(n)$, puis que $\nu(n!) = n - s(n)$.

2. Soit $r \geqslant 1$ et $\mathrm{D} : \mathbb{N}^r \to \mathbb{N}^r$ définie pour $(a_1, \ldots, a_r) \in \mathbb{N}^r$ par

$$\mathrm{D}(a_1, \ldots, a_r) = (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_{r-1} - a_r|, |a_r - a_1|).$$

Montrer qu'il y a équivalence entre :

(*i*) pour tout $a \in \mathbb{N}^r$, la suite $(\mathrm{D}^n(a))_{n \geqslant 0}$ stationne à 0 ;

(*ii*) r est une puissance de 2.

On pourra utiliser le $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/2\mathbb{Z})^r$.

(École normale supérieure)

Solution.

1. Si $n \in \mathbb{N}$, $s(n)$ désigne le nombre de 1 figurant dans l'écriture de n en base 2. Si $n \neq 0$, $\nu(n)$ désigne la valuation 2-adique de n, *i.e.* le plus grand entier k tel que 2^k divise n, ou encore l'exposant de 2 dans la décomposition de n en produit de facteurs premiers.

• Soit $n \geqslant 1$. Supposons que le chiffre des unités de $n-1$ soit 0. Alors celui de n est 1, les autres chiffres restant inchangés. On a dans ce cas $\nu(n) = 0$, $s(n) = s(n-1) + 1$; la relation $\nu(n) = 1 + s(n-1) - s(n)$ est vérifiée.

Supposons maintenant qu'il y ait r chiffres 1 à droite de l'écriture de $n-1$: $\varepsilon_q(n-1) = 1$ si $0 \leqslant q \leqslant r-1$ et $\varepsilon_r(n-1) = 0$. Alors, par le jeu des retenues, n va s'écrire avec r zéros à droite et un 1 ensuite : $\varepsilon_q(n) = 0$ si $0 \leqslant q \leqslant r-1$ et $\varepsilon_r(n) = 1$, les autres chiffres restant inchangés. Par exemple, en binaire $1011100111 + 1 = 1011101000$. Par conséquent, on a

$$s(n) = s(n-1) - r + 1 \quad \text{et} \quad \nu(n) = r = 1 + s(n-1) - s(n).$$

On conclut que pour tout $n \geqslant 1$, $\boxed{\nu(n) = r = 1 + s(n-1) - s(n)}$.

• Comme, pour $n \geqslant 1$, $\nu(n)$ est l'exposant de 2 dans la décomposition de n en facteurs premiers, on a, si $(a,b) \in \mathbb{N}^{*2}$, $\nu(ab) = \nu(a) + \nu(b)$. On en déduit que

$$\nu(n!) = \sum_{k=1}^{n} \nu(k) = \sum_{k=1}^{n} (1 + s(k-1) - s(k)) = n + s(0) - s(n),$$

$$\boxed{\nu(n!) = n - s(n)}.$$

2. • L'idée est de «plonger» le problème dans $\mathbb{Z}/2\mathbb{Z}$ pour le rendre linéaire. On introduit donc l'application linéaire $\delta : (\mathbb{Z}/2\mathbb{Z})^r \to (\mathbb{Z}/2\mathbb{Z})^r$ qui à $a = (a_1, \ldots, a_r)$ associe $\delta(a) = (a_1 + a_2, a_2 + a_3, \ldots, a_r + a_1)$. Si on note $\overline{a}$ le projeté dans $(\mathbb{Z}/2\mathbb{Z})^r$ d'un r-uplet $a = (a_1, \ldots, a_r) \in \mathbb{N}^r$ on a $\delta(\overline{a}) = \overline{\mathrm{D}(a)}$ puisque, quels que soient les entiers x et y, $|x-y|$ et $x+y$ ont même parité.

Montrons que la propriété (i) équivaut à dire que δ nilpotent.

⋆ Supposons (i). Pour tout $a \in \mathbb{N}^r$, si n est un entier naturel tel que $\mathrm{D}^n(a) = 0$, on obtient $\delta^n(\overline{a}) = \overline{\mathrm{D}^n(a)} = 0$. On applique ce résultat aux vecteurs $e_1, \ldots, e_r$ de la base canonique de $(\mathbb{Z}/2\mathbb{Z})^r$. Pour $1 \leqslant i \leqslant r$, il existe $n_i \in \mathbb{N}$ tel que $\delta^{n_i}(e_i) = 0$. Si p désigne le plus grand des n_i, on obtient $\delta^p = 0$, puisque cet endomorphisme est nul sur une base. L'endomorphisme δ est nilpotent.

⋆ Réciproquement, supposons δ nilpotent, d'indice de nilpotence k. Pour $\mathrm{X} = (a_1, \ldots, a_r) \in \mathbb{N}^r$, on pose $m(\mathrm{X}) = \max\limits_{1 \leqslant i \leqslant r} a_i$. Il est facile de voir que $m(\mathrm{D}(\mathrm{X})) \leqslant m(\mathrm{X})$. Si on fixe X, la suite $(m(\mathrm{D}^n(\mathrm{X})))$ est donc décroissante et le problème est de montrer qu'elle est stationnaire à 0. On a $\overline{\mathrm{D}^k(\mathrm{X})} = \delta^k(\mathrm{X}) = 0$, puisque $\delta^k = 0$. Tous les coefficients de $\mathrm{D}^k(\mathrm{X})$ sont donc pairs et on peut poser $\mathrm{D}^k(\mathrm{X}) = 2\mathrm{X}_1$. On a alors $m(\mathrm{X}_1) \leqslant \frac{1}{2} m(\mathrm{X})$. On reprend le raisonnement avec X_1 : $\mathrm{D}^k(\mathrm{X}_1)$ a tous ses coefficients pairs. On écrit $\mathrm{D}^k(\mathrm{X}_1) = 2\mathrm{X}_2$. Mais comme $\mathrm{D}(2\mathrm{X}) = 2\mathrm{D}(\mathrm{X})$, on a

$$\mathrm{D}^{2k}(\mathrm{X}) = 2\mathrm{D}^k(\mathrm{X}_1) = 4\mathrm{X}_2 \quad \text{et} \quad m(\mathrm{X}_2) \leqslant \frac{1}{2} m(\mathrm{X}_1) \leqslant \frac{1}{4} m(\mathrm{X}).$$

On itère ce raisonnement jusqu'à un indice p tel que

$$m(\mathrm{X}_p) \leqslant \frac{1}{2^p} m(\mathrm{X}) < 1.$$

On a alors $\mathrm{X}_p = 0$ et $\mathrm{D}^{pk}(\mathrm{X}) = 0$ La propriété (i) est vérifiée.

• Il faut maintenant démontrer que la propriété (ii) équivaut à δ nilpotent, c'est-à-dire à $\delta^r = 0$. En effet, l'espace vectoriel $(\mathbb{Z}/2\mathbb{Z})^r$ étant de dimension r, on sait que si δ est nilpotent, alors $\delta^r = 0$ (on se reportera à l'exercice 6.8 pour une démonstration de ce résultat). La matrice de l'application linéaire δ dans la base canonique est

$$\mathrm{A} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \\ 0 & & & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 \end{pmatrix} = \mathrm{I} + \mathrm{P}.$$

où P est la matrice de permutation d'ordre r

$$\mathrm{P} = \begin{pmatrix} 0 & 1 & 0 & \dots & \dots & 0 \\ 0 & 0 & 1 & & & \vdots \\ 0 & 0 & 0 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ \vdots & & & 0 & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 & 0 \end{pmatrix}.$$

On a alors

$$\mathrm{P}^2 = \begin{pmatrix} 0 & 0 & 1 & \dots & \dots & 0 \\ 0 & 0 & 0 & 1 & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ 0 & & & \ddots & \ddots & 1 \\ 1 & 0 & & & \ddots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \end{pmatrix}, \dots, \mathrm{P}^{r-1} = \begin{pmatrix} 0 & 0 & 0 & \dots & \dots & 1 \\ 1 & 0 & 0 & & & \vdots \\ 0 & 1 & 0 & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & 1 & 0 & 0 \\ 0 & \dots & \dots & 0 & 1 & 0 \end{pmatrix}, \mathrm{P}^r = \mathrm{I}.$$

On en déduit que

$$\mathrm{A}^r = (\mathrm{I}+\mathrm{P})^r = \sum_{k=0}^{r} \mathrm{C}_r^k \mathrm{P}^k = 2\mathrm{I} + \sum_{k=1}^{r-1} \mathrm{C}_r^k \mathrm{P}^k = \sum_{k=1}^{r-1} \mathrm{C}_r^k \mathrm{P}^k.$$

L'endomorphisme δ est nilpotent, autrement dit $\mathrm{A}^r = 0$, si et seulement si les C_r^k sont tous pairs pour $1 \leqslant k \leqslant r-1$, car $(\mathrm{I}, \mathrm{P}, \mathrm{P}^2, \dots, \mathrm{P}^{r-1})$ est une famille libre de matrices. Montrons que c'est le cas si et seulement si r est une puissance de 2.

$\star$ Supposons que les C_r^k soient pairs, pour tout $1 \leqslant k \leqslant r-1$. Pour prouver que r est une puissance de 2, il suffit de vérifier que $s(r) = 1$. On a, d'après la question 1, pour tout $1 \leqslant k \leqslant r-1$,

$$1 \leqslant \nu(\mathrm{C}_r^k) = \nu(r!) - \nu(k!) - \nu((r-k)!) = s(k) + s(r-k) - s(r). \quad (*)$$

En numération binaire r s'écrit $1\alpha_p\alpha_{p-1}\dots\alpha_0$. Si r n'est pas une puissance de 2, l'un des α_i est non nul. Par conséquent, si on pose $k = \alpha_p\alpha_{p-1}\dots\alpha_0$, on obtient $1 \leqslant k \leqslant r-1$, $r-k = 10\dots0$ (avec k zéros) et clairement,

$$s(r) = s(k) + s(r-k),$$

ce qui contredit l'inégalité $(*)$. Donc r est une puissance de 2.

$\star$ Réciproquement, supposons que r soit une puissance de 2. Ceci entraîne $s(r) = 1$ et, pour $1 \leqslant k \leqslant r-1$,

$$\nu(\mathrm{C}_r^k) = s(k) + s(r-k) - s(r) = s(k) + s(r-k) - 1 \geqslant 1,$$

ce qui traduit bien que les C_r^k sont pairs.

Le lecteur pourra se reporter à l'exercice 4.25 sur les congruences de Lucas pour une autre preuve de cette propriété.

Ainsi, nous avons prouvé que δ est nilpotent si et seulement si la propriété (ii) est vérifiée. Cela achève la démonstration. $\lhd$

Une fonction arithmétique est une application de $\mathbb{N}^*$ dans $\mathbb{C}$. Le lecteur aura déjà pu rencontrer l'un ou l'autre des exemples importants suivants : φ l'indicatrice d'Euler, σ (qui à n associe la somme des diviseurs de n), μ la fonction de Möbius, τ (qui à n associe le nombre de diviseurs de n)... Elles ont la propriété suivante : si n et n' sont premiers entre eux, l'image de nn' est le produit de l'image de n par l'image de n'. On dit qu'elles sont multiplicatives.

Ces fonctions sont au centre des exercices suivants.

4.28. Expression de $\sum_{k=1}^{n} \tau(k)$

On note $\tau(n)$ le nombre de diviseurs positifs de l'entier n. Montrer que

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \mathrm{E}\left(\frac{n}{k}\right) = 2\sum_{k=1}^{r} \mathrm{E}\left(\frac{n}{k}\right) - r^2, \quad \text{où } r = \mathrm{E}(\sqrt{n}).$$

(École normale supérieure)

$\rhd$ **Solution.**

• La première égalité provient simplement d'une interversion de sommation :

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \sum_{d|k} 1 = \sum_{d=1}^{n} \sum_{\substack{1 \leqslant k \leqslant n \\ d|k}} 1 = \sum_{d=1}^{n} \mathrm{E}\left(\frac{n}{d}\right),$$

car $\sum_{\substack{1 \leqslant k \leqslant n \\ d|k}} 1$ compte le nombre de multiples de d dans l'intervalle $[\![1, n]\!]$ et il y en a bien $\mathrm{E}\left(\frac{n}{d}\right)$.

• Pour établir la deuxième expression, on écrit

$$\sum_{k=1}^{n} \tau(k) = \sum_{k=1}^{n} \sum_{d|k} 1 = \sum_{dd' \leqslant n} 1,$$

en posant $d' = \frac{k}{d}$. L'ensemble des couples (d, d') vérifiant $dd' \leqslant n$ est la réunion des couples (d, d') tels que $d \leqslant \sqrt{n}$ et des couples (d, d') tels

que $d' \leqslant \sqrt{n}$. L'intersection de ces deux parties étant formée des couples (d, d') avec $d \leqslant \sqrt{n}$ et $d' \leqslant \sqrt{n}$, on a

$$\sum_{k=1}^{n} \tau(k) = \sum_{\substack{dd' \leqslant n \\ d \leqslant \sqrt{n}}} 1 + \sum_{\substack{dd' \leqslant n \\ d' \leqslant \sqrt{n}}} 1 - \sum_{\substack{dd' \leqslant n \\ d, d' \leqslant \sqrt{n}}} 1.$$

Par symétrie, les deux premières sommes sont égales et on a donc

$$\sum_{k=1}^{n} \tau(k) = 2 \sum_{\substack{dd' \leqslant n \\ d \leqslant \sqrt{n}}} 1 - r^2 = 2 \sum_{k=1}^{r} \mathrm{E}\left(\frac{n}{k}\right) - r^2. \lhd$$

La première égalité de l'énoncé permet de montrer que le nombre moyen de diviseurs d'un entier entre 1 *et* n, *c'est-à-dire* $\frac{1}{n} \sum_{k=1}^{n} \tau(k)$, *est équivalent à* $\ln n$ *en l'infini (cf. l'exercice 3.21 du tome 1 d'analyse pour un développement asymptotique plus précis).*

4.29. Une majoration de σ

Pour $n \in \mathbb{N}^*$, on note $\sigma(n)$ la somme des diviseurs de n. Montrer que $\sigma(n) \leqslant n + n \ln n$.

(École normale supérieure)

1 - **Solution.**

Soit $\mathcal{D}$ l'ensemble des diviseurs de n. Si $d \in \mathcal{D}$, il existe $k \in [\![1, n]\!]$ tel que $d = \frac{n}{k}$. On a donc $\mathcal{D} \subset \left\{ \frac{n}{k}, k \in [\![1, n]\!] \right\}$, d'où l'on déduit l'inégalité

$$\sigma(n) \leqslant n \sum_{k=1}^{n} \frac{1}{k}.$$

Le résultat demandé se déduit de $\sum_{k=1}^{n} \frac{1}{k} \leqslant 1 + \ln n$, ce qui se démontre en remarquant que $\frac{1}{k} \leqslant \int_{k-1}^{k} \frac{1}{t} \mathrm{d}t$ pour $k \in [\![2, n]\!]$. $\lhd$

4.30. Équation faisant intervenir σ

On note $\sigma(n)$ la somme des diviseurs de n (n entier > 0).

1. Montrer que $\sigma(n)$ est impair si et seulement si n est de la forme $2^\alpha q^2$ avec q impair.

2. Résoudre l'équation $3\sigma(n) = 4n - 17$.

(École normale supérieure)

▷ **Solution.**

1. L'équivalence est triviale pour $n = 1$. Soit donc un entier $n \geqslant 2$. On peut l'écrire sous la forme $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, où les p_i sont des nombres premiers impairs deux à deux distincts (les α_i sont dans $\mathbb{N}^*$ mais α peut être nul). La somme des diviseurs de n a la même parité que la somme des diviseurs impairs de n, c'est-à-dire que le nombre de diviseurs impairs de n. Ceux-ci sont les entiers de la forme $p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, avec pour tout i, $0 \leqslant \beta_i \leqslant \alpha_i$. Il y en a donc $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$. Il en résulte donc que $\sigma(n)$ est impair si et seulement si tous les α_i sont pairs, ce qui conduit directement au résultat demandé.

2. Supposons l'équation $3\sigma(n) = 4n-17$ possède une solution $n > 0$. D'après la question précédente, on peut écrire n sous la forme $n = 2^\alpha q^2$ avec q impair.

• Si $\alpha \geqslant 1$ alors $\dfrac{n}{2}$ est un diviseur de n et on a $\sigma(n) \geqslant n + \dfrac{n}{2} = \dfrac{3n}{2}$. Mais dans ce cas $3\sigma(n) \geqslant \dfrac{9n}{2} > 4n - 17$.

• On a donc $\alpha = 0$ et $n = q^2$. Si on passe alors modulo 3, on obtient $4n \equiv 17 \equiv 2$ [3]. Or, $4n = (2q)^2$ est congru à 0 ou 1 modulo 3 (2 n'est pas un carré modulo 3).

Conclusion. L'équation proposée n'a pas de solution. ◁

4.31. Sur la fonction σ

On note toujours $\sigma(n)$ la somme des diviseurs de n.

Pour $p \in \mathbb{N}^*$, on pose $f(p) = \sup\{n \in \mathbb{N}^*, \sigma(n) \leqslant p\}$. Montrer que pour tout $k \in \mathbb{N}^*$, l'équation $p - f(p) = k$ a une infinité de solutions.

(École polytechnique)

▷ **Solution.**

• On a $f(1) = 1$. Pour $p \geqslant 2$, on pose $\mathrm{F} = \{n \in \mathbb{N}^*, \sigma(n) \leqslant p\}$. L'ensemble F contient 1 et est clairement majoré par $p-1$ car on a $\sigma(n) \geqslant n+1$ pour $n \geqslant 2$. Donc $f(p)$ est bien définie et $f(p) \leqslant p-1$.

• On remarque que, si $p-1$ est premier, $p-1$ appartient à F et donc que $f(p) = p-1$. Les nombres de la forme $1+q$, avec q premier sont donc solutions de l'équation pour $k = 1$. Il y en a bien une infinité.

• Prenons $k \geqslant 2$.

⋆ Analyse. Soit $(p_n)_{n\geqslant 0}$ une suite de nombres premiers à choisir, tendant vers l'infini. On a

$$\sigma(p_n) = 1 + p_n \leqslant p_n + k \text{ et donc } f(p_n + k) \geqslant p_n.$$

On obtient l'encadrement $p_n \leqslant f(p_n+k) \leqslant (p_n+k)-1$. Pour avoir $f(p_n+k) = p_n$, il suffit donc que, pour tout $1 \leqslant m \leqslant k-1$, $p_n + m$ ne

soit pas premier (du moins pour n est assez grand). En effet, dans ces conditions, $p_n + m$ admet un diviseur strict plus grand que $\sqrt{p_n + m}$ et

$$\sigma(p_n + m) \geqslant p_n + m + \sqrt{p_n + m} + 1 \geqslant p_n + \sqrt{p_n} + 1.$$

Donc à partir d'un certain n_0, si $n \geqslant n_0$, $\sqrt{p_n} \geqslant k$ et la somme des diviseurs de $p_n + m$ est donc strictement plus grande que $p_n + k$. Par conséquent, si $n \geqslant n_0$, $f(p_n + k) = p_n$. Il s'agit donc de trouver une suite $(p_n)_{n \geqslant 0}$ de nombres premiers, tendant vers l'infini, telle que pour tout $n \geqslant 0$ et tout $1 \leqslant m \leqslant k - 1$, $p_n + m$ ne soit pas premier.

$\star$ Synthèse. Pour $n > k$, on considère p_n le plus grand nombre premier inférieur ou égal à $n! - (k+1)$. La suite (p_n) tend vers l'infini. Pour tout $m \in [\![1, k-1]\!]$, on a

$$p_n < p_n + m \leqslant n! - (k+1) + (k-1) = n! - 2.$$

Si $p_n + m \leqslant n! - (k+1)$ alors, par définition de p_n, $p_n + m$ n'est pas premier puisque $p_n + m > p_n$. Si $n! - k \leqslant p_n + m \leqslant n! - 2$, $p_n + m$ s'écrit $n! - i$ avec $2 \leqslant i \leqslant k$. Dans ces conditions, i divise $n! - i$ et i est bien distinct de $n! - i$ car

$$n! - i - i = n! - 2i \geqslant ni - 2i > ki - 2i = (k-2)i \geqslant 0.$$

Donc $p_n + m = n! - i$ ne peut être premier. Par conséquent, la suite $(p_n)_{n > k}$ répond à ce que nous recherchions : d'après l'analyse, $p_n + k$ sera solution de l'équation $p - f(p) = k$ pour n assez grand. La suite $(p_n)_{n > k}$ tendant vers l'infini, il y a bien une infinité de solutions. $\triangleleft$

Il s'agit dans l'exercice suivant de déterminer les fonctions arithmétiques multiplicatives qui sont croissantes.

4.32. Un théorème d'Erdös (1946)

1. Une fonction $f : \mathbb{N}^* \to \mathbb{R}$ est dite complètement multiplicative si pour tout $(a, b) \in (\mathbb{N}^*)^2$, on a $f(ab) = f(a)f(b)$. Déterminer toutes les applications complètement multiplicatives. Quelles sont celles qui sont croissantes ?

2. Une application $f : \mathbb{N}^* \to \mathbb{R}$ est dite multiplicative si on a $f(ab) = f(a)f(b)$ lorsque a et b sont des entiers naturels premiers entre eux. Montrer qu'une application multiplicative croissante est complètement multiplicative.

(**École normale supérieure**)

▷ **Solution.**

1. Soit f une application complètement multiplicative. On a pour tout $n \geqslant 1$, $f(n) = f(n)f(1)$. Donc soit f est nulle, soit $f(1) = 1$. On ne s'intéresse dans la suite qu'au cas où f est non nulle.

• L'application f est complètement déterminée par la suite des images des nombres premiers. En effet, on a pour tout entier naturel $n \geqslant 1$,

$$f(n) = \prod_{p \in \mathcal{P}} f(p)^{\nu_p(n)}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers et pour tout $p \in \mathcal{P}$, $\nu_p(n)$ est la valuation p-adique de n (le produit est parfaitement défini puisque la famille $(\nu_p(n))_{p \in \mathcal{P}}$ est à support fini).

Réciproquement, si on se donne une suite quelconque $(u_p)_{p \in \mathcal{P}}$ de nombres réels indicée par l'ensemble $\mathcal{P}$, l'application qui, à tout $n \geqslant 1$, associe $\prod\limits_{p \in \mathcal{P}} u_p^{\nu_p(n)}$ est complètement multiplicative.

• En gardant ces notations, on va maintenant chercher à quelles conditions sur la suite (u_p) l'application f obtenue est croissante. Les applications $n \longmapsto n^\alpha$, pour $\alpha \in \mathbb{R}_+$, conviennent. On va voir que ce sont les seules. Pour p premier, on a $1 \leqslant p$ et donc $f(1) = 1 \leqslant u_p$. Posons $\alpha_p = \dfrac{\ln u_p}{\ln p}$. On a alors $f(p) = u_p = p^{\alpha_p}$. On va prouver que tous les α_p sont égaux. Choisissons $p < q$, deux nombres premiers et $m \in \mathbb{N}^*$. Soit n l'unique entier tel que $p^n < q^m < p^{n+1}$. Par croissance de f, il vient $p^{\alpha_p n} \leqslant q^{\alpha_q m} \leqslant p^{\alpha_p(n+1)}$. En passant au logarithme, et en divisant par $n \ln p$, on obtient

$$\alpha_p \leqslant \alpha_q \frac{m}{n} \times \frac{\ln q}{\ln p} \leqslant \alpha_p \frac{n+1}{n}.$$

On fait tendre m vers l'infini. Alors, $n = \mathrm{E}\Big(\dfrac{m \ln q}{\ln p}\Big)$ tend aussi vers l'infini et $n \sim \dfrac{m \ln q}{\ln p}$. Par passage à la limite dans l'inégalité ci-dessus, il vient $\alpha_p \leqslant \alpha_q \leqslant \alpha_p$, ce qui donne le résultat annoncé.

Conclusion. Les seules applications non nulles complètement multiplicatives et croissantes sont les applications $n \longmapsto n^\alpha$ pour $\alpha \in \mathbb{R}_+$.

2. Soit f une application multiplicative non nulle et croissante. En particulier si $n \in \mathbb{N}^*$, $f(n) \geqslant f(1) = 1$. On souhaite prouver que la quantité $\dfrac{\ln f(a)}{\ln a}$ ne dépend pas de $a \geqslant 2$. Une difficulté supplémentaire provient de ce qu'il est dorénavant impossible d'écrire $f(a^k) = f(a)^k$. On va commencer par estimer $f(a)^k$ en utilisant la monotonie de f.

On a $f(a-1) \leqslant f(a) \leqslant f(a+1)$ avec $a \wedge (a-1) = a \wedge (a+1) = 1$. Ainsi, $f(a)^2 \leqslant f(a)f(a+1) = f(a^2+a)$ et $f(a)^2 \geqslant f(a)f(a-1) = f(a^2-a)$.

Essayons maintenant d'encadrer $f(a)^3$. On a $f(a)^3 \leqslant f(a)f(a^2+a)$. Mais ici a et a^2+a ne sont pas premiers entre eux. On majore donc $f(a^2+a)$ par $f(a^2+a+1)$ et $f(a)^3 \leqslant f(a^3+a^2+a)$. De même $f(a)^3 \geqslant f(a^3-a^2-a)$. On montre alors par une récurrence facile que, pour $a \geqslant 2$ et $k \geqslant 1$,

$$f(a^k - a^{k-1} - \cdots - a - 1) \leqslant f(a)^k \leqslant f(a^k + a^{k-1} + \cdots + a + 1).$$

Pour $a = 2$, on a $a^k - a^{k-1} - \cdots - a - 1 = 1$ pour tout k : la minoration obtenue est triviale. On regardera le cas de l'entier 2 à la fin. Prenons deux entiers a et b supérieurs à 3. Soit $n \geqslant 1$. Notons m_n le plus petit entier tel que

$$1 + a + \cdots + a^n \leqslant b^{m_n} - b^{m_n - 1} - \cdots - b - 1$$

et p_n le plus grand entier tel que

$$1 + b + b^2 + \cdots + b^{p_n} \leqslant a^n - a^{n-1} - \cdots - 1.$$

On a

$$f(a)^n \leqslant f(1 + a + \cdots + a^n) \leqslant f(b^{m_n} - b^{m_n - 1} - \cdots - b - 1) \leqslant f(b)^{m_n}$$

et

$$f(b)^{p_n} \leqslant f(1 + b + b^2 + \cdots + b^{p_n}) \leqslant f(a^n - a^{n-1} - \cdots - 1) \leqslant f(a)^n,$$

de sorte qu'en passant au logarithme, on obtient

$$\frac{p_n}{n} \ln f(b) \leqslant \ln f(a) \leqslant \frac{m_n}{n} \ln f(b).$$

Il ne reste plus qu'à étudier les limites de $\dfrac{p_n}{n}$ et $\dfrac{m_n}{n}$ lorsque n tend vers l'infini. Les suites (p_n) et (m_n) tendent vers $+\infty$. Par définition de p_n, on a les inégalités

$$1 + b + b^2 + \cdots + b^{p_n} \leqslant a^n - a^{n-1} - \cdots - 1 \leqslant 1 + b + \cdots + b^{p_n} + b^{p_n+1}.$$

On passe au logarithme. Des équivalences

$$\ln(1 + b + b^2 + \cdots + b^{p_n}) \sim p_n \ln b \quad \text{et} \quad \ln(a^n - a^{n-1} - \cdots - 1) \sim n \ln a,$$

on déduit $\displaystyle\lim_{n \to +\infty} \frac{p_n}{n} = \frac{\ln a}{\ln b}$. On obtient le même résultat pour $\dfrac{m_n}{n}$. On a donc $\ln f(a) = \dfrac{\ln a}{\ln b} \ln f(b)$. En conséquence, il existe $\alpha \in \mathbb{R}^+$ tel que pour tout $n \geqslant 3$, $f(n) = n^\alpha$.

Reste le cas de $n = 2$. De $f(6) = 6^\alpha = f(2.3) = f(2).f(3) = f(2)3^\alpha$, on tire aussi $f(2) = 2^\alpha$.

Conclusion. Toute application non nulle multiplicative et croissante est de la forme $n \longmapsto n^\alpha$ pour $\alpha \in \mathbb{R}_+$ (théorème d'Erdös). $\lhd$

4.33. Probabilité pour que deux entiers soient premiers entre eux

Pour $n \geqslant 1$, on note r_n la probabilité pour que deux entiers choisis aléatoirement dans $[\![1, n]\!]^2$ soient premiers entre eux. D'autre part, on définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{Z}$ de la manière suivante : $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier et $\mu(p_1 \dots p_r) = (-1)^r$. si les p_i sont des nombres premiers deux à deux distincts.

1. Montrer que $r_n = \dfrac{1}{n^2} \sum\limits_{d=1}^{n} \mu(d)\, \mathrm{E}\left(\dfrac{n}{d}\right)^2$.
2. Calculer $\sum\limits_{d|n} \mu(d)$.
3. Montrer que $\lim\limits_{n \to +\infty} r_n = \dfrac{6}{\pi^2}$.

(**École normale supérieure**)

▷ **Solution.**

1. Pour $n \geqslant 1$, notons A_n l'ensemble des couples $(a, b) \in [\![1, n]\!]^2$ tels que $a \wedge b = 1$. On a $r_n = \dfrac{\mathrm{Card}\, \mathrm{A}_n}{n^2}$. Soit $p_1, \dots, p_k$ les nombres premiers inférieurs à n et U_i l'ensemble des couples (a, b) de $[\![1, n]\!]^2$ tels que $p_i | a$ et $p_i | b$. Il est clair que A_n est le complémentaire de la réunion des U_i. Rappelons la *formule du crible* donnant le cardinal d'une réunion finie d'ensembles finis.

Lemme. *Soit* $\mathrm{U}_1, \dots, \mathrm{U}_k$ *k ensembles finis. Alors, le cardinal de la réunion des* U_i *est donné par*

$$\mathrm{Card}\left(\bigcup_{i=1}^{k} \mathrm{U}_i\right) = \sum_{\emptyset \neq \mathrm{I} \subset [\![1,k]\!]} (-1)^{1+\mathrm{Card}\,\mathrm{I}}\, \mathrm{Card}\left(\bigcap_{i \in \mathrm{I}} \mathrm{U}_i\right).$$

Démonstration. Ce résultat se prouve par récurrence sur k ou à l'aide des fonctions caractéristiques. ◇

Si $\mathrm{I} \subset [\![1, k]\!]$ est non vide, le cardinal de l'intersection $\bigcap_{i \in \mathrm{I}} \mathrm{U}_i$ est égal au nombre de couples de multiples strictement positifs de $\prod\limits_{i \in \mathrm{I}} p_i$ inférieurs ou égaux à n ; il vaut donc $\mathrm{E}\left(\dfrac{n}{\prod\limits_{i \in \mathrm{I}} p_i}\right)^2$. La formule du crible donne alors

$$\begin{aligned}\mathrm{Card}\, \mathrm{A}_n &= n^2 - \mathrm{Card}\left(\bigcup_{i=1}^{k} \mathrm{U}_k\right) \\ &= n^2 - \sum_{\emptyset \neq \mathrm{I} \subset [\![1,k]\!]} (-1)^{\mathrm{Card}\,\mathrm{I}+1}\, \mathrm{Card}\left(\bigcap_{i \in \mathrm{I}} \mathrm{U}_i\right)\end{aligned}$$

$$= n^2 - \sum_{\emptyset \neq I \subset [\![1,k]\!]} (-1)^{\operatorname{Card} I+1} \mathrm{E}\left(\frac{n}{\prod_{i\in I} p_i}\right)^2 = \sum_{d=1}^{n} \mu(d) \mathrm{E}\left(\frac{n}{d}\right)^2.$$

On en déduit la probabilité r_n :

$$\boxed{r_n = \frac{1}{n^2} \sum_{d=1}^{n} \mu(d) \mathrm{E}\left(\frac{n}{d}\right)^2}.$$

2. Si nous notons $\mathrm{S}(n) = \sum_{d|n} \mu(d)$, nous avons $\mathrm{S}(1) = 1$ et nous allons prouver que $\mathrm{S}(n) = 0$, si $n \geqslant 2$. Pour cela, considérons la décomposition de n en en facteurs premiers : $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, où $p_1, \ldots, p_k$ sont des nombres premiers distincts et $\alpha_1, \ldots, \alpha_k$ des entiers strictement positifs. Les seuls diviseurs d de n pour lesquels $\mu(d)$ est non nul sont les produits de nombres premiers distincts pris parmi $p_1, \ldots, p_k$. Pour un tel diviseur, on a $\mu(d) = (-1)^i$, où i est le nombre de diviseurs premiers de d. Or, n possède C_k^i diviseurs d correspondant à un i fixé. On en déduit que

$$\sum_{d|n} \mu(d) = \sum_{i=0}^{k} \mathrm{C}_k^i (-1)^i = (1-1)^k = 0.$$

On conclut que $\boxed{\sum_{d|n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geqslant 2 \end{cases}}$.

3. Pour l'étude asymptotique de r_n, il paraît naturel de remplacer le terme $\frac{1}{n^2}\mathrm{E}\left(\frac{n}{d}\right)^2$ par son équivalent $\frac{1}{d^2}$. La différence entre les deux sommes s'écrit

$$\left| r_n - \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \right| = \left| \sum_{d=1}^{n} \mu(d) \left(\frac{1}{n^2} \mathrm{E}\left(\frac{n}{d}\right)^2 - \frac{1}{d^2} \right) \right|.$$

Comme $\mathrm{E}\left(\frac{n}{d}\right) > \frac{n}{d} - 1$, on a $\frac{1}{n^2} - \frac{2}{dn} < \frac{1}{n^2}\mathrm{E}\left(\frac{n}{d}\right)^2 - \frac{1}{d^2} \leqslant 0$, ce qui donne la majoration

$$\left| r_n - \sum_{d=1}^{n} \frac{\mu(d)}{d^2} \right| \leqslant \sum_{d=1}^{n} \left(\frac{2}{dn} + \frac{1}{n^2} \right) \leqslant \frac{2}{n} \sum_{d=1}^{n} \frac{1}{d} + \frac{1}{n} = \mathrm{O}\left(\frac{\ln n}{n}\right),$$

parce que la somme partielle de la série harmonique est équivalente à $\ln n$. Il en résulte donc que $\lim_{n\to+\infty} r_n = \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}$ (la série est absolument convergente).

• La quantité $\frac{6}{\pi^2}$ est l'inverse de $\zeta(2) = \sum_{n=1}^{+\infty} \frac{1}{n^2}$. Cela nous invite à calculer le produit des sommes $\sum_{n=1}^{+\infty} \frac{1}{n^2}$ et $\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}$. Les familles $\left(\frac{\mu(d)}{d^2}\right)_{d\geqslant 1}$ et $\left(\frac{1}{n^2}\right)_{n\geqslant 1}$ sont sommables, donc la suite double $\left(\frac{\mu(d)}{d^2n^2}\right)_{n,d\geqslant 1}$ l'est aussi et est elle est justifiable du théorème d'associativité :

$$\begin{aligned}\left(\sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2}\right)\left(\sum_{n=1}^{+\infty} \frac{1}{n^2}\right) &= \sum_{d,n\geqslant 1} \frac{\mu(d)}{(dn)^2} = \sum_{\substack{d\geqslant 1\\ d|p}} \frac{\mu(d)}{p^2} \\ &= \sum_{p\geqslant 1}\sum_{d|p} \frac{\mu(d)}{p^2} = \sum_{p\geqslant 1} \frac{1}{p^2}\left(\sum_{d|p} \mu(d)\right) = 1,\end{aligned}$$

d'après le calcul de la question précédente.

Conclusion. $\boxed{\lim_{n\to+\infty} r_n = \frac{6}{\pi^2}}$. ◁

L'importance de la fonction de Möbius provient de la «formule d'inversion» suivante. Si f est une fonction de $\mathbb{N}^*$ dans $\mathbb{C}$ et qu'on définit la fonction $g : \mathbb{N}^* \to \mathbb{C}$ par $g(n) = \sum_{d|n} f(d)$, on peut retrouver f à partir de g puisque, pour tout $n \in \mathbb{N}^*$, on a $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$. Par exemple, pour $n \geqslant 1$, on a $n = \sum_{d|n} \varphi(n)$ (voir 4.17). On en déduit que $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$.

Les deux exercices suivants proposent d'établir, avec des arguments complètement différents, le fait que tout nombre premier p congru à 1 modulo 4 est somme de deux carrés. C'est le premier pas vers la caractérisation des entiers naturels n s'écrivant comme somme de deux carrés : n est somme de deux carrés si, et seulement si, pour tout nombre premier p congru à 3 modulo 4, l'exposant de p dans la décomposition en produits de facteurs premiers de n est pair.

4.34. Écriture d'un nombre premier comme somme de deux carrés

Soit p un nombre premier impair.

1. Montrer que si p est une somme de deux carrés d'entiers, on a alors $p \equiv 1 \pmod 4$.

On suppose p congru à 1 modulo 4.

2. Dénombrer les carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$.

3. En déduire qu'il existe $n \in \mathbb{Z}$ tel que $n^2 \equiv -1 \pmod{p}$.

4. Démontrer qu'il existe $(a, b) \in \mathbb{Z}^2$ tels que :

$$0 < b < \sqrt{p} \quad \text{et} \quad \left| b\frac{n}{p} - a \right| \leqslant \frac{1}{\sqrt{p}}.$$

5. Montrer que $(bn - ap)^2 + b^2 = p$.

(**École polytechnique**)

Solution.

1. Modulo 4, un carré est congru à 0 ou à 1. Si un entier est somme de deux carrés, il sera donc congru modulo 4 à 0, 1 ou 2.

Comme p est un entier premier impair, il ne peut être congru ni 0, ni à 2 (car il serait alors divisible par 2). Il s'ensuit qu'un entier premier impair, somme de deux carrés d'entiers est congru à 1 modulo 4.

2. L'entier p étant premier, $\mathrm{K} = \mathbb{Z}/p\mathbb{Z}$ est un corps. On a donc, pour $(x, y) \in \mathrm{K}^{*2}$,

$$x^2 = y^2 \Longleftrightarrow (x - y)(x + y) = 0 \Longleftrightarrow x = y \text{ ou } x = -y.$$

Par conséquent, à tout carré de K^*, correspondent exactement deux antécédents dans K^* par l'application $x \longmapsto x^2$ (on a bien $x \neq -x$ pour $x \in \mathrm{K}^*$, puisque la caractéristique de K est $p > 2$). Il y a donc exactement $\dfrac{\operatorname{Card} \mathrm{K}^*}{2} = \dfrac{p-1}{2}$ carrés dans K^*.

3. Il suffit de prouver que -1 est un carré dans K. Si $x \in \mathrm{K}^*$ est un carré, on peut écrire $x = y^2$ avec $y \in \mathrm{K}^*$ et d'après le petit théorème de Fermat,

$$x^{\frac{p-1}{2}} = y^{2 \times \frac{p-1}{2}} = y^{p-1} = 1.$$

Donc x est racine du polynôme $\mathrm{P} = \mathrm{X}^{\frac{p-1}{2}} - 1$. Les $\dfrac{p-1}{2}$ carrés non nuls de K sont donc racines de P. Or, P a au plus $\dfrac{p-1}{2}$ racines distinctes ou confondues dans le corps K. Nécessairement, P est scindé et ses racines sont exactement les carrés de K^*.

Comme $p \equiv 1 \pmod{4}$, $\dfrac{p-1}{2}$ est pair, $(-1)^{\frac{p-1}{2}} = 1$ et -1 est un carré dans K.

4. On pose $\mathrm{N} = \mathrm{E}(\sqrt{p}) + 1$ et $\xi = \dfrac{n}{p}$ et on considère les N réels $x_k = k\xi - \mathrm{E}(k\xi)$ de l'intervalle $[0, 1[$, pour $0 \leqslant k \leqslant \mathrm{N} - 1$, et les N intervalles $\left[0, \dfrac{1}{\mathrm{N}}\right[, \left[\dfrac{1}{\mathrm{N}}, \dfrac{2}{\mathrm{N}}\right[, \ldots, \left[\dfrac{\mathrm{N}-1}{\mathrm{N}}, 1\right[$.

• Supposons d'abord que l'un des x_k soit dans l'intervalle $\left[\frac{N-1}{N}, 1\right[$. On a $k > 0$ car $x_0 = 0$. En posant $b = k$ et $a = E(k\xi) + 1$, on obtient

$$0 < b \leqslant N - 1 < \sqrt{p} \quad \text{et} \quad \left|b\frac{n}{p} - a\right| = |x_k - 1| \leqslant \frac{1}{N} \leqslant \frac{1}{\sqrt{p}},$$

l'inégalité $N - 1 < \sqrt{p}$ étant stricte car $\sqrt{p} \notin \mathbb{N}$.

• Dans le cas contraire, les N réels x_k sont dans les $N - 1$ intervalles $\left[\frac{k}{N}, \frac{k+1}{N}\right[$, avec $0 \leqslant k \leqslant N - 2$. D'après le principe des tiroirs de Dirichlet, il existe k et ℓ distincts tels que x_k et x_ℓ soient dans le même intervalle. Supposons par exemple $k < \ell$. Notons alors $b = \ell - k$ et $a = E(\ell\xi) - E(k\xi)$. On a de nouveau $0 < b \leqslant N - 1 < \sqrt{p}$ et

$$\left|b\frac{n}{p} - a\right| = |(\ell - k)\xi - (E(\ell\xi) - E(k\xi))| = |x_\ell - x_k| \leqslant \frac{1}{N} \leqslant \frac{1}{\sqrt{p}}.$$

Dans tous les cas, nous avons montré l'existence de $(a, b) \in \mathbb{Z}^2$ tel que

$$0 < b < \sqrt{p} \quad \text{et} \quad \left|b\frac{n}{p} - a\right| \leqslant \frac{1}{\sqrt{p}}.$$

5. Les inégalités obtenues dans la question 4 impliquent

$$0 < b^2 < p \quad \text{et} \quad (bn - ap)^2 \leqslant p \quad \text{et donc } 0 < (bn - ap)^2 + b^2 < 2p$$

D'autre part, on a $n^2 + 1 \equiv 0 \pmod{p}$ et donc

$$(bn - ap)^2 + b^2 = b^2(n^2 + 1) - 2abnp + a^2p^2 \equiv 0 \pmod{p}.$$

Comme cet entier appartient à l'intervalle $]0, 2p[$, cela implique l'égalité

$$(bn - ap)^2 + b^2 = p.$$

Conclusion. Tout nombre premier congru à 1 modulo 4 s'écrit comme somme de deux carrés d'entiers. ◁

4.35. Théorème des deux carrés, preuve combinatoire

Soit p premier congru à 1 modulo 4, $p = 4k + 1$. On considère l'ensemble

$$S = \{(a, b, c) \in \mathbb{N}^2 \times \mathbb{Z},\ 4ab + c^2 = p\}.$$

1. Montrer que S est non vide, fini et inclus dans $(\mathbb{N}^*)^2 \times \mathbb{Z}^*$. Prouver que $S_1 = \{(a, b, c) \in S,\ a > b + c\}$ et $S_2 = \{(a, b, c) \in S,\ a < b + c\}$ forment une partition de S. Exhiber une bijection de S_1 sur S_2.

2. Montrer que $f : (a, b, c) \longmapsto (a-b-c, b, -2b-c)$ est une involution de S_1. Chercher ses points fixes et en déduire que le cardinal de S est congru à 2 modulo 4.

3. Montrer que $S_3 = \{(a, b, c) \in S,\ a \neq b\}$ a un cardinal divisible par 4. En déduire que p est somme de deux carrés.

(École normale supérieure)

Solution.

1. Comme $(k, 1, 1) \in S$, S est non vide. Si $(a, b, c) \in S$ les entiers a, b et $|c|$ sont majorés par p. Donc S est fini. De plus, si $a = 0$ ou $b = 0$, on a $p = c^2$, ce qui est impossible car p est premier et si $c = 0$, $p = 4ab$ est pair ce qui est tout aussi absurde. Donc S est inclus dans $(\mathbb{N}^*)^2 \times \mathbb{Z}^*$.

On a $(k, 1, 1) \in S_1$ et $(1, k, 1) \in S_2$, de sorte que S_1 et S_2 sont non vides. Comme S_1 et S_2 sont visiblement disjoints, il suffit de prouver qu'il n'y a pas de triplet $(a, b, c) \in S$ tel que $a = b + c$. Or, on aurait dans ce cas

$$p = 4b(b + c) + c^2 = (c + 2b)^2,$$

ce qui est impossible. On a bien $S_1 \cup S_2 = S$.

D'autre part, on peut vérifier que l'application qui à (a, b, c) associe $(b, a, -c)$ est une bijection de S_1 sur S_2. Les ensembles S_1 et S_2 ont donc même cardinal et $|S| = 2|S_1|$.

2. Montrons pour commencer que si le triplet (a, b, c) est dans S_1, alors $(a - b - c, b, -2b - c)$ est aussi dans S_1. En effet, $a - b - c$ et b sont positifs, $4(a - b - c)b + (-2b - c)^2 = 4ab + c^2 = p$ et $a - b - c > -b - c$ car $a > 0$. Donc f est une application de S_1 dans S_1. Enfin $f \circ f = \mathrm{Id}_{S_1}$ de sorte qu'on a bien une involution.

Le triplet (a, b, c) est fixe par f si $a = a - b - c$ et $c = -2b - c$, c'est-à- dire si $c = -b$. Il vient alors $p = 4ab + b^2 = b(4a + b)$. Comme p est premier, cela impose $b = 1$ et $a = k$. Il y a donc un unique point fixe. Par ailleurs, la décomposition en cycles à supports disjoints de la permutation f est composée uniquement de transpositions (car f est d'ordre 2). La réunion de leurs supports (S_1 privé du point fixe) est donc de cardinal pair. Il en résulte que le cardinal de S_1 est impair et donc que $|S| \equiv 2 \pmod 4$ (puisque $|S| = 2|S_1|$).

3. À tout $(a, b, c) \in S$ avec $a \neq b$, on peut associer les 4 triplets *distincts* (a, b, c), $(a, b, -c)$, (b, a, c) et $(b, a, -c)$ tous dans S. Le cardinal de S_3 est donc divisible par 4. Il résulte de cela et du résultat de la question précédente que $|S_3|$ ne peut être égal à $|S|$ et que S_3 est donc strictement inclus dans S. On peut donc trouver un triplet de la forme (a, a, c) dans S. On a alors $p = 4a^2 + c^2 = (2a)^2 + c^2$ qui est somme de deux carrés. $\triangleleft$

Cette preuve combinatoire du théorème des deux carrés est très récente. Elle est due à Don Zagier et date de 1990.

On s'intéresse dans ce qui suit aux sommes de quatre carrés.

4.36. Théorème des quatre carrés de Lagrange (1770)

1. Établir que pour tout $(a, b, c, d, x, y, z, t) \in \mathbb{Z}^8$,

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) = (ax+by+cz+dt)^2 + (ay-bx-ct+dz)^2 + (az+bt-cx-dy)^2 + (at-bz+cy-dx)^2.$$

2. Soit p un nombre premier impair. Montrer qu'il existe (a, b) dans $\mathbb{Z}^2$ tel que p divise $1 + a^2 + b^2$.

3. Soit E l'ensemble des entiers naturels $n \geqslant 1$ tel que np soit somme de quatre carrés d'entiers. Montrer que E n'est pas vide. On note m son plus petit élément. Montrer que $m < p$, puis que m est impair.

4. Supposons que $1 < m$ et que $mp = a^2 + b^2 + c^2 + d^2$. En considérant les résidus de a, b, c, d modulo m de valeur absolue minimale, construire $m' < m$ appartenant à E. Conclure.

5. En déduire que tout entier naturel peut s'écrire comme somme de quatre carrés.

(École normale supérieure)

▷ **Solution.**

1. Prendre un logiciel de calcul formel ou développer de tête le membre de droite et se convaincre que les doubles produits s'éliminent.

2. Notons que p divise $1 + a^2 + b^2$ si et seulement si $-\overline{1} = \overline{a}^2 + \overline{b}^2$ dans $\mathbb{Z}/p\mathbb{Z}$. Il nous suffit de montrer que $-\overline{1}$ est somme de deux carrés dans $\mathbb{Z}/p\mathbb{Z}$.

On sait qu'il y a exactement $\dfrac{p+1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}$. Rappelons-en rapidement la preuve. L'application $x \longmapsto x^2$ est un morphisme de groupes de $(\mathbb{Z}/p\mathbb{Z})^*$ dans lui-même, de noyau $\{\pm\overline{1}\}$ et d'image le groupe C des carrés non nuls. Le premier théorème d'isomorphisme permet d'affirmer que C est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*/\{\pm\overline{1}\}$. Comme $-\overline{1} \neq \overline{1}$ (car p est impair), il y a exactement $\dfrac{p-1}{2}$ carrés non nuls. En rajoutant 0 le compte est bon.

Les ensembles $\{x^2,\ x \in (\mathbb{Z}/p\mathbb{Z})\}$ et $\{-1-y^2,\ y \in (\mathbb{Z}/p\mathbb{Z})\}$ sont donc tous les deux de cardinal $\dfrac{p+1}{2}$, donc ils se coupent. Notons que cela prouve plus généralement que tout élément de $\mathbb{Z}/p\mathbb{Z}$ est somme de deux carrés.

3. La question 2 montre l'existence de $n \in \mathbb{N}^*$ tel que

$$np = 1 + a^2 + b^2 = 0^2 + 1^2 + a^2 + b^2.$$

Donc E n'est pas vide. En fait, on peut choisir a et b avec une valeur absolue minimale, c'est-à-dire vérifiant $|a| < \frac{p}{2}$ et $|b| < \frac{p}{2}$. En effet, si ce n'est pas le cas, on considère a' et b', congrus respectivement à a et b modulo p, tels que $|a'| < \frac{p}{2}$ et $|b'| < \frac{p}{2}$ (les inégalités sont strictes car p est impair). On a alors

$$1 + a'^2 + b'^2 \equiv 1 + a^2 + b^2 \equiv 0 \pmod{p}$$

et il existe $n' \in \mathbb{N}^*$ tel que $1 + a'^2 + b'^2 = n'p$. Si a et b vérifient cette condition supplémentaire, on a $np = 1 + a^2 + b^2 < 1 + \frac{p^2}{2}$. On en déduit que $n < p$ et donc $m < p$, par définition de m.

Supposons par l'absurde que m soit pair. On sait qu'on peut écrire $mp = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$. Les entiers $\alpha, \beta, \gamma, \delta$ sont soit tous pairs, soit tous impairs, soit deux pairs et deux impairs. Quitte à changer l'ordre des termes, on suppose dans le troisième cas que α et β sont pairs et γ et δ sont impairs. Mais alors, dans les trois cas on peut écrire

$$\frac{m}{2}p = \left(\frac{\alpha+\beta}{2}\right)^2 + \left(\frac{\alpha-\beta}{2}\right)^2 + \left(\frac{\gamma+\delta}{2}\right)^2 + \left(\frac{\gamma-\delta}{2}\right)^2,$$

ce qui contredit la minimalité de m. Donc m est impair.

4. Notons $\alpha, \beta, \gamma, \delta$ les résidus respectifs de a, b, c, d introduits par l'énoncé. On a $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$. Soit $m' \in \mathbb{N}$ tel que $mm' = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$. L'entier m' n'est pas nul car sinon m diviserait a, b, c et d, m^2 diviserait mp et m diviserait p, ce qui est impossible, car $1 < m < p$.

Par ailleurs, comme $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 < 4\left(\frac{m}{2}\right)^2 = m^2$ (l'inégalité est stricte car m est impair), on a $0 < m' < m$. D'après la première question, on peut écrire

$$m^2 m' p = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)(a^2 + b^2 + c^2 + d^2) = \mathrm{A}^2 + \mathrm{B}^2 + \mathrm{C}^2 + \mathrm{D}^2,$$

avec

$$\begin{aligned} \mathrm{A} &= a\alpha + b\beta + c\gamma + d\delta \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}, \\ \mathrm{B} &= a\beta - b\alpha - c\delta + d\gamma \equiv ab - ab - cd + cd \equiv 0 \pmod{m} \end{aligned}$$

et de même, C et D divisibles par m. On a donc

$$m'p = \left(\frac{\mathrm{A}}{m}\right)^2 + \left(\frac{\mathrm{B}}{m}\right)^2 + \left(\frac{\mathrm{C}}{m}\right)^2 + \left(\frac{\mathrm{D}}{m}\right)^2$$

et m' appartient à E. Cela contredit la définition de m. On conclut que $m = 1$.

5. Il est clair que $0, 1$ et 2 sont sommes de quatre carrés. D'après la question 4, tout nombre premier impair également. Le théorème de décomposition en facteurs premiers et la question 1 permettent de conclure. $\lhd$

Voici un exercice sur les sommes de trois carrés.

4.37. Lemme de Davenport-Cassels

Soit $n \in \mathbb{N}$. On suppose que n est la somme des carrés de trois rationnels. Montrer que n est la somme des carrés de trois entiers.
(École normale supérieure)

$\rhd$ **Solution.**

La propriété est évidente pour $n = 0$. Nous supposerons donc $n > 0$. Nous donnons de ce problème une formulation géométrique : si la sphère S de $\mathbb{R}^3$ d'équation $x^2 + y^2 + z^2 = n$ passe par un point rationnel, alors elle passe aussi par un point entier. Nous raisonnerons par l'absurde et supposerons que S contient un point à coordonnées rationnelles, mais pas de point à coordonnées entières.

Soit $a \in \mathbb{Q}^3 \cap \mathrm{S}$. Il existe $u \in \mathbb{Z}^3$ et $d \geqslant 2$ tel que $a = \dfrac{1}{d}u$. Nous supposerons a et u choisis de telle façon que d soit minimal.

Montrons qu'il existe $a' \in \mathbb{Z}^3$ tel que $\|a - a'\| < 1$ (il s'agit de norme euclidienne). Si $a = (x, y, z)$, on considère les entiers x', y', z' les plus proches de x, y, z respectivement. On obtient $|x - x'| \leqslant \dfrac{1}{2}$, $|y - y'| \leqslant \dfrac{1}{2}$ et $|z - z'| \leqslant \dfrac{1}{2}$. On en déduit que $\|a - a'\| \leqslant \sqrt{\dfrac{1}{4} + \dfrac{1}{4} + \dfrac{1}{4}} = \dfrac{\sqrt{3}}{2} < 1$.

Puisque a n'appartient pas à $\mathbb{Z}^3$, a' est distinct de a. La droite qui joint a à a' coupe la sphère S en a. Elle la recoupe en point a_1 dont nous allons calculer les coordonnées.

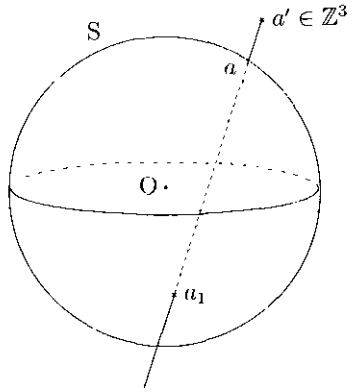
Il existe $\lambda \in \mathbb{R}$ tel que $a_1 = a' + \lambda(a - a')$. On écrit que a_1 appartient à S :

$$n = \|a_1\|^2 = \|a'\|^2 + 2\lambda\langle a', a - a'\rangle + \lambda^2\|a - a'\|^2.$$

Une solution de cette équation du second degré est 1, puisque $a \in \mathrm{S}$. L'autre est donc $\lambda = \dfrac{\|a'\|^2 - n}{\|a - a'\|^2}$. Examinons $\|a - a'\|^2$; on obtient

$$\|a - a'\|^2 = \|a'\|^2 + \|a\|^2 - 2\langle a', a\rangle = \|a'\|^2 + n - \frac{2}{d}\langle a', u\rangle = \frac{d_1}{d},$$

avec $d_1 \in \mathbb{N}^*$, puisque a' et u sont dans $\mathbb{Z}^3$ et $0 < d_1 < d$, puisque $0 \leqslant \|a - a'\| < 1$.



On en déduit $\lambda = \dfrac{\|a'\|^2 - n}{\|a - a'\|^2} = \dfrac{d(\|a'\|^2 - n)}{d_1}$ et

$$\begin{aligned} a_1 &= a' + \lambda(a - a') = a' + \frac{d(\|a'\|^2 - n)}{d_1}\frac{1}{d}(u - da') \\ &= a' + \frac{\|a'\|^2 - n}{d_1}(u - da'). \end{aligned}$$

Il existe donc $v \in \mathbb{Z}^3$ tel que $a_1 = \dfrac{1}{d_1}v$. Par ailleurs, a_1 appartient à S. Mais on a $0 < d_1 < d$, ce qui contredit la minimalité de d. Nous obtenons la contradiction souhaitée. $\lhd$

4.38. Une équation diophantienne

Soit $n \in \mathbb{N}$, $\alpha \in \mathbb{N}$, avec $\alpha > n \geqslant 2$. Montrer que l'équation

$$x_1^2 + \cdots + x_n^2 = \alpha x_1 \ldots x_n$$

n'a pas de solution entière autre que $(0, \ldots, 0)$.

(École normale supérieure)

$\rhd$ **Solution.**

Nous allons raisonner par l'absurde, en utilisant la méthode de la descente infinie : supposant qu'il existe une solution $(x_1, \ldots, x_n)$, différente de $(0, \ldots, 0)$, nous démontrerons qu'on peut trouver une autre solution $(y_1, \ldots, y_n)$, différente de $(0, \ldots, 0)$, telle que $y_1 + \cdots y_n < x_1 + \cdots + x_n$. Le procédé peut être réitéré. La somme $x_1 + \cdots + x_n$, qui appartient

à $\mathbb{N}$, ne pouvant décroître indéfiniment, cela donnera la contradiction souhaitée.

Si $(x_1, \ldots, x_n)$ est une solution différente de $(0, \ldots, 0)$, on a, pour tout $i \in [\![1, n]\!]$, $x_i \neq 0$. On peut sans perte de généralité supposer que $x_1 \leqslant \cdots \leqslant x_n$. On va chercher une autre solution de l'équation sous la forme $(x_1, \ldots, x_{n-1}, y)$ et vérifier que $y < x_n$. Pour que $(x_1, \ldots, x_{n-1}, y)$ soit solution, il faut que y soit racine du polynôme

$$\mathrm{P} = \mathrm{X}^2 - \alpha x_1 \ldots x_{n-1} \mathrm{X} + \sum_{i=1}^{n-1} x_i^2.$$

On sait déjà que l'entier x_n est une racine de P. La somme des racines de ce polynôme étant $\alpha x_1 \ldots x_{n-1}$, l'autre racine y est entière et strictement positive (car le produit des racines est $\sum_{i=1}^{n-1} x_i^2$). Comparons-la à x_{n-1}. Le calcul de

$$\begin{aligned} \mathrm{P}(x_{n-1}) &= x_{n-1}^2 - \alpha x_1 \ldots x_{n-2} x_{n-1}^2 + \sum_{i=1}^{n-1} x_i^2 \\ &= (n - \alpha x_1 \ldots x_{n-2}) x_{n-1}^2 + \sum_{i=1}^{n-2} x_i^2 - (n-2) x_{n-1}^2 \end{aligned}$$

montre que $\mathrm{P}(x_{n-1})$ est strictement négatif, car $\sum_{i=1}^{n-2} x_i^2 \leqslant (n-2) x_{n-1}^2$, et $\alpha x_1 \ldots x_{n-2} \geqslant \alpha > n$. On en déduit que x_{n-1} est entre x_n et y. On a donc $y < x_{n-1} < x_n$.

On a obtenu une autre solution $(x_1, \ldots, x_{n-1}, y)$ de notre équation, différente de $(0, \ldots, 0)$ vérifiant $x_1 + \cdots + x_{n-1} + y < x_1 + \cdots + x_{n-1} + x_n$. ◁

Ce chapitre d'arithmétique ne pouvait s'achever sans citer le grand théorème de Fermat : pour $n \geqslant 3$, l'équation $x^n + y^n = z^n$ n'a pas de solution non triviale dans $\mathbb{Z}$. On trouve mention de ce résultat dans une annotation marginale, écrite dans l'ouvrage de Diophante par Fermat, qui déclarait ne pas pouvoir donner sa preuve par manque de place. On est certain aujourd'hui que Fermat ne pouvait pas en avoir une démonstration complète. Mais le mythe était créé et des générations de mathématiciens pendant trois siècles allaient s'évertuer à le démontrer. Le Français Lamé crut son heure de gloire arrivée lorsqu'au siècle dernier, il en présenta une preuve. Malheureusement, il utilisait implicitement la factorialité de certains sous-anneaux de $\mathbb{C}$, qui n'est pas toujours vérifiée. De cette erreur furent tirés des prolongements qui ont contribué à mettre en place la théorie moderne des anneaux et des idéaux.

C'est en 1994 que le mathématicien anglais Wiles achevait ce long chemin dont le bout était éclairé depuis déjà une vingtaine d'années par les avancées de Weil.

L'exercice suivant résout ce qu'on appelle le premier cas du théorème de Fermat pour certains nombres premiers.

4.39. Théorème de Sophie Germain (1823)

Soit p un nombre premier de Sophie Germain, c'est-à-dire un nombre premier impair tel que $q = 2p+1$ soit premier. On se propose de prouver le théorème de Sophie Germain : *il n'existe pas de triplet* $(x, y, z) \in \mathbb{Z}^3$ *tel que* $xyz \not\equiv 0\ [p]$ *et* $x^p + y^p + z^p = 0$.

1. On raisonne par l'absurde. On suppose donné dans la suite un triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $x^p + y^p + z^p = 0$ et $xyz \not\equiv 0\ [p]$. Montrer qu'on peut supposer $\operatorname{pgcd}(x, y, z) = 1$ et qu'alors, x, y, z sont premiers entre eux deux à deux.

2. Montrer qu'il existe deux entiers a et α tels que $y + z = a^p$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k = \alpha^p$. Établir l'existence de deux entiers b, c tels que $x + y = c^p$ et $x + z = b^p$.

3. Si $m \in \mathbb{Z}$ n'est pas divisible par q, montrer que $m^p \equiv \pm 1\ [q]$. En déduire qu'un et un seul des trois entiers x, y, z est divisible par q. On supposera que c'est x.

4. Établir successivement les congruences suivantes, toutes modulo q

$$b^p + c^p - a^p \equiv 0 \ ; \ a \equiv 0 \ ; \ y \equiv c^p \quad \text{et} \quad \alpha^p \equiv p y^{p-1}.$$

Obtenir une contradiction et conclure.

(École normale supérieure)

Solution.

1. Soit $d = \operatorname{pgcd}(x, y, z)$, $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$ et $z' = \dfrac{z}{d}$. On a alors $x'^p + y'^p + z'^p = 0$, $\operatorname{pgcd}(x', y', z') = 1$ et bien entendu $x'y'z' \not\equiv 0\ [p]$. On peut donc supposer $\operatorname{pgcd}(x, y, z) = 1$. Supposons alors que $\operatorname{pgcd}(x, y) > 1$ et notons p_0 un diviseur premier de $\operatorname{pgcd}(x, y)$. Comme p_0 divise $x^p + y^p$, il divise z^p et donc z d'après le lemme d'Euclide, ce qui est contradictoire avec $\operatorname{pgcd}(x, y, z) = 1$. Donc x et y sont premiers entre eux. Le même raisonnement s'applique aux autres couples.

2. Montrons en raisonnant par l'absurde que $y+z$ et $\sum_{k=0}^{p-1} (-z)^{p-1-k} y^k$ sont premiers entre eux. Supposons donc qu'ils ont un codiviseur premier p'. On a classiquement

$$(1) \qquad (y+z)\left(\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k\right) = y^p + z^p = -x^p = (-x)^p.$$

On en déduit qu'alors p'^2 divise $-x^p$ et donc que p' divise x. De plus, comme $y \equiv -z\ [p']$, on a

$$\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1} \equiv 0 \quad [p'],$$

c'est-à-dire que p' divise py^{p-1}. Par le lemme de Gauss, soit $p'|p$, c'est-à-dire $p' = p$, et dans ce cas p divise x, ce qui est exclu par hypothèse, soit p' divise y^{p-1} et divise donc y. Mais alors, x et y ne sont pas premiers entre eux : nouvelle contradiction.

Ainsi, $y+z$ et $\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k$ sont premiers entre eux et de l'égalité (1) ci-dessus, on déduit l'existence de deux entiers a et α tels que

$$y + z = a^p \quad \text{et} \quad \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = \alpha^p.$$

(Si le produit de deux entiers u et v premiers entre eux est une puissance k-ième, alors u et v sont tous les deux des puissances k-ièmes comme nous l'avons prouvé à l'exercice 4.22).

Par symétrie, on prouve de même qu'il existe deux entiers b, c tels que $x + y = c^p$ et $x + z = b^p$.

3. Soit m un entier non divisible par q. Par le petit théorème de Fermat, on sait que $m^{q-1} \equiv 1\ [q]$, ce qui donne $(m^p)^2 \equiv 1\ [q]$ et donc, comme q est premier, $m^p \equiv 1\ [q]$ ou $m^p \equiv -1\ [q]$ ($\mathbb{Z}/q\mathbb{Z}$ est un corps).

Supposons par l'absurde qu'aucun des trois entiers x, y, z n'est divisible par q. Alors on a $x^p \equiv \pm 1$, $y^p \equiv \pm 1$ et $z^p \equiv \pm 1$ modulo q et en sommant, on obtient que $x^p + y^p + z^p$ est congru à 3, 1, -1 ou -3 modulo q (selon le nombre de signe $+$). C'est absurde (car $q > 5$). Donc l'un des trois entiers est divisible par q. On peut évidemment supposer sans perte de généralité que c'est x. Alors on a $yz \not\equiv 0\ [q]$, puisque x, y, z sont deux à deux premiers entre eux.

4. Toutes les congruences suivantes sont modulo q. On sait d'après la question 2 que $y + z = a^p$, $x + y = c^p$ et $x + z = b^p$. Il en résulte que $b^p + c^p - a^p = 2x \equiv 0$. On a évidemment $y \equiv c^p$ puisque $x \equiv 0$. Par ailleurs, q ne divise pas y, donc ne divise pas c. Il en résulte que $y \equiv \pm 1$. De la même manière, on obtient $z \equiv \pm 1$. Si maintenant q ne divise pas a, on a $a^p \equiv \pm 1$. Mais alors $c^p + b^p - a^p$ est congru à $3, 1, -1$ ou -3 modulo q, ce qui est impossible (car q divise $c^p + b^p - a^p$). On conclut que q divise a.

Regardons maintenant α^p. Sachant que $y + z \equiv a^p \equiv 0$, on en déduit que

$$\alpha^p = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1}.$$

Nous avons montré que $y \equiv \pm 1$. Il s'en suit que $\alpha^p \equiv p(-1)^{p-1} \equiv p$ (car $p-1$ est pair). C'est absurde puisque, d'après la question 3, une puissance p ième est congrue à 0, -1 ou 1 modulo q. Nous aboutissons dans tous les cas à une contradiction. Il ne peut exister de triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $xyz \not\equiv 0\ [p]$ et $x^p + y^p + z^p = 0$. $\lhd$

Sophie Germain (1776-1831) est quasiment la seule femme mathématicienne de son temps. Elle suivit les cours de l'École polytechnique par correspondance car les femmes n'y étaient pas admises et c'est sous le pseudonyme masculin de Maurice Leblanc qu'elle écrivit à Gauss pour lui faire part de ses découvertes arithmétiques. C'est dans cette correspondance qu'apparaît le théorème ci-dessus. Le plus grand nombre premier de Sophie Germain connu en 2001 est $109433307 \times 2^{66452} - 1$ *et il comporte* 20013 *chiffres. On conjecture qu'il en existe une infinité.*

Chapitre 5

Polynômes

La théorie des équations polynomiales, qui précède de loin la définition formelle des polynômes, a été le propos essentiel de l'algèbre jusqu'au XIXe *siècle. Elle est à l'origine de nombreuses notions : corps, nombres algébriques... Son développement est lié aux extensions successives de la notion de nombre : introduction des nombres négatifs, des nombres irrationnels, puis des nombres complexes.*

Dès la plus haute Antiquité, on rencontre des exemples de résolutions d'équations. Les Babyloniens savent résoudre l'équation du second degré et les Grecs en font la base même de leur géométrie.

Après l'Antiquité, il faudra attendre le XVIe *siècle pour que des progrès substantiels apparaissent, dus à l'école italienne. Scipione del Ferro, Tartaglia et Cardan apportent la solution de l'équation du troisième degré. L'équation générale est ramenée à la forme réduite* $x^3 + px + q = 0$, *dont une solution s'écrit*

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

Cette solution soulève des difficultés : si $\frac{q^2}{4} + \frac{p^3}{27}$ *est négatif, cas où l'équation a des racines — on le sait depuis Archimède — on ne peut pas calculer* x. *Pour lever la difficulté, Cardan introduit timidement de nouveaux nombres, «impossibles» ou «imaginaires». Ferrari et Bombelli résolvent l'équation du quatrième degré.*

Grâce à l'école italienne, la théorie générale des équations algébriques se précise. L'équation étant mise sous la forme $\mathrm{P}(x) = 0$, *on prend conscience de l'importance du degré de* P *pour le nombre de solutions. On découvre que si* a *est une racine de* P, *on peut factoriser par* $x - a$. *Les relations entre les coefficients et les fonctions symétriques des racines d'un polynôme apparaissent chez Viète (1540-1603), mais c'est Girard qui en 1629 leur donne toute leur extension. Suivi par Newton, il exprime les sommes des puissances des racines en fonction des coefficients. L'étude des fonctions symétriques des racines va se développer au* XVIIe *siècle avec Waring et au* XIXe *siècle avec Cauchy.*

Au XVIIe *siècle, la majorité des mathématiciens est convaincue qu'une équation de degré* n *possède* n *racines, celles-ci pouvant ne pas être réelles, mais il faut attendre d'Alembert pour trouver en 1724 une*

définition précise des nombres complexes (sous la forme $a + \sqrt{-1}b$). En 1799, Gauss fournit plusieurs preuves rigoureuses du «théorème fondamental de l'algèbre» ou «théorème de d'Alembert-Gauss» .

Des progrès sont réalisés également dans l'étude du nombre de racines réelles, et de leur signe. En 1637, Descartes énonce la règle qui porte son nom sur le nombre de racines positives d'un polynôme. On trouve dans l'Algèbre *de Rolle (1690), la propriété suivante : entre deux solutions de l'équation* $P(x) = 0$, *il existe au moins une solution de l'équation* $P'(x) = 0$. *C'est Sturm qui formule, en 1829, les résultats les plus précis sur le nombre de racines réelles d'un polynôme.*

Après les succès de l'école italienne au XVIe *siècle, les mathématiciens se sont attachés à trouver des formules analogues pour les degrés suivants. Les réflexions sur cette question prennent un tour nouveau avec les travaux de Lagrange (1771), qui étudie les permutations des racines d'une équation laissant invariantes certaines fonctions de ces racines. Ces idées sont approfondies par Cauchy et Ruffini. Abel donne une démonstration rigoureuse de l'impossibilité de résoudre par radicaux l'équation générale de degré* 5 *en 1829. Enfin, en introduisant la notion de groupe, Galois énonce la condition générale à laquelle satisfait toute équation résoluble par radicaux (1831).*

La distinction entre les nombres algébriques, racines d'un polynôme à coefficients entiers, et les autres qu'on nomme transcendants, date du XVIIe *siècle, mais il faut attendre 1844 pour que Liouville démontre l'existence de nombres transcendants et plus longtemps encore pour que soit démontrée la transcendance de* e *(par Hermite en 1872) et celle de* π *(par Lindemann en 1882).*

Quant à la définition formelle des polynômes et à l'étude de leur structure, elles chemineront tout au long du XIXe *siècle au rythme lent du processus d'axiomatisation de l'algèbre : par exemple, Dedekind introduit la notion de corps et définit les idéaux vers 1870.*

Les cours modernes remontent l'histoire à l'envers et commencent presque toujours par introduire les polynômes en tant qu'objet formel. Suivant cet usage, les premiers exercices concernent les polynômes formels et la structure d'algèbre que l'on obtient.

5.1. Égalité polynomiale

Dans quels corps a-t-on $X^4 - X^2 + 1 = (X^2 - 5X + 1)(X^2 + 5X + 1)$?
(École polytechnique)

▷ **Solution.**
En développant, on obtient

$$(X^2 - 5X + 1)(X^2 + 5X + 1) = X^4 - 23X^2 + 1.$$

Remarquons que si K est un corps qui convient, les polynômes en question sont dans $K_0[X]$, K_0 étant le sous-corps premier de K, autrement dit le plus petit sous-corps de K. On sait que K_0 est isomorphe à $\mathbb{Q}$ (si K est de caractéristique nulle) ou à $\mathbb{Z}/p\mathbb{Z}$ (si K est de caractéristique p, avec p premier).

En caractéristique nulle, $23 \neq 1$, donc K est de caractéristique p premier et on doit avoir $23 \equiv 1 \pmod{p}$. Cela arrive uniquement pour $p = 2$ et $p = 11$.

Réciproquement, dans tout corps de caractéristique 2 ou 11, $23 = 1$ et l'égalité $X^4 - X^2 + 1 = (X^2 - 5X + 1)(X^2 + 5X + 1)$ est vérifiée.

Conclusion. Les corps de caractéristique 2 ou 11 sont les seuls corps répondant au problème. ◁

5.2. Une sous-algèbre de $\mathbb{R}[X]$

Soit A la sous-algèbre de $\mathbb{R}[X]$ engendrée par X^2 et X^3. Montrer que A n'est pas isomorphe à $\mathbb{R}[X]$.

(**École normale supérieure**)

▷ **Solution.**

• Pour commencer, explicitons la sous-algèbre A. Pour tout entier $k \geqslant 2$, A contient X^k, car on peut écrire, si k est pair, $X^k = (X^2)^{\frac{k}{2}}$ et si k est impair, $X^k = X^3\,(X^2)^{\frac{k-3}{2}}$. Comme A est une sous-algèbre de $\mathbb{R}[X]$, elle contient l'unité de $\mathbb{R}[X]$ et donc $\mathbb{R}$. Ainsi A contient $\underset{k\neq 1}{\mathrm{Vect}}(X^k)$.

Mais il est clair que $\underset{k\neq 1}{\mathrm{Vect}}(X^k)$ est une sous-algèbre de $\mathbb{R}[X]$ qui contient X^2 et X^3. En effet, c'est par définition un sous-espace vectoriel, qui contient 1 et qui est stable pour la multiplication, car pour tout$(k, \ell) \in (\mathbb{N} \setminus \{1\})^2$, on a $X^k X^\ell = X^{k+\ell}$ et $k + \ell \in \mathbb{N} \setminus \{1\}$. C'est donc A.

• Soit Φ un morphisme d'algèbres de $\mathbb{R}[X]$ dans A. Il est déterminé de manière unique par la donnée de $P = \Phi(X)$. On a, pour tout $Q \in \mathbb{R}[X]$, $\Phi(Q) = Q \circ P$ et en particulier, $\deg \Phi(Q) = \deg P \deg Q$. Si Φ était surjective, $\deg P$ diviserait à la fois 2 et 3 puisque X^2 et X^3 seraient dans l'image. Nécessairement $\deg P$ vaudrait 1 ce qui est exclu pour un polynôme de A.

Le morphisme Φ ne peut pas être un isomorphisme de $\mathbb{R}[X]$ sur A.

Conclusion. A n'est pas isomorphe à $\mathbb{R}[X]$. ◁

On remarque cependant que A *et* $\mathbb{R}[X]$ *ont même corps de fractions.*

On peut aussi démontrer que A *n'est pas factoriel, donc n'est pas principal (cf. exercice 3.10), ce qui fournit une autre solution de l'exer-*

cice. En effet, supposons A *factoriel. On se rappelle que* X *n'est pas dans* A. *On en déduit que* X^2 *et* X^3 *sont irréductibles (car un diviseur d'un élément dans* A *est encore un diviseur dans* $\mathbb{R}[X]$*). On écrit alors*

$$(X^3)^2 = (X^2)^3.$$

On remarque que X^2 *divise le côté droit de l'égalité et est premier avec* X^3*, donc avec son carré, ce qui fournit la contradiction voulue.*

Les exercices suivants ont pour thème commun les propriétés arithmétiques de l'anneau $K[X]$ *où* K *est un corps. Comme* $\mathbb{Z}$*, il s'agit d'un anneau euclidien. Cela explique qu'on y dispose des résultats fondamentaux : principalité, théorèmes de Bezout et de Gauss, décomposition en produit de polynômes irréductibles...*

Lorsque le corps de base est $\mathbb{C}$*, les irréductibles de* $\mathbb{C}[X]$ *sont les polynômes de degré* 1*, et les problèmes de divisibilité sont très simplifiés comme le montrent les trois exercices suivants.*

5.3. Condition de divisibilité (1)

Soit a, b deux réels strictement positifs. Quels sont les entiers naturels n tels que $X^2 - (a^2 + b^2)$ divise $X^{2n} - (a^n + b^n)^2$?
(École Polytechnique)

▷ **Solution.**

Il faut et il suffit que $\pm\sqrt{a^2 + b^2}$ soient racines de $X^{2n} - (a^n + b^n)^2$, ce qui donne $(a^2 + b^2)^n = (a^n + b^n)^2$. Visiblement $n = 2$ convient mais pas 0 et 1.

Soit $\rho = \sqrt{a^2 + b^2}$ et $\theta \in \left]0, \frac{\pi}{2}\right[$ tel que $a + ib = \rho e^{i\theta}$. En divisant par ρ^{2n} et en prenant la racine carrée, on obtient, $1 = \cos^n\theta + \sin^n\theta$. Si $n > 2$, on a $\cos^n\theta + \sin^n\theta < \cos^2\theta + \sin^2\theta = 1$, puisque $\sin\theta$ et $\cos\theta$ appartiennent à $]0, 1[$.

Conclusion. La seule solution est $n = 2$. ◁

5.4. Condition de divisibilité (2)

Donner une condition nécessaire et suffisante sur p et q dans $\mathbb{C}$ pour que $X^8 + X^4 + 1$ divise $X^{8m} + pX^{4m} + q$ où $m \in \mathbb{N}^*$ est fixé.
(École polytechnique)

▷ **Solution.**

Le complexe ω est racine du polynôme $P = X^8 + X^4 + 1$ si et seulement si ω^4 est racine de $X^2 + X + 1$, c'est-à-dire si $\omega^4 = j$ ou $\overline{j}$. Les racines de

P sont donc simples : il s'agit des racines quatrièmes de j et des racines quatrièmes de $\overline{j}$. Il en résulte que P divise $Q = X^{8m} + pX^{4m} + q$ si et seulement si toute racine ω de P est racine de Q. Or si ω est racine de P, on a

$$Q(\omega) = (\omega^4)^{2m} + p(\omega^4)^m + q = j^{2m} + pj^m + q \text{ ou } \overline{j}^{2m} + p\overline{j}^m + q.$$

La condition nécessaire et suffisante pour que P divise Q est donc

$$j^{2m} + pj^m + q = \overline{j}^{2m} + p\overline{j}^m + q = 0.$$

Deux cas se présentent :

• Si 3 divise m, alors $j^m = \overline{j}^m = 1$ et la condition cherchée est $\boxed{p + q + 1 = 0}$.

• Si m n'est pas divisible par 3, alors $\{j^{2m} + pj^m + q, \overline{j}^{2m} + p\overline{j}^m + q\}$ est égal à $\{j^2 + pj + q, j + pj^2 + q\}$. On obtient $j^2 + pj + q = j + pj^2 + q = 0$ et on trouve finalement la condition $\boxed{p = q = 1}$. ◁

5.5. Condition pour que $(P')^p$ divise P^q

1. Trouver les polynômes $P \in \mathbb{C}[X]$ tels qu'existent p, q dans $\mathbb{N}^*$ tels que $(P')^p$ divise P^q.

2. Même question dans $K[X]$, où K est un corps quelconque de caractéristique nulle.

(École normale supérieure)

▷ **Solution.**

1. Excepté le polynôme nul, les constantes ne sont pas solution. On suppose dans la suite que $n = \deg P \geqslant 1$. On peut aussi supposer P unitaire et l'écrire sous la forme $P = \prod_{i=1}^{k} (X - z_i)^{\alpha_i}$ où $z_1, \ldots, z_k$ sont des complexes deux à deux distincts. On a alors

$$P'(X) = nQ(X) \prod_{i=1}^{k} (X - z_i)^{\alpha_i - 1},$$

où Q est un polynôme unitaire de degré $k - 1$ ne s'annulant en aucun z_i.

L'hypothèse implique que toute racine de P' est racine de P. Cela impose $Q = 1$ donc $k = 1$ et $P = (X - z_1)^n$. Réciproquement, tous les polynômes $\lambda(X - z_1)^n$ sont solutions.

2. Là encore, on peut supposer que P est unitaire de degré $n \geqslant 1$. On le décompose en

$$P = \prod_{i=1}^{k} P_i^{\alpha_i},$$

où $P_1, \ldots, P_k$ sont des polynômes irréductibles unitaires distincts et $\alpha_1, \ldots, \alpha_k$ des entiers naturels non nuls. Si R est un polynôme irréductible qui divise P', alors R divise P'^p et donc P^q. Étant irréductible, il divise P. Les diviseurs irréductibles de P' sont donc parmi $P_1, \ldots, P_k$. On va déterminer pour chaque P_i son exposant dans P'.

On a $P = P_i^{\alpha_i} Q_i$, où Q_i est premier avec P_i. On en déduit que

$$P' = \alpha_i P_i^{\alpha_i - 1} P_i' Q_i + P_i^{\alpha_i} Q_i' = P_i^{\alpha_i - 1}(\alpha_i P_i' Q_i + P_i Q_i').$$

Ceci montre que $P_i^{\alpha_i - 1}$ divise P'. Montrons que $P_i^{\alpha_i}$ ne divise pas P'. Pour que $P_i^{\alpha_i}$ divise P', il faudrait que P_i divise $P_i' Q_i$. Le corps K étant de caractéristique nulle, on a $\deg P_i' = \deg P_i - 1$. Ainsi P_i ne divise pas P_i', et puisqu'il est irréductible, il est premier avec P_i'. Il est aussi premier avec Q_i par hypothèse, donc premier avec le produit $P_i' Q_i$: il ne divise pas $P_i' Q_i$ et donc $P_i^{\alpha_i}$ ne divise pas P'.

Ainsi P' s'écrit $P' = n \prod_{i=1}^{k} P_i^{\alpha_i - 1}$. Notons d_i le degré de P_i. On a alors $n = \deg P = \sum_{i=1}^{k} \alpha_i d_i$, et $n - 1 = \deg P' = \sum_{i=1}^{k} (\alpha_i - 1) d_i$. On en déduit que $\sum_{i=1}^{k} d_i = 1$. Chaque P_i étant irréductible donc de degré $d_i \geqslant 1$, on en déduit que $k = 1$ et $d_1 = 1$. Le polynôme P_1 étant de degré 1 et unitaire, il existe $z_1 \in K$ tel que $P_1 = X - z_1$ et donc $P = (X - z_1)^{\alpha_1}$. On trouve donc le même résultat que dans $\mathbb{C}[X]$. $\lhd$

Les exercices ci-après concernent des équations dans l'anneau $\mathbb{C}[X]$.

5.6. Une équation fonctionnelle (1)

Trouver les $P \in \mathbb{R}[X]$ tels que $P(X) = P(1 - X)$.
(École Polytechnique)

$\rhd$ **Solution.**

Soit P un polynôme solution. Si α est une racine (complexe) de P, alors $1 - \alpha$ est aussi racine de P. Si α est différent de $\frac{1}{2}$, on a $1 - \alpha \neq \alpha$, et P est divisible par le polynôme

$$(X - \alpha)(X - 1 + \alpha) = X^2 - X + \alpha(1 - \alpha)$$

(on peut noter que tout polynôme de la forme $X^2 - X + \lambda$ est solution du

problème). Notons alors Q le quotient : $P(X) = (X^2 - X + \alpha(1-\alpha))Q(X)$. Si on compose cette identité par $1 - X$, on obtient que $Q(1-X) = Q(X)$. On peut itérer l'argument précédent avec Q. On en déduit que P a la forme suivante :

$$P = R(X) \prod_{i=1}^{p} (X^2 - X + \lambda_i),$$

où les λ_i sont des complexes et où R est un polynôme dont la seule racine complexe est $\frac{1}{2}$. On peut bien entendu supposer P (et donc R) unitaire. On écrit $R = \left(X - \frac{1}{2}\right)^k$. Si on calcule $R(1-X)$ on voit que P est solution si et seulement si k est pair. On peut noter que $\left(X - \frac{1}{2}\right)^{2q} = \left(X^2 - X + \frac{1}{4}\right)^q$. On peut donc conclure que les polynômes unitaires de $\mathbb{C}[X]$ solutions sont ceux qui s'écrivent sous la forme

$$P = \prod_{i=1}^{n} (X^2 - X + \mu_i),$$

où les μ_i sont des complexes pas forcément distincts. Pour obtenir les solutions de $\mathbb{R}[X]$ il suffit de regarder à quelle condition un polynôme de la forme ci-dessus est à coefficients réels. Cela a lieu si et seulement si l'ensemble des μ_i non réels (pris avec multiplicité) est stable par conjugaison. ◁

De l'exercice suivant, nous donnons une solution élémentaire faisant intervenir presque tous les aspects des polynômes : dérivation, considérations arithmétiques, calcul des coefficients... Nous trouverons une autre solution, plus éclairante, de cette équation dans le chapitre 3 (voir l'exercice 3.14), où elle sera interprétée comme la recherche d'unités dans une extension quadratique de l'anneau $\mathbb{C}[X]$.

5.7. Une équation fonctionnelle (2)

Trouver les couples $(P, Q) \in \mathbb{C}[X]^2$ tels que $P^2 = 1 + (X^2 - 1)Q^2$.
(École polytechnique)

▷ **Solution.**

• On commence par une analyse et on se donne une solution (P, Q).

Si $Q = 0$, on obtient $P = \pm 1$. On supposera dans la suite Q non nul. Dans ce cas, on a $n = \deg P \geqslant 1$ et $\deg(1 - P^2) = 2n$ de sorte que $2 + 2\deg(Q) = 2n$, *i.e.* $\deg(Q) = n - 1$. Si a est le coefficient dominant de P et b celui de Q, le coefficient de X^{2n} dans $P^2 + (1 - X^2)Q^2$ est $a^2 - b^2$.

On a donc $a = \pm b$. Observons que $(-P, Q)$, $(P, -Q)$ et $(-P, -Q)$ sont encore des couples solutions et que P et Q sont premiers entre eux par le théorème de Bezout.

En dérivant la relation on obtient

$$2PP' - 2XQ^2 + 2(1 - X^2)QQ' = 0.$$

Il en résulte que $Q|PP'$ et comme P et Q sont premiers entre eux, le théorème de Gauss nous permet d'affirmer que $Q|P'$. Ces deux polynômes étant de même degré, ils sont associés. Et, au vu des coefficients dominants, on a soit $P' = nQ$, soit $P' = -nQ$.

Dans les deux cas, on obtient $n^2QQ' = P'P''$ et $n^2Q^2 = P'^2$. En remplaçant dans la relation obtenue plus haut multipliée par n^2, on en déduit que

$$2(1 - X^2)P'P'' - 2XP'^2 + 2n^2PP' = 0.$$

En simplifiant par $2P' \neq 0$, on obtient l'équation différentielle vérifiée par P

$$(E_n) \qquad n^2P - XP' + (1 - X^2)P'' = 0.$$

Cherchons P sous la forme $a_0 + a_1X + \cdots + a_nX^n$. Après un petit calcul, on voit que l'équation différentielle (E_n) équivaut aux relations suivantes sur les coefficients de P :

(*i*) pas de contrainte sur a_n ;

(*ii*) $a_{n-1} = 0$;

(*iii*) pour tout $k \in [\![0, n-2]\!]$, $a_{k+2} = \dfrac{k^2 - n^2}{(k+1)(k+2)} a_k$.

Il en résulte que tous les coefficients d'indice de parité opposée à celle de n sont nuls (c'est-à-dire que P a la parité de n). Pour les autres on obtient

$$a_{n-2k} = a_n \frac{(-1)^k n(n-k-1)!}{4^k k!(n-2k)!} = a_n \frac{(-1)^k}{4^k} \frac{n}{n-k} C_{n-k}^k.$$

Pour tout $n \geqslant 1$, il existe donc un unique polynôme de degré n, unitaire, solution de l'équation différentielle (E_n). Notons-le A_n. Ses coefficients sont donnés en prenant $a_n = 1$ dans les formules ci-dessus. Il résulte alors de cette analyse, que (P, Q) doit être l'un des couples $(\alpha A_n, \dfrac{\varepsilon}{n}\alpha A_n')$ où $\varepsilon = \pm 1$ et où α est un nombre complexe non nul quelconque.

• Synthèse : soit $P = \alpha A_n$ avec α complexe non nul et $Q = \dfrac{1}{n}P'$ (on peut se limiter à étudier le cas $\varepsilon = 1$). Déterminons les valeurs de α pour lesquelles le couple (P, Q) est effectivement solution. On va essayer de remonter les implications faites lors de l'analyse. En multipliant l'équation (E_n) par $2P'$, on obtient $[n^2P^2]' = [(X^2 - 1)P'^2]'$. Ainsi, il existe une

constante complexe c telle que $n^2P^2 + (1 - X^2)P'^2 = c$. On aimerait avoir $c = n^2$. Or pour calculer c, il suffit de regarder la valeur en 0 du polynôme de gauche : $c = n^2P(0)^2 + P'(0)^2 = n^2\alpha^2A_n(0)^2 + \alpha^2A'_n(0)^2$. Distinguons suivant la parité de n.

⋆ Si $n = 2p$ est pair, le terme de degré 1 de A_n est nul et donc $A'_n(0) = 0$. De plus, en faisant $n = 2p$ et $k = p$ dans les formules précédentes, on obtient

$$A_n(0) = \frac{(-1)^p(2p)(p-1)!}{4^p p!} = \frac{(-1)^p}{2^{2p-1}}.$$

Il y a donc exactement deux valeurs de α, à savoir $\pm 2^{n-1}$, qui conviennent.

⋆ Si $n = 2p + 1$ est impair, cette fois on obtient $A_n(0) = 0$ et $A'_n(0) = (-1)^p \dfrac{n}{4^p}$. Ici encore, on trouve $\alpha = \pm 2^{n-1}$.

En conclusion, les couples solutions de l'équation sont $(\pm 1, 0)$ et les couples $(\pm 2^{n-1}A_n, \pm \dfrac{2^{n-1}}{n} A'_n)$, $n \geqslant 1$. Il s'agit de polynômes réels. ◁

Ces polynômes sont bien connus. Le lecteur aura peut-être reconnu l'équation différentielle vérifiée par le n-ième polynôme de Tchebychev de première espèce T_n. *On a en fait* $T_n = 2^{n-1}A_n$ *et* $U_{n-1} = \dfrac{2^{n-1}}{n} A'_n$, *où* U_{n-1} *est le n-ième polynôme de Tchebychev de seconde espèce. Ces polynômes seront étudiés dans les exercices 5.41 et 5.42.*

On ne manquera pas de rapprocher le théorème de Liouville ci-après du grand théorème de Fermat.

5.8. Un théorème de Liouville (1879)

Soit $n \in \mathbb{N}$, $n \geqslant 3$. Montrer qu'il n'existe pas de polynômes P, Q, R de $\mathbb{C}[X]$ tels que $P^n + Q^n + R^n = 0$ sans que P, Q et R soient tous égaux, à une constante multiplicative près, à un même polynôme.

(École normale supérieure)

Solution.

Notons E l'ensemble des triplets $(P, Q, R) \in \mathbb{C}[X]^3$ vérifiant

$$P^n + Q^n + R^n = 0. \quad (1)$$

Considérons un triplet non nul (P, Q, R) de E. Quitte à diviser P, Q, R par leur pgcd, on peut également supposer que $\text{pgcd}(P, Q, R) = 1$. Il apparaît alors que P, Q, R sont deux à deux premiers entre eux. En effet, si P_0 est un diviseur irréductible de P et Q, P_0 divise $P^n + Q^n = -R^n$ et donc P_0 divise R d'après le lemme d'Euclide. Il en est de même pour

les deux autres cas. Le problème se ramène alors à montrer que P, Q, R sont des polynômes constants.

Supposons, sans perte de généralité, que $\deg(R) \leqslant \deg(Q) \leqslant \deg(P)$. Observons que si R est constant, $P^n + Q^n = \prod_{k=1}^{n} (P - \xi_k Q)$ l'est aussi, $\xi_1, \ldots, \xi_n$ étant les racines n-ièmes de -1. Donc les $P - \xi_k Q$ sont tous constants et on en déduit que P et Q sont constants.

Supposons donc par l'absurde que $\deg R \geqslant 1$. En dérivant la relation (1) et en simplifiant par n, il vient

$$P^{n-1}P' + Q^{n-1}Q' + R^{n-1}R' = 0 \quad (2).$$

En multipliant (1) par R', (2) par R et en faisant la différence, on obtient :

$$P^{n-1}(PR' - P'R) = Q^{n-1}(Q'R - QR').$$

Les polynômes P et Q étant premiers entre eux, on déduit du théorème de Gauss que P^{n-1} divise $Q'R - QR'$. Le polynôme $QR' - Q'R$ n'est pas nul, sinon la fraction $\dfrac{R}{Q}$ aurait une dérivée nulle, elle serait donc constante et Q et R seraient proportionnels, ce qui est impossible car ils sont premiers entre eux et de degré $\geqslant 1$. En regardant les degrés on en déduit que

$$\begin{aligned}(n-1)\deg P &\leqslant \max(\deg(Q'R), \deg(QR')) = \deg Q + \deg R - 1 \\ &\leqslant 2\deg(P) - 1,\end{aligned}$$

ce qui est absurde car $n \geqslant 3$.

Conclusion. E est l'ensemble des triplets (aP, bP, cP) où $P \in \mathbb{C}[X]$ et où (a, b, c) est un triplet de complexes vérifiant $a^n + b^n + c^n = 0$. $\lhd$

Dans le langage de la géométrie algébrique, le résultat de l'exercice montre que la courbe algébrique $X^n + Y^n = 1$ *n'est pas unicursale*[1], *c'est-à-dire n'admet pas de paramétrisation rationnelle, pour* $n \geqslant 3$. *En revanche, le cercle est une courbe unicursale et pour* $n = 2$, *l'équation a des solutions non triviales, par exemple* $(1 - X^2)^2 + (2X)^2 = (1 + X^2)^2$.

5.9. Théorème de Mason (1984)

1. Soit A, B, C trois polynômes de $\mathbb{C}[X]$, non constants, premiers entre eux dans leur ensemble et tels que $A + B = C$. Soit m le nombre de racines complexes distinctes de ABC.

1. PERRIN (D.), *Géométrie algébrique, une introduction*, Savoirs actuels, InterÉditions/CNRS Éditions, 1995, p. 1-5.

Montrer que $A\left(\frac{A'}{A}-\frac{C'}{C}\right)=B\left(\frac{C'}{C}-\frac{B'}{B}\right)$.
En déduire que $\max(\deg A, \deg B, \deg C) < m$.
2. Retrouver le résultat de l'exercice précédent.
(**École normale supérieure**)

Solution.

1. La relation $A+B=C$ conduit à $\frac{C'}{C}=\frac{A'+B'}{A+B}$ qui s'écrit encore

$$A\left(\frac{A'}{A}-\frac{C'}{C}\right)=B\left(\frac{C'}{C}-\frac{B'}{B}\right).$$

Décomposons en éléments simples ces différentes fractions rationnelles. Les polynômes A, B, C sont deux à deux premiers entre eux, car si deux de ces polynômes ont une racine commune z, celle-ci est aussi racine du troisième, car $A+B=C$, et $X-z$ divise $\operatorname{pgcd}(A,B,C)$. Posons

$$A=\alpha\prod_{i=1}^{n_A}(X-a_i)^{\alpha_i}\quad B=\beta\prod_{i=1}^{n_B}(X-b_i)^{\beta_i}\quad C=\gamma\prod_{i=1}^{n_C}(X-c_i)^{\gamma_i},$$

où les a_i, b_i, c_i sont les racines distinctes de A, B, C, respectivement. On a donc $m=n_A+n_B+n_C$. On obtient alors

$$\frac{A'}{A}=\sum_{i=1}^{n_A}\frac{\alpha_i}{X-a_i},\qquad \frac{B'}{B}=\sum_{i=1}^{n_B}\frac{\beta_i}{X-b_i},\qquad \frac{C'}{C}=\sum_{i=1}^{n_C}\frac{\gamma_i}{X-c_i}.$$

Le polynôme $U=\prod_{i=1}^{n_A}(X-a_i)\prod_{i=1}^{n_B}(X-b_i)\prod_{i=1}^{n_C}(X-c_i)$ est un dénominateur commun à ces trois fractions. Il existe donc deux polynômes non nuls P et Q tels que $\frac{A'}{A}-\frac{C'}{C}=\frac{P}{U}$ et $\frac{C'}{C}-\frac{B'}{B}=\frac{Q}{U}$. De plus, les degrés de P et Q sont majorés par $\deg U-1=m-1$ car les fractions sont de degré -1. De l'égalité $AP=BQ$, démontrée plus haut, on déduit, puisque A et B sont premiers entre eux, que A divise Q et B divise P. Il en résulte que $\deg A\leqslant m-1$ et $\deg(B)\leqslant m-1$. Cela vaut aussi pour $C=A+B$. On obtient finalement $\max(\deg A, \deg B, \deg C)\leqslant m-1$.

2. Soit (P,Q,R) un triplet non nul de polynômes premiers entre eux vérifiant $P^n+Q^n+R^n=0$. On a vu dans l'exercice précédent que, si l'un des trois polynômes est constant, les deux autres le sont aussi. Dans le cas contraire, le théorème de Mason conduit à

$$n\max(\deg P, \deg Q, \deg R) < m \leqslant \deg(PQR),$$

et

$$n\max(\deg P, \deg Q, \deg R) < 3\max(\deg P, \deg Q, \deg R).$$

C'est impossible si $n \geqslant 3$. $\lhd$

L'analogue du théorème de Mason pour les entiers aurait d'importantes applications en arithmétique : il s'agit de la conjecture abc, formulée par Masser et Oesterlé[2].

Le résultant donne une condition portant sur les coefficients de deux polynômes pour qu'ils soient premiers entre eux.

5.10. Résultant de deux polynômes

Soit F et G deux polynômes non constants à coefficients complexes de degrés respectifs n et m.

1. On considère

$$\Phi : \begin{array}{ccc} \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X] & \longrightarrow & \mathbb{C}_{n+m-1}[X] \\ (U, V) & \longmapsto & UF + VG \end{array}.$$

Montrer que Φ est bien définie, qu'elle est linéaire, et donner une condition nécessaire et suffisante pour qu'elle soit injective. Écrire la matrice de Φ dans les bases canoniques.

Le déterminant de cette matrice, noté $\mathrm{Res}(F, G)$, est appelé *résultant* des polynômes F et G.

2. Soit $\Gamma = \{(F(t), G(t)) \in \mathbb{C}^2,\ t \in \mathbb{C}\}$. Établir l'existence de $R \in \mathbb{C}[X, Y]$ tel que, pour tout $(x, y) \in \mathbb{C}^2$,

$$(x, y) \in \Gamma \iff R(x, y) = 0.$$

(École polytechnique)

$\rhd$ **Solution.**

1. • Tout d'abord Φ est bien définie : si $(U, V) \in \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X]$, on a $\deg UF \leqslant m - 1 + n$ et $\deg VG \leqslant n - 1 + m$ d'où l'on déduit $\deg(UF + VG) \leqslant m + n - 1$. Ensuite Φ est clairement linéaire.

Supposons Φ injective. Alors Φ est surjective, car

$$\dim\left(\mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X]\right) = m + n = \dim \mathbb{C}_{n+m-1}[X]$$

et il existe $(U, V) \in \mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X]$ tel que $UF + VG = \Phi(U, V) = 1$ donc, d'après le théorème de Bezout, F et G sont premiers entre eux.

Réciproquement, supposons que F et G sont premiers entre eux et considérons (U, V) dans $\mathrm{Ker}\,\Phi$. On obtient $UF = -VG$ donc F divise VG.

2. Pour l'énoncé de cette conjecture nous renvoyons le lecteur intéressé à LANG (S.), *Algebra*. Addison-Wesley, 3e éd., 1993, p. 194-199 ou au chapitre 5 de NATHANSON (M.B.), *Elementary Methods in Number Theory*, GTM 195, Springer-Verlag, 2000.

Comme F est premier avec G, le lemme de Gauss assure que F divise V. Puisque $\deg V < \deg F$, on conclut que $V = 0$. De même, $U = 0$. Donc Φ est injective.

On conclut que Φ est injective si, et seulement si, F et G sont premiers entre eux, ou encore, puisque $\mathbb{C}$ est algébriquement clos si, et seulement si, F et G n'ont aucune racine commune.

• Il s'agit de prendre dans l'espace vectoriel $\mathbb{C}_{m-1}[X] \times \mathbb{C}_{n-1}[X]$ la base $(E_i)_{0 \leqslant i \leqslant n+m-1}$ où E_i vaut $(X^i, 0)$ si $0 \leqslant i \leqslant m-1$ et $(0, X^{i-m})$ si $i \geqslant m$. Sur $\mathbb{C}_{n+m-1}[X]$, il s'agit de la base $(1, X, X^2, \ldots, X^{n+m-1})$. Si $F = a_n X^n + \cdots + a_1 X + a_0$ et $G = b_m X^m + \cdots + b_1 X + b_0$, la matrice de Φ dans ces bases est alors

$$\begin{pmatrix}
a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & \ldots & \ldots & 0 \\
a_1 & a_0 & & \vdots & b_1 & b_0 & & & & \vdots \\
a_2 & a_1 & \ddots & 0 & \vdots & \vdots & \ddots & & & \vdots \\
\vdots & \vdots & & a_0 & b_{m-1} & \vdots & & \ddots & & \vdots \\
\vdots & \vdots & & a_1 & b_m & \vdots & & & \ddots & \vdots \\
\vdots & \vdots & & \vdots & 0 & b_m & & & \ddots & 0 \\
a_{n-1} & \vdots & & \vdots & 0 & 0 & \ddots & & b_1 & b_0 \\
a_n & a_{n-1} & & a_{n-m+1} & 0 & 0 & & \ddots & & b_1 \\
0 & a_n & & \vdots & 0 & 0 & & & \ddots & \vdots \\
0 & & \ddots & \vdots & \vdots & \vdots & & & \ddots & \vdots \\
0 & 0 & \ldots & a_n & 0 & 0 & \ldots & \ldots & 0 & b_m
\end{pmatrix}.$$

Le résultant de F et G, $\mathrm{Res}(F, G)$, est nul si, et seulement si, F et G ont une racine commune. Le *discriminant de* F est le résultant de F et F′. Il est nul si, et seulement si, F a une racine double. Si $F = aX^2 + bX + c$, on trouve $\mathrm{Res}(F, F') = a(4ac - b^2)$ et si $F = X^3 + pX + q$, on obtient $\mathrm{Res}(F, F') = 4p^3 + 27q^2$.

2. Soit $(x, y) \in \mathbb{C}^2$. Dire que $(x, y) \in \Gamma$ équivaut à dire qu'il existe $t \in \mathbb{C}$ tel que $F(t) = x$ et $G(t) = y$. Cela signifie que $F - x$ et $G - y$ ont une racine commune ce qui donne à l'aide du résultant

$$(x, y) \in \Gamma \Longleftrightarrow \mathrm{Res}(F - x, G - y) = 0.$$

On définit $R(X, Y)$ comme étant le déterminant

$$\begin{vmatrix} a_0 - X & 0 & \dots & 0 & b_0 - Y & 0 & \dots & \dots & 0 \\ a_1 & a_0 - X & & \vdots & b_1 & b_0 - Y & & & \vdots \\ a_2 & a_1 & \ddots & 0 & \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & a_0 - X & b_{m-1} & \vdots & & \ddots & \vdots \\ \vdots & \vdots & & a_1 & b_m & \vdots & & & \vdots \\ \vdots & \vdots & & \vdots & 0 & b_m & & \ddots & 0 \\ a_{n-1} & \vdots & & \vdots & 0 & 0 & \ddots & b_1 & b_0 - Y \\ a_n & a_{n-1} & & a_{n-m+1} & 0 & 0 & \ddots & & b_1 \\ 0 & a_n & & \vdots & 0 & 0 & & \ddots & \vdots \\ 0 & & \ddots & \vdots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & a_n & 0 & 0 & \dots & 0 & b_m \end{vmatrix}.$$

On a $R \in \mathbb{C}[X, Y]$ et $(x, y) \in \Gamma \iff R(x, y) = 0$. $\lhd$

On peut définir de la même manière le résultant de deux polynômes de $K[X]$ *pour un corps* K *quelconque. Si* K *n'est pas algébriquement clos, l'annulation du discriminant n'est pas une condition suffisante d'existence d'une racine double pour les polynômes de degré* $\geqslant 4$. *Pour* $K = \mathbb{R}$ *et* $F = X^3 + pX + q$, F *possède trois racines réelles si et seulement si son discriminant* $4p^3 + 27q^2$ *est négatif ou nul.*

Bien qu'il y soit question de racines, les arguments arithmétiques sont essentiels dans l'exercice suivant.

5.11. Caractérisation d'un polynôme par les antécédents de deux points distincts

Soit P et Q deux polynômes non constants de $\mathbb{C}[X]$ tels que l'ensemble des racines de P (resp. $P - 1$) soit égal à l'ensemble des racines de Q (resp. $Q - 1$). Montrer que $P = Q$.

(École polytechnique)

$\rhd$ **Solution.**

• Si P et Q sont des polynômes, on notera $Z(P)$ l'ensemble des racines de P et $P \wedge Q$ le pgcd de P et Q. Soit $n = \deg P \geqslant 1$ et $m = \deg Q \geqslant 1$. On suppose sans perte de généralité que $n \geqslant m$ et on pose $R = P - Q$. On a $\deg R \leqslant n$ et on va prouver que R est nul en montrant qu'il a plus de $n + 1$ racines.

• Par hypothèse, R s'annule sur $Z(P)$ et sur $Z(P - 1)$, ensembles

évidemment disjoints. Déterminons le cardinal de ces ensembles. Le nombre de racines distinctes de P est égal à $\deg P - \deg(P \wedge P')$. En effet, si $P = \lambda \prod_{i=1}^{p} (X - z_i)^{n_i}$, où les z_i sont deux à deux distincts, on obtient $P \wedge P' = \prod_{i=1}^{p} (X - z_i)^{n_i - 1}$ et $\deg(P \wedge P') = (n_1 - 1) + \cdots + (n_p - 1) = n - p$.

• On a donc

$$\begin{aligned} \mathrm{Card}(Z(P)) &= n - \deg(P \wedge P') \quad \text{et} \\ \mathrm{Card}(Z(P-1)) &= \deg(P-1) - \deg((P-1) \wedge (P-1)') \\ &= n - \deg((P-1) \wedge P'). \end{aligned}$$

Mais comme P et $P - 1$ sont premiers entre eux, $(P-1) \wedge P'$ et $P \wedge P'$ sont deux diviseurs premiers entre eux de P'. En particulier, on a

$$\deg((P-1) \wedge P') + \deg(P \wedge P') \leqslant n - 1.$$

Il en résulte que

$$\mathrm{Card}(Z(R)) \geqslant 2n - \deg(P \wedge P') - \deg((P-1) \wedge P') \geqslant 2n - (n-1) = n + 1.$$

On a donc $R = 0$, ce qu'il fallait démontrer. ◁

Bien entendu, on peut remplacer 0 *et* 1 *par deux complexes distincts* a *et* b *quelconques : un polynôme non constant* $P \in \mathbb{C}[X]$ *est uniquement déterminé si on connaît les antécédents de* a *et de* b *par* P *(i.e. les racines de* $P - a$ *et de* $P - b$*).*

Les deux exercices suivants utilisent encore le fait que le nombre de racines complexes distinctes de $P \in \mathbb{C}[X]$ *est égal à* $\deg P - \deg(P \wedge P')$.

5.12. Image réciproque d'une partie finie par un polynôme

> Soit $P \in \mathbb{C}[X]$ non constant et E un sous-ensemble fini de $\mathbb{C}$. Montrer que $|P^{-1}(E)| \geqslant (|E| - 1)\deg P + 1$.
>
> **(École Polytechnique)**

Solution.

Si $w \in \mathbb{C}$, le nombre d'antécédents de w par P est le nombre de racines distinctes de $P(X) - w$. Ce nombre vaut $\deg P - \deg(P - w) \wedge P'$. Notons $w_1, \ldots, w_r$ les éléments de E (avec $r = |E|$). On a donc

$$|P^{-1}(E)| = \sum_{i=1}^{r} (\deg P - \deg((P - w_i) \wedge P')) = r \deg P - \sum_{i=1}^{r} \deg((P - w_i) \wedge P')$$

Or, les polynômes $P - w_i$ sont deux à deux premiers entre eux (ils n'ont aucune racine commune). Il en est donc de même des polynômes $\mathrm{pgcd}(P - w_i, P')$) et comme ils divisent tous P', leur produit aussi. Par conséquent, il vient

$$\sum_{i=1}^{r} \deg((P - w_i) \wedge P') = \deg \prod_{i=1}^{r} ((P - w_i) \wedge P') \leqslant \deg P' = \deg P - 1,$$

et $|P^{-1}(E)| \geqslant |E| \deg P - \deg P + 1$ ce qui est le résultat voulu. $\lhd$

5.13. Sur le nombre d'antécédents d'un point par un polynôme

> Soit $P \in \mathbb{C}[X]$ de degré $d \geqslant 1$. On note $n(z)$ le nombre de racines de l'équation $P(x) = z$. Donner une expression de $\sum_{z \in \mathbb{C}} (d - n(z))$.
>
> **(École Polytechnique)**

$\rhd$ **Solution.**

Cet exercice utilise encore la formule

$$n(z) = d - \deg((P - z) \wedge P').$$

La somme considérée a l'air infinie, mais il n'y a en fait qu'un nombre fini de nombres complexes z tels que $d - n(z)$ soit non nul (z doit être l'image par P d'une racine de P' sans quoi $P - z$ et P' sont premiers entre eux). Notons $u_1, ..., u_p$ les racines distinctes de P' et n_i l'ordre de multiplicité de u_i. Supposons dans un premier temps que les nombres complexes $P(u_i)$ sont deux à deux distincts. Dans ce cas, on a pour tout i, $(P - P(u_i)) \wedge P' = (X - u_i)^{n_i}$ car u_j n'est pas racine de $P(X) - P(u_i)$ pour $j \neq i$, et u_i est racine d'ordre $n_i + 1$ de $P(X) - P(u_i)$ (il suffit d'écrire la formule de Taylor en u_i pour P pour s'en convaincre). On a alors

$$\begin{aligned}\sum_{z \in \mathbb{C}} (d - n(z)) &= \sum_{z \in \mathbb{C}} \deg((P - z) \wedge P') = \sum_{i=1}^{p} \deg((P - P(u_i)) \wedge P') \\ &= \sum_{i=1}^{p} n_i = \deg P' = d - 1.\end{aligned}$$

Que se passe-t-il maintenant si certains des $P(u_i)$ sont égaux ? Soit z l'une des valeurs $P(u_i)$ et supposons que z soit atteint avec $u_{i_1}, \ldots, u_{i_s}$. Dans ce cas, le pgcd de $P(X) - z$ et P' est égal à $\prod_{j=1}^{s} (X - u_{i_j})^{n_{i_j}}$ et son degré est égal à la somme des ordres de multiplicité des racines u_{i_j}.

Il en résulte que le résultat est identique. Dans tous les cas, la somme cherchée vaut $d-1$. ◁

Si L *est un sur-corps de* K, *deux polynômes* P, Q *de* K[X] *peuvent être regardés comme des polynômes de* L[X]. *Le pgcd de* P *et* Q *ne va pas dépendre du corps dans lequel on se place : il est obtenu par l'algorithme d'Euclide et ses coefficients appartiennent au plus petit corps contenant les coefficients de* P *et* Q. *On dira que le pgcd est invariant par extension de corps. L'exercice suivant utilise ce fait.*

5.14. Polynôme rationnel inséparable de degré 5

1. Soit P un polynôme irréductible de $\mathbb{Q}[X]$. Démontrer que P n'a pas de racine double dans $\mathbb{C}$.

2. Soit $P \in \mathbb{Q}[X]$ de degré 5. On suppose que P admet une racine multiple dans $\mathbb{C}$. Montrer que P possède une racine dans $\mathbb{Q}$.

(**École normale supérieure**)

▷ **Solution.**

1. Comme $1 \leqslant \deg P' < \deg P$, les polynômes P' et P sont premiers entre eux dans $\mathbb{Q}[X]$, puisque P est irréductible. Ils le sont donc encore dans $\mathbb{C}[X]$ par invariance du pgcd par extension de corps. Si α était une racine double de P dans $\mathbb{C}$, on aurait $P(\alpha) = P'(\alpha) = 0$ et $X - \alpha$ serait un facteur commun à P et P' dans $\mathbb{C}[X]$. On aboutit à une contradiction.

2. Notons α une racine multiple complexe de P. Supposons par l'absurde, que P n'ait pas de racine rationnelle et regardons sa décomposition en éléments irréductibles dans $\mathbb{Q}[X]$. Il ne peut pas y avoir de facteur de degré 1 ; le polynôme P ne pouvant être irréductible d'après la première question, il s'écrit $P = QR$ avec $\deg Q = 2$, $\deg R = 3$ et Q, R tous deux irréductibles dans $\mathbb{Q}[X]$, puisque sans racine rationnelle.

Les polynômes Q et R ne peuvent avoir α comme racine commune dans $\mathbb{C}$. En effet, si on considère D le pgcd de Q et R dans $\mathbb{Q}[X]$, il est égal à 1 puisque Q et R sont deux polynômes irréductibles non proportionnels. Mais D est aussi le pgcd de Q et R en tant que polynômes de $\mathbb{C}[X]$, du fait de l'invariance du pgcd par extension de corps. Par conséquent, si on avait $Q(\alpha) = R(\alpha) = 0$, $X - \alpha$ diviserait D, qui serait de degré $\geqslant 1$, ce qui n'est pas le cas.

Par conséquent, comme $(X-\alpha)^2$ divise P, $(X-\alpha)^2$ divise soit Q, soit R. Mais alors Q ou R est un polynôme irréductible ayant une racine multiple dans $\mathbb{C}$, ce qui est impossible.

L'hypothèse faite au départ est fausse : P possède donc une racine rationnelle. ◁

Le thème commun aux exercices qui suivent est l'irréductibilité de polynômes à coefficients entiers. Rappelons qu'un polynôme non nul P *de* $\mathbb{Z}[X]$ *est dit irréductible si l'écriture* $P = QR$ *avec* $(Q, R) \in \mathbb{Z}[X]^2$ *impose* $Q = \pm 1$ *ou* $R = \pm 1$.

5.15. Un polynôme irréductible de $\mathbb{Z}[X]$

Soit $n \geqslant 2$ et $a_1, \ldots, a_n$ des éléments de $\mathbb{Z}$ deux à deux distincts. Montrer que le polynôme $P = (X - a_1)(X - a_2)\ldots(X - a_n) - 1$ est irréductible dans $\mathbb{Z}[X]$.

(École normale supérieure)

▷ **Solution.**

Supposons que $P = QR$ où Q et R sont dans $\mathbb{Z}[X]$. On a, pour tout k de $[\![1, n]\!]$, $Q(a_k)R(a_k) = P(a_k) = -1$ et donc, soit $Q(a_k) = 1 = -R(a_k)$, soit $Q(a_k) = -1 = -R(a_k)$, puisque ce sont des entiers. Dans les deux cas, on a $Q(a_k) + R(a_k) = 0$ Le polynôme $Q + R$ s'annule en n points distincts. Si $\deg(Q+R) < n$, on a alors $Q+R = 0$ et $P = -Q^2$ ce qui est absurde car $P(x)$ serait négatif pour tout x réel et de limite égale à $+\infty$ en $+\infty$. On a donc $\deg(Q + R) = n$. Mais alors, Q ou R est constant. Le produit des coefficients dominants de Q et R étant égal à 1, on a donc soit $Q = \pm 1$, soit $R = \pm 1$. Ainsi, P est irréductible dans $\mathbb{Z}[X]$. ◁

L'exercice suivant établit un critère fort utile pour montrer qu'un polynôme à coefficients entiers est irréductible.

5.16. Critère d'Eisenstein

1. a. On dit qu'un polynôme non nul de $\mathbb{Z}[X]$ est *primitif* si le pgcd de ses coefficients est égal à 1. Montrer que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est primitif.

b. Pour $A \in \mathbb{Z}[X]$ non nul, on appelle *contenu de* A, et on note $c(A)$ le pgcd des coefficients de A. Soit A et B deux polynômes non nuls de $\mathbb{Z}[X]$. Montrer que $c(AB) = c(A)c(B)$.

2. Soit $A = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que :

(*i*) p ne divise pas a_n ;

(*ii*) p divise $a_0, a_1, \ldots, a_{n-1}$;

(*iii*) p^2 ne divise pas a_0.

Montrer que A est irréductible dans $\mathbb{Q}[X]$.

(École normale supérieure)

Solution.

1.a. Soit $A = \sum_{k=0}^{n} a_k X^k$, $B = \sum_{k=0}^{m} b_k X^k$ des polynômes à coefficients entiers et $C = \sum_{k=0}^{m+n} c_k X^k = AB$. Supposons A et B primitifs et montrons, en raisonnant par l'absurde, que C est primitif. Si ce n'est pas le cas, il existe un nombre premier p qui divise tous les c_k. Pour tout $P \in \mathbb{Z}[X]$, on note $\overline{P}$ le projeté de P dans $(\mathbb{Z}/p\mathbb{Z})[X]$: si $P = \sum_{k\in\mathbb{N}} s_k X^k$, $\overline{P} = \sum_{k\in\mathbb{N}} \overline{s_k} X^k$ où $\overline{s_k}$ est la classe de s_k modulo p. Comme p divise tous les c_k, on a $\overline{C} = 0$ et donc $\overline{A}\ \overline{B} = \overline{AB} = \overline{C} = 0$. Mais $(\mathbb{Z}/p\mathbb{Z})[X]$ est intègre, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, donc on a $\overline{A} = 0$ ou $\overline{B} = 0$. Autrement dit, p divise tous les coefficients de A ou tous les coefficients de B. Ceci est exclu.

On conclut que le produit de deux polynômes primitifs de $\mathbb{Z}[X]$ est encore primitif.

b. On peut écrire $AB = c(A)c(B)\dfrac{A}{c(A)}\dfrac{B}{c(B)}$. Les polynômes $\dfrac{A}{c(A)}$ et $\dfrac{B}{c(B)}$ sont alors primitifs, donc leur produit aussi d'après la question précédente et le contenu de AB est $c(A)c(B)$.

2. Montrons que si A n'est pas irréductible dans $\mathbb{Q}[X]$, alors il peut s'écrire $A = BC$ avec B et C dans $\mathbb{Z}[X]$ de degrés strictement inférieurs à celui de A.

Soit $\alpha = c(A)$ et $A' = \dfrac{1}{\alpha}A \in \mathbb{Z}[X]$; A' est primitif. Comme A est composé, par hypothèse, A' l'est aussi et on peut écrire $A' = B'C'$, avec B' et C' dans $\mathbb{Q}[X]$ de degrés strictement inférieurs à celui de A. Notons β (resp. γ) le produit des dénominateurs des coefficients de B' (resp. C'). Alors les polynômes $B = \beta B'$ et $C = \gamma C'$ sont dans $\mathbb{Z}[X]$ et $\beta\gamma A' = BC$. En passant aux contenus, on obtient $\beta\gamma = \beta\gamma c(A') = c(B)c(C)$. Par conséquent, on a

$$A = \alpha\left(\frac{1}{\beta}B\right)\left(\frac{1}{\gamma}C\right) = \alpha\left(\frac{1}{c(B)}B\right)\left(\frac{1}{c(C)}C\right) = \left(\frac{\alpha}{c(B)}B\right)\left(\frac{1}{c(C)}C\right)$$

et $\dfrac{\alpha}{c(B)}B$ et $\dfrac{1}{c(C)}C$ sont à coefficients entiers de degré strictement inférieur à celui de A.

Passons à la démonstration proprement dite du critère d'Eisenstein. Raisonnons par l'absurde et supposons A non irréductible. D'après ce qui précède, il existe B et C dans $\mathbb{Z}[X]$, de degrés strictement inférieurs à n, tels que $A = BC$. Écrivons alors $B = b_k X^k + \cdots + b_1 X + b_0$ et $C = c_\ell X^\ell + \cdots + c_1 X + c_0$, avec $k = \deg B$ et $\ell = \deg C$. Comme dans la question précédente, on projette l'égalité $A = BC$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. On obtient $\overline{a_n}X^n = \overline{B}\ \overline{C}$. Les polynômes $\overline{B}$ et $\overline{C}$ sont de degrés respectifs k et ℓ car $b_k c_\ell = a_n$ n'étant pas divisible par p, $\overline{b_k} \neq 0$ et $\overline{c_\ell} \neq 0$. Par

unicité de la décomposition en irréductibles dans $(\mathbb{Z}/p\mathbb{Z})[X]$, $\overline{B} = \overline{b_k}X^k$ et $\overline{C} = \overline{c_\ell}X^\ell$. On a alors $\overline{b_0} = \overline{c_0} = 0$ c'est-à-dire $p|b_0$ et $p|c_0$. On en déduit que p^2 divise $a_0 = b_0c_0$ ce qui contredit (iii). $\lhd$

Il résulte du critère d'Eisenstein que le polynôme $X^n - 2$ est irréductible dans $\mathbb{Q}[X]$ pour tout entier $n \geqslant 1$ (prendre $p = 2$), ce qui prouve qu'il y a dans $\mathbb{Q}[X]$ des irréductibles de tout degré. Voici une autre application du critère d'Eisenstein.

5.17. Irréductibilité de Φ_p dans $\mathbb{Q}[X]$

Soit $\omega = e^{\frac{2i\pi}{p}}$, où p est premier, et $\Phi_p = X^{p-1} + \cdots + X + 1$ (p-ième polynôme cyclotomique).

1. On admet que Φ_p est irréductible dans $\mathbb{Q}[X]$. Démontrer que l'ensemble $\mathcal{I}$ des polynômes annulateurs de ω dans $\mathbb{Q}[X]$ est $\Phi_p\mathbb{Q}[X]$.

2. Montrer que le polynôme $(X+1)^{p-1} + \cdots + (X+1) + 1$ est irréductible dans $\mathbb{Q}[X]$ (on pourra utiliser l'exercice précédent).

3. En déduire que Φ_p est irréductible dans $\mathbb{Q}[X]$.

4. Démontrer que $\mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right] = \{Q(\omega), Q \in \mathbb{Q}[X]\}$ est un corps, appelé *corps cyclotomique*. Quelle est sa dimension comme espace vectoriel sur $\mathbb{Q}$?

(École normale supérieure)

$\rhd$ **Solution.**

1. Posons $\mathcal{I} = \{Q \in \mathbb{Q}[X], Q(\omega) = 0\}$. C'est un idéal de $\mathbb{Q}[X]$ en tant que noyau du morphisme d'algèbre $Q \in \mathbb{Q}[X] \longmapsto Q(\omega) \in \mathbb{C}$. Nous savons que tout idéal de $\mathbb{Q}[X]$ est principal. Comme I est non nul, il existe donc un unique polynôme unitaire Q tel que $\mathcal{I} = Q\mathbb{Q}[X]$. Or, nous savons que $\Phi_p(\omega) = 0$, puisque $(\omega - 1)\Phi_p(\omega) = \omega^p - 1 = 1 - 1 = 0$. On en déduit que Q divise Φ_p, puisque $\Phi_p \in \mathcal{I}$. Comme $Q \neq 1$ et comme Φ_p est supposé irréductible, on a nécessairement $Q = \Phi_p$. On conclut

$$\boxed{\mathcal{I} = \Phi_p\mathbb{Q}[X]}.$$

2. Posons $U = (X+1)^{p-1} + \cdots + (X+1) + 1 = \Phi_p(X+1)$, c'est-à-dire

$$\begin{aligned} U &= \frac{1 - (X+1)^p}{1 - (X+1)} = \frac{(X+1)^p - 1}{X} \\ &= X^{p-1} + C_p^{p-1}X^{p-2} + \cdots + C_p^2X + C_p^1 \in \mathbb{Z}[X]. \end{aligned}$$

Pour montrer que U est irréductible, nous allons utiliser le critère d'Eisenstein de l'exercice précédent avec le nombre premier p. Les hypothèses (i) et (iii) sont clairement vérifiées. Il s'agit de vérifier (ii), c'est-à-dire que les C_p^k sont divisibles par p pour $1 \leqslant k \leqslant p-1$. En effet,

si $1 \leqslant k \leqslant p-1$, on a $k!C_p^k = p(p-1)\dots(p-k+1)$. Donc p divise $k!C_p^k$. Comme $k < p$, p est premier avec $k!$ donc divise C_p^k.

On conclut à l'aide du critère d'Eisenstein que U est irréductible.

3. Supposons que Φ_p est composé et posons $\Phi_p = BC$ où B, C sont dans $\mathbb{Q}[X]$ avec $\deg B < \deg \Phi_p$ et $\deg C < \deg \Phi_p$. On en déduit que $U = \Phi_p(X+1) = B(X+1)C(X+1)$, avec $\deg B(X+1) = \deg B < \deg U$ et $\deg C(X+1) = \deg C < \deg U$. Il en résulte que U n'est pas irréductible, ce qui est faux.

Conclusion. $\Phi_p = X^{p-1} + \dots + X + 1$ est irréductible dans $\mathbb{Q}[X]$.

4. Le polynôme Φ_p est le polynôme unitaire de plus petit degré annulant ω. Donc la famille $(1, \omega, \dots, \omega^{p-2})$ est libre sur $\mathbb{Q}$ (toute combinaison linéaire non triviale nulle offrirait un polynôme non nul, de degré strictement inférieur à $p-1$, annulant ω). Si $Q \in \mathbb{Q}[X]$ et si on note R le reste de Q modulo Φ_p, il vient $Q(\omega) = R(\omega)$ puisque $\Phi_p(\omega) = 0$, ce qui montre que

$$\mathbb{Q}[\omega] = \mathrm{Vect}(1, \omega, \dots, \omega^{p-2}).$$

Le système $(1, \omega, \dots, \omega^{p-2})$ est donc une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}[\omega]$, d'où l'on déduit

$$\boxed{\dim \mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right] = p-1}.$$

Reste à démontrer que $\mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right]$ est un corps. En premier lieu, $\mathbb{Q}[\omega]$ est l'image par le morphisme d'algèbre $P \longmapsto P(\omega)$ de l'algèbre $\mathbb{Q}[X]$; c'est donc une sous-algèbre de la $\mathbb{Q}$-algèbre $\mathbb{C}$ et en particulier un sous-anneau de $\mathbb{C}$. Soit x un élément non nul de $\mathbb{Q}[\omega]$. Il existe $R \in \mathbb{Q}[X]$ non nul de degré strictement inférieur à $p-1$ tel que $x = R(\omega)$. Comme Φ_p est irréductible, il est premier avec R. D'après le théorème de Bezout, il existe $(U, V) \in \mathbb{Q}[X]^2$ tel que $U\Phi_p + VR = 1$. En évaluant en ω, cela donne $U(\omega) \times 0 + V(\omega)x = 1$, soit $V(\omega)x = 1$ et $V(\omega) \in \mathbb{Q}[\omega]$ est l'inverse de x.

Conclusion. $\mathbb{Q}\left[e^{\frac{2i\pi}{p}}\right]$ est un corps de dimension $p-1$ sur $\mathbb{Q}$. $\lhd$

Les racines de Φ_p sont les racines p-ièmes de l'unité différentes de 1. Plus généralement, pour $n \in \mathbb{N}^*$, on note Π_n l'ensemble des racines primitives n-ièmes de l'unité (rappelons qu'une racine n-ième est primitive si, et seulement si, elle engendre le groupe multiplicatif U_n, et que $\mathrm{Card}\,\Pi_n = \varphi(n)$, *où φ est l'indicateur d'Euler) et $\Phi_n = \prod_{\xi \in \Pi_n} (X - \xi)$. On peut alors montrer que Φ_n appartient à $\mathbb{Z}[X]$ (ce qui est fait dans l'exercice 4.18) et est irréductible dans $\mathbb{Q}[X]$, ce qui constitue le théorème de Dirichlet* [3]. *Il en résulte que si ξ est un élément de Π_n, alors $\mathbb{Q}[\xi]$ est un corps de dimension $\varphi(n)$ sur $\mathbb{Q}$.*

3. PERRIN (D.), *Cours d'algèbre*. Ellipses, 1996.

5.18. Décomposition de $1 + X + X^2 + \cdots + X^{n-1}$

On suppose que $1 + X + X^2 + \cdots + X^{n-1} = P(X)Q(X)$ où P, Q sont deux polynômes réels unitaires à coefficients positifs ou nuls. Montrer que les coefficients de P et Q sont dans $\{0, 1\}$.

(École normale supérieure)

▷ **Solution.**

• Les racines complexes de $1 + X + X^2 + \cdots + X^{n-1}$ (et donc celles de P ou Q) sont les racines n-ièmes de l'unité différentes de 1. La seule racine réelle est -1, si n est pair. Les facteurs du second degré de P sont de la forme $(X - \alpha)(X - \overline{\alpha}) = X^2 - 2\,\mathrm{Re}(\alpha)X + 1$, où α est une racine n-ième de l'unité. Comme P est unitaire, il est produit de tels facteurs avec éventuellement $X + 1$ pour n pair, de sorte que le terme constant de P est égal à 1. On remarque d'autre part que si α est racine de P, $\dfrac{1}{\alpha} = \overline{\alpha}$ est aussi racine de P, avec la même multiplicité égale à 1 (un tel polynôme est appelé polynôme réciproque). Les polynômes P et $\widehat{P} = X^{\deg(P)}P\left(\dfrac{1}{X}\right)$ ont donc les mêmes racines, toutes simples : ils sont proportionnels. Étant unitaires, ils sont égaux. Si $P = \sum\limits_{k=0}^{p} a_k X^k$, où p est le degré de P, alors $\widehat{P} = \sum\limits_{k=0}^{p} a_{p-k} X^k$. On en déduit que l'on a, pour tout $k \in [\![0, p]\!]$, $a_{p-k} = a_k$. On obtient évidemment un résultat analogue pour le polynôme Q, dont on notera q le degré et $b_0, \ldots, b_q$ les coefficients.

• Supposons par exemple $p \leqslant q$. Considérons, pour $0 \leqslant k \leqslant p$, le coefficient d'ordre k de PQ ; il est égal à 1. On obtient $\sum\limits_{i=0}^{k} a_{k-i} b_i = 1$. En particulier, pour $k = p$, on a, compte tenu de la symétrie des coefficients de P,

$$1 = \sum_{i=0}^{p} a_{p-i} b_i = \sum_{i=0}^{p} a_i b_i.$$

Sachant que $a_0 = b_0 = 1$ et que tous les coefficients sont positifs, on en déduit que, pour $1 \leqslant i \leqslant p$, on a $a_i b_i = 0$. On observe en particulier que $b_p = 0$ et donc que $q > p$.

On peut ensuite montrer simplement, par récurrence sur k entier entre 0 et p, que a_k et b_k sont dans $\{0, 1\}$. C'est vrai pour $k = 0$ (car $a_0 = b_0 = 1$). Si la propriété est établie jusqu'au rang $k - 1$, alors

$$a_k + b_k = a_k b_0 + a_0 b_k = 1 - \sum_{i=1}^{k-1} a_{k-i} b_i$$

est un entier plus petit que 1 et positif par hypothèse, donc égal à 0 ou 1. Nous avons le résultat voulu puisque nous savons que $a_k = 0$ ou $b_k = 0$.

Considérons ensuite, pour $p+1 \leqslant k \leqslant q$, le coefficient d'ordre k de PQ. On obtient $1 = \sum_{i=k-p}^{k} a_{k-i}b_i$, et donc

$$b_k = 1 - \sum_{i=k-p}^{k-1} a_{k-i}b_i.$$

Nous savons déjà que, pour $0 \leqslant k \leqslant p$, les coefficients a_k et b_k sont dans $\{0,1\}$. Une récurrence semblable à la précédente permet de démontrer que $b_k \in \{0,1\}$, pour $p+1 \leqslant k \leqslant q$. ◁

On peut se demander s'il existe de telles décompositions du polynôme $1 + X + X^2 + \cdots + X^{n-1}$. *L'exercice précédent démontre que si n est premier, ce polynôme est irréductible dans* $\mathbb{Q}[X]$. *Il faut donc avoir* $P = 1$ *ou* $Q = 1$. *Si $n = ab$ avec a et b entiers naturels, $a \neq 1$ et $b \neq 1$, on peut écrire*

$$\begin{aligned} 1 + X + X^2 + \cdots + X^{n-1} &= \frac{X^n - 1}{X - 1} = \frac{(X^a)^b - 1}{X - 1} \\ &= \frac{X^a - 1}{X - 1}\left(\sum_{i=0}^{b-1} X^{ai}\right) = \sum_{i=0}^{a-1} X^i \times \sum_{i=0}^{b-1} X^{ai}, \end{aligned}$$

ce qui est une décomposition non triviale du type considéré.

Nous allons maintenant nous intéresser aux fonctions polynomiales et à leurs propriétés. Si K *est un corps et* A *une partie infinie de* K, *il y un isomorphisme entre l'algèbre* K[X] *et l'algèbre des fonctions polynomiales de* A *dans* K. *Cela permet d'identifier ces deux algèbres, ce que font les exercices suivants.*

5.19. Polynômes complexes d'image réelle

> Quels sont les polynômes complexes P dont l'image est incluse dans $\mathbb{R}$?
>
> **(École normale supérieure)**

▷ **Solution.**

Si $P \in \mathbb{C}[X]$ est de degré supérieur ou égal à 1, la fonction polynôme associée à P est une surjection de $\mathbb{C}$ dans lui-même. En effet, pour tout complexe w, l'équation $P(z) = w$ admet une solution par le théorème de d'Alembert.

Conclusion. Si $P(\mathbb{C}) \subset \mathbb{R}$, c'est que P est un polynôme constant réel. $\lhd$

L'exercice suivant s'intéresse aux sommes de deux carrés dans l'anneau $\mathbb{R}[X]$. La situation est nettement plus simple que dans $\mathbb{Z}$.

5.20. Sommes de deux carrés dans $\mathbb{R}[X]$

Soit $P \in \mathbb{R}[X]$. Montrer que $P(x) \geqslant 0$ pour tout $x \in \mathbb{R}$ si, et seulement si, P s'écrit $A^2 + B^2$ avec A et B dans $\mathbb{R}[X]$.
(École polytechnique)

$\rhd$ **Solution.**

Si P est somme de deux carrés de polynômes réels, il est évident que $P(x) \geqslant 0$ pour tout x réel.

Réciproquement, supposons que $P(x) \geqslant 0$ pour tout x réel. Le cas P constant étant trivial, supposons $\deg P \geqslant 1$. En considérant la limite de P en $+\infty$ qui ne peut être que $+\infty$, il apparaît que le coefficient dominant de P est positif. Si a est une racine réelle de P d'ordre n, P s'écrit $(X-a)^n Q$ avec $Q(a) \neq 0$. En particulier, Q étant continu sur $\mathbb{R}$, il garde un signe constant au voisinage de a. Comme P ne change pas de signe en a, n est nécessairement pair. Par conséquent, P se décompose sur $\mathbb{C}$ de la manière suivante

$$P = \lambda \prod_{i=1}^{p} (X - a_i)^{\alpha_i} \prod_{j=1}^{q} (X - \lambda_j)^{n_j} (X - \overline{\lambda_j})^{n_j},$$

où $a_1, \ldots, a_p$ sont les racines réelles de P, $\alpha_1, \ldots, \alpha_p$ sont des entiers pairs et $\lambda \in \mathbb{R}_+^*$ (dans le second produit on a associé chaque racine non réelle avec sa conjuguée qui a le même ordre de multiplicité puisque P est réel). Si on pose

$$C = \sqrt{\lambda} \prod_{i=1}^{p} (X - a_i)^{\frac{\alpha_i}{2}} \prod_{j=1}^{q} (X - \lambda_j)^{n_j},$$

on constate que $P = C\overline{C}$. En écrivant $C = A + iB$, avec A et B dans $\mathbb{R}[X]$, on obtient $P = (A + iB)(A - iB) = A^2 + B^2$. $\lhd$

L'exercice suivant caractérise les polynômes réels prenant des valeurs positives sur $[-1, 1]$.

5.21. Polynômes positifs sur $[-1,1]$

Soit $P \in \mathbb{R}[X]$ tel que $P(x) \geqslant 0$, pour tout x dans $[-1,1]$.

1. On suppose que P est de degré inférieur ou égal à 2. Montrer qu'on peut écrire $P = \alpha(X-a)^2 + \beta(1-X^2)$, avec $\alpha \geqslant 0$, $\beta \geqslant 0$ et $a \in [-1,1]$.

2. On revient au cas général. Montrer l'existence de A et B dans $\mathbb{R}[X]$ tel que $P = A^2 + (1-X^2)B^2$.

(École polytechnique)

▷ **Solution.**

1. Supposons d'abord que P s'annule sur $[-1,1]$, en a.

Si $a \in]-1,1[$, P ne change pas de signe en a, donc a ne peut pas être racine simple de P. Si P est de degré 2, il s'écrit donc $\alpha(X-a)^2$, avec $\alpha > 0$; sinon, c'est le polynôme nul, ce qui revient à prendre $\alpha = 0$. Si $a \in]-1,1[$, P a donc la forme voulue, avec $\beta = 0$.

Examinons maintenant le cas où P s'annule seulement en $a = \pm 1$. Quitte à considérer le polynôme $P(-X)$, on peut supposer que $a = 1$. Il existe alors $(b,c) \in \mathbb{R}^2$ tel que $P = (1-X)(bX+c)$. De l'hypothèse, on déduit que $bx + c \geqslant 0$ pour tout $x \in [-1,1]$, ce qui équivaut à $b + c \geqslant 0$ et $-b+c \geqslant 0$. Alors P est de la forme voulue, avec $a = 1$, si et seulement si $P = (1-X)(\alpha(1-X)+\beta(1+X))$, c'est-à-dire $b = -\alpha+\beta$ et $c = \alpha+\beta$, ce qui s'obtient en posant $\alpha = \frac{1}{2}(c-b)$ et $\beta = \frac{1}{2}(c+b)$. Les réels α et β sont bien positifs d'après les conditions trouvées sur b et c.

Dans le cas où P est strictement positif sur $[-1,1]$, nous allons montrer qu'en lui soustrayant un terme de la forme $\beta(1-X^2)$, on peut se ramener au cas précédent. Soit E l'ensemble des $k > 0$ tels que $P - k(1-X^2)$ soit positif ou nul sur $[-1,1]$. Puisque P possède sur $[-1,1]$ un minimum strictement positif m, E n'est pas vide : si $0 < k \leqslant m$, k appartient à E. Cet ensemble est majoré, par exemple par $P(0)$. Soit β sa borne supérieure. Le polynôme $Q = P - \beta(1-X^2)$ s'annule sur $[-1,1]$, sinon le même raisonnement appliqué à Q permettrait d'exhiber $k > 0$ tel que $Q - k(1-X^2)$ soit positif ou nul sur $[-1,1]$, ce qui contredirait la définition de β. Si a est une racine de Q sur $[-1,1]$, a est différent de ± 1, sinon P s'annulerait en ± 1. Le polynôme Q est positif sur $[-1,1]$ et s'annule en $a \in]-1,1[$. Nous avons montré qu'alors il existe $\alpha \geqslant 0$ tel que $Q = \alpha(X-a)^2$, ce qui conduit à $P = \alpha(X-a)^2 + \beta(1-X^2)$, avec $\alpha \geqslant 0$ et $\beta \geqslant 0$, ce qui est le résultat demandé.

2. Montrons pour commencer que P peut s'écrire comme produit de polynômes de degré inférieur ou égal à 2, positifs sur $[-1,1]$. Notons $a_1, \ldots, a_k$ les racines de P appartenant à $]-1,1[$. Puisque P ne change pas de signe en a_i, la multiplicité de a_i est paire ; on la note $2n_i$. Le

polynôme P se décompose donc en

$$P = \prod_{i=1}^{k}(X - a_i)^{2n_i} \prod_{j=1}^{\ell} P_j,$$

où $P_1, P_2, \ldots, P_\ell$ sont des polynômes irréductibles, donc de degré inférieur ou égal à 2, ne s'annulant pas sur $]-1,1[$. Comme P est positif sur $[-1,1]$, on en déduit que $\prod_{j=1}^{\ell} P_j$ est strictement positif sur $]-1,1[$. Quitte à multiplier certains P_j par -1, on peut supposer que $P_1, \ldots, P_\ell$ sont tous strictement positifs sur $]-1,1[$ et donc positifs sur $[-1,1]$. On a montré que P s'écrit comme produit de polynômes de la forme $(X - a_i)^2$ ou P_j, tous positifs sur $[-1,1]$ et de degré inférieur ou égal à 2.

D'après la question 4, chacun de ces polynômes peut s'écrire

$$\alpha(X-a)^2 + \beta(1 - X^2) = (\sqrt{\alpha}(X-a))^2 + (1 - X^2)(\sqrt{\beta})^2,$$

ce qui est de la forme $A^2 + (1 - X^2)B^2$. Pour conclure, il reste à montrer qu'un produit de polynômes de cette forme est encore un polynôme ayant la même forme. Le montrer pour deux polynômes est d'ailleurs suffisant. Cela résulte alors de l'identité de Lagrange, valable dans tout anneau :

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

Formellement, on est tenté d'écrire, pour des polynômes A, B, C, D,

$$\begin{aligned} Q &= \left(A^2 + (1 - X^2)B^2\right)\left(C^2 + (1 - X^2)D^2\right) \\ &= \left(A^2 + (\sqrt{1 - X^2}B)^2\right)\left(C^2 + (\sqrt{1 - X^2}D)^2\right) \\ &= \left(AC - (1 - X^2)BD\right)^2 + \left(\sqrt{1 - X^2}(AD + BC)\right)^2 \\ &= \left(AC - (1 - X^2)BD\right)^2 + (1 - X^2)(AD + BC)^2. \end{aligned}$$

L'égalité entre Q et le dernier terme peut se vérifier directement. Elle démontre le résultat voulu. Elle tient moins du miracle qu'il n'en paraît puisque ce calcul se justifierait en se plaçant sur une «extension» de $\mathbb{R}[X]$ dans laquelle $1 - X^2$ aurait une racine. ◁

Il est évident que réciproquement, tout polynôme à coefficients réels qui s'écrit $A^2 + (1 - X^2)B^2$ *est positif sur* $[-1,1]$.

Voici encore un exercice sur les polynômes réels positifs. On n'oubliera pas qu'un polynôme réel est en particulier une fonction de classe C^∞ *à laquelle on peut appliquer tous les résultats classiques de l'analyse réelle.*

5.22. Polynôme positif

Soit $P \in \mathbb{R}[X]$ tel que pour tout $x \in \mathbb{R}$, $P(x) \geqslant 0$. Soit n le degré de P et $Q = P + P' + \cdots + P^{(n)}$. Montrer que pour tout $x \in \mathbb{R}$, on a $Q(x) \geqslant 0$.

(École normale supérieure)

▷ **Solution.**

Le polynôme P étant positif, n est pair et le coefficient dominant de P est positif. Le degré de Q vaut alors n et son coefficient dominant est celui de P. Il en résulte que Q tend vers $+\infty$ en $+\infty$ et en $-\infty$ de sorte que Q est minoré sur $\mathbb{R}$. Si m est sa borne inférieure, il existe $A > 0$ tel que $|Q(x)| \geqslant m + 1$ si $|x| \geqslant A$, ce qui montre que m est aussi la borne inférieure de Q sur le compact $[-A, A]$. La fonction Q étant continue, cette borne inférieure est atteinte en un point x_0. On a alors $Q'(x_0) = 0$. On remarque que $Q - Q' = P$. On a donc $Q(x_0) = P(x_0) \geqslant 0$. D'où le résultat. ◁

L'exercice suivant étudie les racines modulo p premier d'un polynôme à coefficients entiers.

5.23. Diviseurs d'un polynôme de $\mathbb{Z}[X]$

Soit $P \in \mathbb{Z}[X]$ et p premier. On dit que p est un *diviseur* de P s'il existe un entier $n \in \mathbb{N}$ tel que $P(n) \equiv 0 \pmod{p}$ et $P(n) \neq 0$. Montrer que tout polynôme non constant a une infinité de diviseurs.

(École normale supérieure)

▷ **Solution.**

On peut supposer que le coefficient constant a_0 de P n'est pas nul. Sinon, on écrit $P = X^k Q$, où k est la valuation de P et il suffit de démontrer la propriété pour Q.

On note D l'ensemble des diviseurs de P. L'ensemble des entiers n tels que $|P(n)| \leqslant 1$ est fini car P n'est pas constant. Si n est un entier naturel tel que $|P(n)| \geqslant 2$, alors $P(n)$ possède un diviseur premier p qui appartient à D : D n'est pas vide.

Montrons que le cardinal de D n'est pas fini en raisonnant par l'absurde. Si $D = \{p_1, p_2, \ldots, p_\ell\}$ ($\ell \in \mathbb{N}^*$) considérons, pour $m \in \mathbb{N}^*$, le produit $n = m \cdot |a_0| \cdot p_1 \ldots p_\ell$. Il existe $N_m \in \mathbb{Z}$ tel que $P(n) = a_0 N_m$ et $N_m \equiv 1 \pmod{p_1 \ldots p_\ell}$. L'entier $|N_m|$ tend vers $+\infty$ avec m, donc pour m assez grand, on a $|N_m| \geqslant 2$. Alors N_m possède alors un diviseur premier p qui appartient à D. D'où la contradiction cherchée, car on devrait avoir $N_m \equiv 1 \pmod{p}$. ◁

On s'intéresse maintenant aux polynômes à coefficients réels qu laissent $\mathbb{Z}$ stable.

5.24. Polynômes de Hilbert

On pose $H_0 = 1$ et, pour $n \in \mathbb{N}^*$,

$$H_n = \frac{X(X-1)\dots(X-n+1)}{n!}.$$

1. Montrer que, pour tout $n \in \mathbb{N}$, on a $H_n(\mathbb{Z}) \subset \mathbb{Z}$. En déduire que le produit de n entiers consécutifs dans $\mathbb{Z}$ est divisible par $n!$.

2. Soit $P \in \mathbb{R}[X]$, avec $\deg P \leqslant n$. Montrer qu'il y a équivalence entre :

(*i*) $P(\mathbb{Z}) \subset \mathbb{Z}$;

(*ii*) $P(k) \in \mathbb{Z}$, pour $k = 0, 1, \dots, n$;

(*iii*) il existe $(\lambda_0, \dots, \lambda_n) \in \mathbb{Z}^{n+1}$ tel que $P = \sum_{k=0}^{n} \lambda_k H_k$.

(École polytechnique)

▷ **Solution.**

1. Soit $n \in \mathbb{N}$. On a

$$H_n(k) = \begin{cases} 0 & \text{si} \quad 0 \leqslant k \leqslant n-1 \\ C_k^n & \text{si} \quad k \geqslant n \\ (-1)^n C_{n-k-1}^n & \text{si} \quad k < 0. \end{cases}$$

Pour tout k entier, le produit des entiers $k, k+1, \dots, k+n-1$ vaut donc $n!\,H_n(k-n+1)$, qui est un multiple de $n!$.

Il convient de remarquer que $P(\mathbb{Z}) \subset \mathbb{Z}$ *n'implique pas* $P \in \mathbb{Z}[X]$, *comme le prouve l'exemple des polynômes* H_n.

2. Bien entendu (*i*) implique (*ii*). Si P est de la forme $\sum_{k=0}^{n} \lambda_k H_k$, avec $(\lambda_0, \dots, \lambda_n) \in \mathbb{Z}^{n+1}$, alors la question 1 montre que $P(\mathbb{Z}) \subset \mathbb{Z}$. Donc (*iii*) implique (*i*).

Il reste à prouver que (*ii*) implique (*iii*). Chaque polynôme H_k étant de degré k, la famille $(H_0, \dots, H_n)$ est une base de $\mathbb{R}_n[X]$. Il existe donc $(\lambda_0, \dots, \lambda_n) \in \mathbb{R}^{n+1}$ tel que $P = \sum_{k=0}^{n} \lambda_k H_k$. Montrons, par récurrence sur $k \in [\![0, n]\!]$ que $\lambda_k \in \mathbb{Z}$.

- On a $P(0) = \lambda_0 \in \mathbb{Z}$.
- Si, pour $k \in [\![1, n]\!]$, $(\lambda_0, \dots, \lambda_{k-1}) \in \mathbb{Z}^k$, on a alors

$$\mathrm{P}(k) = \sum_{\ell=0}^{k} \lambda_\ell \mathrm{H}_\ell(k) = \sum_{\ell=0}^{k} \lambda_\ell \mathrm{C}_k^\ell \text{ et donc } \lambda_k = \mathrm{P}(k) - \sum_{\ell=0}^{k-1} \lambda_\ell \mathrm{C}_k^\ell \in \mathbb{Z},$$

car $\mathrm{P}(k), \lambda_0, \ldots, \lambda_{k-1}$ sont dans $\mathbb{Z}$, ce qui achève la démonstration. $\lhd$

Si K *est un corps,* $x_1, \ldots, x_n$ *et* $y_1, \ldots, y_n$ *des éléments de* K, *les* x_i *étant deux à deux distincts, il existe un unique polynôme* $\mathrm{P} \in \mathrm{K}_{n-1}[\mathrm{X}]$ *tel que l'on ait, pour* $1 \leqslant i \leqslant n$, $\mathrm{P}(x_i) = y_i$. *C'est le polynôme d'interpolation de Lagrange relatif à* $(x_i, y_i)_{1 \leqslant i \leqslant n}$. *Il s'écrit*

$$\mathrm{P} = \sum_{i=1}^{n} y_i \mathrm{L}_i, \quad \text{où} \quad \mathrm{L}_i = \frac{\prod_{j \neq i} (\mathrm{X} - x_j)}{\prod_{j \neq i} (x_i - x_j)}.$$

On peut remarquer que si $\Phi(\mathrm{X}) = \prod_{i=1}^{n} (\mathrm{X} - x_i)$, *alors* $\mathrm{L}_i(\mathrm{X}) = \dfrac{\Phi(\mathrm{X})}{(\mathrm{X} - x_i)\Phi'(x_i)}$.
Nous appellerons les polynômes L_i *les polynômes interpolateurs de base relatifs au* n*-uplet* $(x_1, \ldots, x_n)$.

Il en résulte en particulier qu'un polynôme $\mathrm{P} \in \mathrm{K}_{n-1}[\mathrm{X}]$ *est uniquement déterminé par ses valeurs en* n *points distincts* $x_1, \ldots, x_n$ *de* K. *Les valeurs* $\mathrm{P}(x_i)$ *sont alors les coordonnées de* P *dans la base de* $\mathrm{K}_{n-1}[\mathrm{X}]$ *formée des polynômes* $\mathrm{L}_1, \ldots, \mathrm{L}_n$. *Cette idée est à la base de l'exercice suivant, qui regroupe en fait trois petits exercices sur le même thème.*

5.25. Interpolation de Lagrange

1. Soit $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$ de degré $n \geqslant 1$. On suppose qu'il existe $k \in \mathbb{Z}$ tel que $\mathrm{P}(k)$, $\mathrm{P}(k+1)$, ... , $\mathrm{P}(k+n)$ soient dans $\mathbb{Z}$. Montrer que pour tout $x \in \mathbb{Z}$, $\mathrm{P}(x) \in \mathbb{Z}$.

2. Soit $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ de degré $n \geqslant 1$. On note N le pgcd de $\mathrm{P}(0)$, $\mathrm{P}(1)$, ..., $\mathrm{P}(n)$. Montrer que N divise $\mathrm{P}(x)$ pour tout $x \in \mathbb{Z}$.

3. Soit $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ de degré n tel que $\mathrm{P}(0)$, $\mathrm{P}(1)$, $\mathrm{P}(4)$, ..., $\mathrm{P}(n^2)$ soient dans $\mathbb{Z}$. Montrer que, pour tout $a \in \mathbb{Z}$, $\mathrm{P}(a^2) \in \mathbb{Z}$.

(École normale supérieure)

$\rhd$ **Solution.**

1. Quitte à considérer le polynôme Q tel que $\mathrm{Q}(\mathrm{X}) = \mathrm{P}(\mathrm{X} + k)$, on peut supposer que $k = 0$. On note $\mathrm{L}_0, \mathrm{L}_1, \ldots, \mathrm{L}_n$ les polynômes interpolateurs de base pour le $(n+1)$-uplet $(0, 1, \ldots, n)$. On a alors, pour tout entier x, $\mathrm{P}(x) = \sum_{i=0}^{n} \mathrm{P}(i)\mathrm{L}_i(x)$. Pour montrer le résultat voulu, il suffit de prouver que $\mathrm{L}_i(x) \in \mathbb{Z}$ pour tout entier x et tout $i \in [\![0, n]\!]$.

On a, pour $i \in [\![0, n]\!]$ et $x \in \mathbb{Z}$,

$$\mathrm{L}_i(x) = \frac{\prod\limits_{j\in[\![0,n]\!]\setminus\{i\}} (x-j)}{\prod\limits_{j\in[\![0,n]\!]\setminus\{i\}} (i-j)} = \frac{(-1)^{n-i}\prod\limits_{j=0}^{i-1}(x-j)}{i!} \times \frac{\prod\limits_{j=i+1}^{n}(x-j)}{(n-i)!}.$$

Le produit de k entiers consécutifs est divisible par $k!$ (c'est ce que montre la première question de l'exercice 5.24) donc $\mathrm{L}_i(x)$ est entier.

2. On a encore $\mathrm{P}(x) = \sum\limits_{i=0}^{n} \mathrm{P}(i)\mathrm{L}_i(x)$ pour tout $x \in \mathbb{Z}$. Comme N divise les $\mathrm{P}(i)$ et que les $\mathrm{L}_i(x)$ sont entiers d'après 1, il est clair que N divise $\mathrm{P}(x)$.

3. Soit $\mathrm{Q}(\mathrm{X}) = \mathrm{P}(\mathrm{X}^2)$. On a $\deg(\mathrm{Q}) = 2n$ et $\mathrm{Q}(-n)$, $\mathrm{Q}(-n+1)$, ..., $\mathrm{Q}(-1)$, $\mathrm{Q}(0)$, $\mathrm{Q}(1)$,...,$\mathrm{Q}(n)$ sont dans $\mathbb{Z}$. D'après la question 1, Q prend des valeurs entières sur $\mathbb{Z}$: c'est le résultat voulu. $\lhd$

Observons que la première question fournit une autre solution de la question 2 de l'exercice 5.24 pour (ii) $\Longrightarrow$ (i). L'exercice qui suit utilise aussi l'interpolation de Lagrange.

5.26. Polynômes complexes envoyant surjectivement $\mathbb{Q}$ sur $\mathbb{Q}$

> Soit $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$. Trouver une condition nécessaire et suffisante pour que P induise une surjection de $\mathbb{Q}$ sur $\mathbb{Q}$.
>
> (**École normale supérieure**)

$\rhd$ **Solution.**

Un polynôme non nul $\mathrm{P} \in \mathbb{C}[\mathrm{X}]$ vérifiant $\mathrm{P}(\mathbb{Q}) \subset \mathbb{Q}$ est à coefficients rationnels. En effet, si n est son degré, on a $\mathrm{P} = \mathrm{P}(0)\mathrm{L}_0 + \cdots + \mathrm{P}(n)\mathrm{L}_n$, où les L_i sont les polynômes interpolateurs de base pour le $(n+1)$-uplet $(0, 1, \ldots, n)$ (et les L_i sont tous dans $\mathbb{Q}[\mathrm{X}]$). On suppose donc $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$. Il est évident que tous les polynômes $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ de degré 1 conviennent. On va en fait montrer que ce sont les seuls. Il est clair que les polynômes constants ne conviennent pas. Montrons qu'il en est de même des polynômes de degré $\geqslant 2$.

Soit $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$ de degré $n \geqslant 2$. Quitte à multiplier P par un entier non nul (ce qui ne modifie pas la surjectivité), on peut supposer que $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$. Écrivons $\mathrm{P} = \sum\limits_{i=0}^{n} a_i\mathrm{X}^i$, avec $(a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}$. Si $\frac{p}{q}$ est un élément non nul de $\mathbb{Q}$, écrit sous forme irréductible, alors $q^n\mathrm{P}\left(\frac{p}{q}\right) = \sum\limits_{i=0}^{n} a_i p^i q^{n-i}$. Considérons un entier premier m. Si $\mathrm{P}\left(\frac{p}{q}\right) = \frac{1}{m}$, alors m divise q^n et donc q, puisque m est premier. Alors m^n divise q^n et en particulier comme $n \geqslant 2$, m divise $\frac{q^n}{m} = \sum\limits_{i=0}^{n} a_i p^i q^{n-i}$. On en déduit que m divise

$a_n p^n$ et donc a_n, car p et q sont premiers entre eux. Un nombre rationnel de la forme $\frac{1}{m}$, où m est un nombre premier ne divisant pas a_n, n'a donc pas d'antécédent par P. Donc $\mathrm{P}(\mathbb{Q})$ n'est pas égal à $\mathbb{Q}$.

Conclusion. Les seuls polynômes complexes qui envoient $\mathbb{Q}$ sur $\mathbb{Q}$ surjectivement sont les polynômes à coefficients rationnels de degré 1. ◁

Soit $n \in \mathbb{N}^*$ et U_n l'ensemble des racines n-ièmes de l'unité. Pour k dans $\mathbb{Z}$, on a $\sum_{w \in \mathrm{U}_n} w^k = 0$ si $k \notin n\mathbb{Z}$ et $\sum_{w \in \mathrm{U}_n} w^k = n$ si $k \in n\mathbb{Z}$. Il en résulte que si $\mathrm{P} \in \mathbb{C}_{n-1}[\mathrm{X}]$, $\frac{1}{n} \sum_{w \in \mathrm{U}_n} \mathrm{P}(w) = \mathrm{P}(0)$. A l'aide d'une similitude, on en déduit facilement que, pour tout polygone régulier de $\mathbb{C}$ et tout $\mathrm{P} \in \mathbb{C}_{n-1}[\mathrm{X}]$, la valeur de P au centre du polygone (qui est l'isobarycentre des sommets) est la moyenne des valeurs de P aux sommets du polygone. L'exercice qui suit montre qu'un polygone $(z_1, \ldots, z_n)$ qui vérifie cette propriété est nécessairement régulier.

5.27. Caractérisation des polygones réguliers

On considère $n+1$ nombres complexes $z_0, z_1, \ldots, z_n$ distincts tels que pour tout polynôme $\mathrm{P} \in \mathbb{C}_{n-1}[\mathrm{X}]$, on ait $\mathrm{P}(z_0) = \frac{1}{n} \sum_{k=1}^{n} \mathrm{P}(z_k)$. Montrer que $z_1, \ldots, z_n$ sont les sommets d'un polygone régulier de centre z_0.

(École normale supérieure)

▷ **Solution.**

On observe que z_0 est l'isobarycentre de $z_1, \ldots, z_n$ (pour le montrer, il suffit de prendre $\mathrm{P} = \mathrm{X}$).

Nous allons exploiter l'hypothèse sur une base de $\mathbb{C}_{n-1}[\mathrm{X}]$. Nous proposons deux solutions de l'exercice.

• Une première méthode consiste à choisir une base de $\mathbb{C}_{n-1}[\mathrm{X}]$ où la somme des $\mathrm{P}(z_k)$ se calcule facilement : la base $(\mathrm{L}_1, \ldots, \mathrm{L}_n)$ des polynômes interpolateurs du n-uplet $(z_1, \ldots, z_n)$ définis, pour $i = 1, \ldots, n$, par

$$\mathrm{L}_i = \frac{\prod_{j \neq i} (\mathrm{X} - z_j)}{\prod_{j \neq i} (z_i - z_j)}.$$

L'hypothèse est que, pour tout $i \in [\![1, n]\!]$, $\mathrm{L}_i(z_0) = \frac{1}{n}$. Si on introduit le polynôme $\mathrm{Q}(\mathrm{X}) = (\mathrm{X} - z_1)(\mathrm{X} - z_2) \ldots (\mathrm{X} - z_n)$, cette égalité s'écrit

$$\frac{\mathrm{Q}(z_0)}{z_0 - z_i} = \frac{1}{n} \mathrm{Q}'(z_i).$$

Cela implique que le polynôme $Q'(X)(X-z_0)-n[Q(X)-Q(z_0)]$ s'annule en chaque z_i, $i=1,\dots,n$. Ce polynôme étant de degré inférieur ou égal à $n-1$, il est nul. On montre alors que $Q(X)-Q(z_0)=(X-z_0)^n$. En effet, on remarque que

$$\left(\frac{Q(X)-Q(z_0)}{(X-z_0)^n}\right)'=\frac{Q'(X)(X-z_0)-n(Q(X)-Q(z_0))}{(X-z_0)^{n+1}}=0.$$

La fraction $\dfrac{Q(z)-Q(z_0)}{(z-z_0)^n}$ est donc constante et, puisque le coefficient dominant de Q est 1, elle vaut 1. On obtient, pour tout $i\in[\![1,n]\!]$,

$$(z_i-z_0)^n=Q(z_i)-Q(z_0)=-Q(z_0).$$

Conclusion. Les complexes $z_1-z_0,\dots,z_n-z_0$ sont les racines n-ièmes de $-Q(z_0)$ et $z_1,\dots,z_n$ forment donc un polygone régulier centré en z_0.

• Une autre idée consiste à exploiter l'hypothèse sur une base de $\mathbb{C}_{n-1}[X]$ où $P(z_0)$ se calcule facilement : la base $((X-z_0)^p)_{0\leqslant p\leqslant n-1}$. On obtient pour $p\in[\![1,n-1]\!]$, $0=\dfrac{1}{n}\sum\limits_{k=1}^{n}(z_k-z_0)^p$. Les sommes de Newton $S_1,S_2,\dots,S_{n-1}$ relatives à $z_1-z_0,z_2-z_0,\dots,z_n-z_0$, définies par $S_p=\sum\limits_{i=1}^{n}(z_k-z_0)^p$ sont donc nulles. D'après les formules de Newton, qui sont démontrées dans l'exercice 5.31, on en déduit que, si $\sigma_1,\dots,\sigma_n$ sont les fonctions symétriques élémentaires de $z_1-z_0,\dots,z_n-z_0$, on a, pour $1\leqslant p\leqslant n-1$,

$$(-1)^{p+1}p\sigma_p=S_{p-1}+\cdots+\sigma_{p-1}S_1=0.$$

On a donc $\sigma_1=\cdots=\sigma_{n-1}=0$ et $z_1-z_0,\dots,z_n-z_0$ sont les racines du polynôme $X^n+(-1)^n\sigma_n$, c'est-à-dire les racines n-ièmes de $(-1)^{n+1}\sigma_n$. On conclut comme dans la solution précédente. ◁

Dans l'exercice suivant, il est encore question de fonctions polynomiales : il s'agit des fonctions induites par un polynôme à coefficients dans $\mathbb{Z}$ ou $\mathbb{Q}$ sur $\mathbb{Z}/p\mathbb{Z}$ ou $\mathbb{Z}/p^i\mathbb{Z}$.

5.28. Polynômes entiers et fonctions polynomiales induites sur $\mathbb{Z}/p^i\mathbb{Z}$

Soit p un nombre premier.

1. On note $\overline{u}$ la classe de l'entier u dans $\mathbb{Z}/p\mathbb{Z}$. Pour $P\in\mathbb{Z}[X]$, on note $\Phi(P)\in\mathcal{F}(\mathbb{Z}/p\mathbb{Z},\mathbb{Z}/p\mathbb{Z})$ l'application qui à toute classe $\overline{u}$ associe la classe $\overline{P(u)}$. Étudier la surjectivité de Φ et son noyau.

2. Pour $n \in \mathbb{N}^*$, on note k_n le produit des entiers non multiples de p qui sont compris entre 1 et n. On pose $H_0 = 1$ et, pour $n \geqslant 1$, $H_n = \dfrac{1}{k_n} X(X-1)\dots(X-n+1)$. Les polynômes H_n engendrent un sous-groupe additif de $\mathbb{Q}[X]$ noté S. Soit $i \in \mathbb{N}^*$. Maintenant on note $\overline{u}$ la classe de l'entier u dans $\mathbb{Z}/p^i\mathbb{Z}$.

a. Soit $Q \in S$. Montrer que $Q(\mathbb{Z}) \subset \mathbb{Z}$ et que $u \equiv u' \ [p^i]$ implique $Q(u) \equiv Q(u') \ [p^i]$.

b. Pour $Q \in S$ on note $\Psi(Q) \in \mathcal{F}(\mathbb{Z}/p^i\mathbb{Z}, \mathbb{Z}/p^i\mathbb{Z})$ l'application qui à toute classe $\overline{u}$ associe la classe $\overline{Q(u)}$. Étudier la surjectivité de Ψ et son noyau.

(École normale supérieure)

▷ **Solution.**

1. L'application qui à $P = \sum_{n\in\mathbb{N}} a_n X^n \in \mathbb{Z}[X]$ associe $\overline{P} = \sum_{n\in\mathbb{N}} \overline{a_n} X^n$ élément de $(\mathbb{Z}/p\mathbb{Z})[X]$ est un morphisme d'anneaux. Comme l'application qui, à un polynôme de $(\mathbb{Z}/p\mathbb{Z})[X]$, associe sa fonction polynomiale est aussi un morphisme d'anneaux, il en va de même de la composée Φ.

• Montrons que Φ est surjective. Si $f \in \mathcal{F}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z})$, nous savons qu'il existe un unique polynôme $A \in (\mathbb{Z}/p\mathbb{Z})[X]$ de degré inférieur ou égal à $p-1$ tel que pour tout $i \in [\![0, p-1]\!]$, $A(\overline{i}) = f(\overline{i})$ (polynôme d'interpolation de Lagrange).

Soit $(b_1, \dots, b_{p-1}) \in \mathbb{Z}^p$ tel que $A = \sum_{j=0}^{p-1} \overline{b_j} X^j$,. On pose $P = \sum_{j=1}^{p-1} b_j X^j$. Par construction, on a, pour tout $i \in [\![0, p-1]\!]$, $\overline{P(i)} = A(\overline{i}) = f(\overline{i})$. Ceci montre que $\Phi(P) = f$. L'application Φ est surjective.

Ce qui précède montre que toute application de $\mathbb{Z}/p\mathbb{Z}$ dans lui-même est polynomiale.

• D'après le petit théorème de Fermat, on a $x^p - x = 0$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, autrement dit $\Phi(X^p - X) = 0$. Le polynôme $X^p - X$ appartient à $\operatorname{Ker}\Phi$. Si $P \in \mathbb{Z}[X]$, on effectue la division euclidienne de P par $X^p - X$. On obtient $P = (X^p - X)Q + R$, avec $Q \in \mathbb{Z}[X]$ et $R \in \mathbb{Z}_{p-1}[X]$. On a alors $\Phi(P) = \Phi(Q)\Phi(X^p - X) + \Phi(R) = \Phi(R)$. Ceci montre que P appartient à $\operatorname{Ker}\Phi$ si et seulement si R est dans $\operatorname{Ker}\Phi$.

On écrit $R = \sum_{j=0}^{p-1} b_j X^j$, avec $(b_0, \dots, b_{p-1}) \in \mathbb{Z}^p$ et on considère son projeté $\overline{R} = \sum_{j=0}^{p-1} \overline{b_j} X^j$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Si R est dans $\operatorname{Ker}\Phi$, tout élément de $\mathbb{Z}/p\mathbb{Z}$ est racine du polynôme $\overline{R}$. Celui-ci étant de degré inférieur ou égal à $p-1$, c'est le polynôme nul. Ainsi, pour tout $j \in [\![0, p-1]\!]$, $\overline{b_j} = \overline{0}$, c'est-à-dire que p divise b_j. On en déduit qu'il existe $T \in \mathbb{Z}_{p-1}[X]$ tel que

$R = pT$ et $P = (X^p - X)Q + pT$. Il est clair, réciproquement, que tout polynôme ayant cette forme appartient à $\operatorname{Ker}\Phi$, et plus généralement tous les polynômes de la forme $(X^p - X)Q + pT$ avec $(Q, T) \in \mathbb{Z}[X]^2$ (qui se ramènent à la forme précédente en divisant T par $X^p - X$).

Conclusion. Le noyau de Φ est l'idéal de $\mathbb{Z}[X]$ engendré par les polynômes $X^p - X$ et p.

2. a. Les éléments de S sont les combinaisons linéaires à coefficients entiers des polynômes H_n. Il suffit donc de démontrer la propriété pour les polynômes H_n ($n \geqslant 1$).

Montrons que $H_n(\mathbb{Z}) \subset \mathbb{Z}$ pour commencer[4]. Soit $x \in \mathbb{Z}$.

• Si $0 \leqslant x \leqslant n-1$, alors $H_n(x) = 0$.

• Si $x \geqslant n$, alors $H_n(x) = \dfrac{x!}{k_n(x-n)!} = \dfrac{n!}{k_n} C_x^n \in \mathbb{Z}$ car, par construction, k_n divise $n!$.

• Enfin, si $x < 0$, alors $H_n(x) = \dfrac{(-1)^n(n-x+1)!}{k_n(-x)!} = \dfrac{(-1)^n n!}{k_n} C_{n-x+1}^n$ et de nouveau $H_n(x) \in \mathbb{Z}$.

Le polynôme $k_n H_n$ est à coefficients entiers. Si $u \equiv u' \,[p^i]$, alors d'après les propriétés des congruences, on a $k_n H_n(u) \equiv k_n H_n(u') \,[p^i]$. Autrement dit, p^i divise $k_n H_n(u) - k_n H_n(u')$. Or, par hypothèse, k_n est premier avec p, donc avec p^i. On en déduit, d'après le théorème de Gauss, que p^i divise $H_n(u) - H_n(u')$, c'est-à-dire que $H_n(u) \equiv H_n(u') \,[p^i]$.

b. On peut remarquer que Ψ est un morphisme de groupes additifs (on ne dispose pas d'une structure d'anneau sur S).

• Soit $d \in \mathbb{N}$ et $Q = \sum_{n=0}^{d} a_n H_n$, avec $(a_0, \ldots, a_d) \in \mathbb{Z}^{d+1}$, un élément de S. D'après ce qui précède, on a, pour $0 \leqslant j \leqslant d$,

$$Q(j) = \sum_{n=0}^{j} a_n \frac{n!}{k_n} C_j^n.$$

Supposons que $Q \in \operatorname{Ker}\Psi$. On a alors $Q(j) \equiv 0 \,[p^i]$, pour tout j de $[\![0, d]\!]$. On obtient, en particulier, pour $j = 0$ et $j = 1$, $a_0 \equiv 0 \,[p^i]$ et $a_0 + \dfrac{a_1}{k_1} \equiv 0 \,[p^i]$ et donc $a_0 \equiv \dfrac{a_1}{k_1} \equiv 0 \,[p^i]$. Supposons démontré que pour tout $n \in [\![1, j-1]\!]$, on a $\dfrac{a_n n!}{k_n} \equiv 0 \,[p^i]$. On obtient alors

$$\frac{a_j j!}{k_j} = Q(j) - \sum_{n=0}^{j-1} a_n \frac{n!}{k_n} C_j^n \equiv 0 \left[p^i\right],$$

ce qui démontre, par récurrence, que pour tout $j \in [\![0, d]\!]$, $\dfrac{a_j j!}{k_j} \equiv 0 \,[p^i]$.

4. En fait, le résultat découle directement de l'exercice 5.24 puisque H_n est un multiple entier d'un polynôme de Hilbert.

Montrons réciproquement, que si cette condition est réalisée, alors $Q \in \operatorname{Ker}\Psi$. En effet, si $0 \leqslant j \leqslant d$, on a $a_j H_j(x) = 0$ pour $0 \leqslant x \leqslant j-1$ et $a_j H_j(x) = \dfrac{a_j j!}{k_j} C_x^j \equiv 0\ [p^i]$, pour $x \geqslant j$. On a donc, pour tout $x \in \mathbb{N}$, $Q(x) \equiv 0\ [p^i]$ et $\Psi(Q) = 0$. Le polynôme Q est dans $\operatorname{Ker}\Psi$.

Notons enfin que la condition trouvée équivaut à $a_j j! \equiv 0[p^i]$, pour tout j de $[\![0, d]\!]$, puisque k_j est premier avec p. On conclut :

$$\boxed{\operatorname{Ker}\Psi = \left\{\sum_{j=0}^{d} a_j H_j, d \in \mathbb{N}, (a_0, \ldots, a_d) \in \mathbb{Z}^{d+1}, \forall j \in [\![0, d]\!]\ a_j j! \equiv 0[p^i]\right\}}.$$

Remarquons que pour tout $j \in \mathbb{N}$, $\nu_p(a_j j!) = \nu_p(a_j) + \nu_p(j!) \geqslant \nu_p(j!)$. Si $\nu_p(j!) \geqslant i$, alors la condition sur a_j est automatiquement réalisée. Soit j_0 le plus petit des entiers j tels que $\nu_p(j!) \geqslant i$. Il résulte de ce qui précède que le sous-groupe de S engendré par les polynômes H_j, $j \geqslant j_0$ est inclus dans le noyau.

• On peut décrire autrement les éléments du noyau. Soit $Q \in \operatorname{Ker}\Psi$. La condition $\dfrac{a_j j!}{k_j} \equiv 0\ [p^i]$ signifie qu'il existe $b_j \in \mathbb{Z}$ tel que $a_j = \dfrac{b_j k_j}{j!} p^i$. Le polynôme Q s'écrit donc $p^i \sum\limits_{j=0}^{d} b_j H'_j$, où les polynômes H'_j sont les polynômes de Hilbert définies par $H'_0 = 1$ et pour tout $n \in \mathbb{N}^*$,

$$H'_n = \frac{1}{n!} X(X-1)\ldots(X-n+1).$$

Il est classique de montrer que les polynômes qui s'écrivent comme combinaisons linéaires à coefficients entiers des polynômes de Hilbert sont les polynômes de $\mathbb{Q}[X]$ qui envoient $\mathbb{Z}$ dans $\mathbb{Z}$ (voir exercice 5.24). On obtient finalement

$$\boxed{\operatorname{Ker}\Psi = \{p^i Q, Q \in \mathbb{Q}[X], Q(\mathbb{Z}) \subset \mathbb{Z}\}}.$$

• Soit $f \in \Psi(S)$ et $Q \in S$ tel que $\Psi(Q) = f$. Notons comme précédemment $Q = \sum\limits_{n=0}^{d} a_n H_n$. La fonction $\Psi(Q)$ ne dépend que des restes des a_j modulo p^i. On peut donc supposer que les coefficients a_j sont dans $[\![0, p^i - 1]\!]$. D'autre part, l'étude du noyau montre qu'on peut prendre $d < j_0$. En notant

$$S' = \left\{Q \in S, Q = \sum_{j=0}^{j_0-1} a_j H_j, (a_0, \ldots, a_{j_0-1}) \in [\![0, p^i - 1]\!]^{j_0}\right\},$$

on a donc $\operatorname{Im}\Psi = \Psi(S')$ et $\operatorname{Card}(\operatorname{Im}\Psi) \leqslant \operatorname{Card}(S') = (p^i)^{j_0}$.

Pour préciser $\operatorname{Card}(S')$, il faut évaluer j_0 (défini ci-dessus). Il résulte de l'exercice 4.21 que

$$\nu_p((p^i - 1)!) = \sum_{k=1}^{i-1} E\left(\frac{p^i - 1}{p^k}\right) = \sum_{k=1}^{i-1} (p^{i-k} - 1) = \frac{p^i - p}{p - 1} - i + 1.$$

⋆ De la formule du binôme on déduit que, si $i \geqslant 2$, on a

$$\nu_p((p^i-1)!) \geqslant \frac{1+(p-1)i+\dfrac{i(i-1)}{2}(p-1)^2-p}{p-1} - i + 1 \geqslant \frac{i(i-1)(p-1)}{2}$$

et $\nu_p((p^i-1)!) \geqslant i$ si $i \geqslant 3$ ou $p \geqslant 3$. On a alors $j_0 \leqslant p^i - 1$ et $\mathrm{Card}(\mathrm{Im}\,\Psi) \leqslant (p^i)^{p^i-1}$. Comme $\mathrm{Card}(\mathcal{F}(\mathbb{Z}/p^i\mathbb{Z}, \mathbb{Z}/p^i\mathbb{Z})) = (p^i)^{p^i}$, l'application Ψ n'est pas surjective si $i \geqslant 3$ ou $i = 2$ et $p \geqslant 3$.

⋆ Dans le cas où $i = 1$, on a $j_0 = p$. Montrons qu'alors la restriction de Ψ à S' est injective. Si $\mathrm{Q} = \sum_{j=0}^{p-1} a_j \mathrm{H}_j$ et $\mathrm{Q}' = \sum_{j=0}^{p-1} b_j \mathrm{H}_j$ sont deux éléments de S' ayant même image par Ψ, on obtient, d'après l'étude du noyau qui précède, pour tout $j \in [\![0, p-1]\!]$, $(a_j - b_j)\dfrac{j!}{k_j} \equiv 0 \ [p]$. Mais ici $k_j = j!$, car $j < p$. On a donc $a_j \equiv b_j[p]$, *i.e.* $a_j = b_j$, car a_j et b_j sont dans $[\![0, p-1]\!]$. La restriction de Ψ à S' est donc une bijection de S' sur $\mathrm{Im}\,\Psi$. On en déduit que $\mathrm{Card}(\mathrm{Im}\,\Psi) = p^p = \mathrm{Card}(\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p))$: l'application Ψ est surjective.

⋆ Enfin, dans le cas où $i = p = 2$, on a $j_0 = 4$. On vérifie que les éléments de $\mathrm{Q} = \sum_{j=0}^{3} a_j \mathrm{H}_j$ et $\mathrm{Q}' = \sum_{j=0}^{3} b_j \mathrm{H}_j$ de S' ont même image par Ψ si et seulement si $a_0 = b_0$, $a_1 = b_1$, $a_2 \equiv b_2[2]$ et $a_3 \equiv b_3[2]$. En notant

$$\mathrm{S}'' = \left\{ \mathrm{Q} \in \mathrm{S}, \mathrm{Q} = \sum_{j=0}^{3} a_j \mathrm{H}_j,\ (a_0, a_1) \in [\![0,3]\!]^2,\ (a_2, a_3) \in [\![0,1]\!]^2 \right\},$$

on a donc $\mathrm{Im}\,\Psi = \Psi(\mathrm{S}'')$ et $\mathrm{Card}(\mathrm{Im}\,\Psi) = \mathrm{Card}(\mathrm{S}'') = 4 \cdot 4 \cdot 2 \cdot 2 = 64$ et $\mathrm{Card}(\mathcal{F}(\mathbb{Z}/p^i\mathbb{Z}, \mathbb{Z}/p^i\mathbb{Z})) = 4^4 = 256$: Ψ n'est pas surjective. ◁

Les exercices suivants ont pour thème les relations entre les coefficients et les fonctions symétriques des racines d'un polynôme.

5.29. Images des racines d'un polynôme

Soit $\mathrm{P} = \mathrm{X}^4 + a\mathrm{X}^2 + b\mathrm{X} + c \in \mathbb{C}[\mathrm{X}]$.

1. Donner une condition nécessaire et suffisante sur a, b, c pour que les racines de P forment un parallélogramme.

2. Même question avec un rectangle.

(École polytechnique)

▷ **Solution.**

1. Notons x_1, x_2, x_3 et x_4 les racines du polynôme P. Leurs images dans le plan complexe forment un parallélogramme si on peut les or-

donner de telle manière que $x_1 + x_2 = x_3 + x_4$ (relation équivalente à $x_1 - x_3 = x_4 - x_2$). Le coefficient de X^3 est nul donc la somme σ_1 des racines de P est nulle et la condition équivaut à $x_1 + x_2 = x_3 + x_4 = 0$. En considérant σ_3 on obtient

$$b = -\sigma_3 = -x_1x_2(x_3 + x_4) - x_3z_4(x_1 + x_2) = 0.$$

Réciproquement, si $b = 0$ on obtient $P = X^4 + aX^2 + c = Q(X^2)$, où $Q = X^2 + aX + c$. En notant z_1 et z_2 les racines de Q, les racines de P sont les racines carrées de z_1 et z_2 ; elles sont deux à deux opposées et leurs images forment un parallélogramme de centre 0.

2. Un rectangle est un parallélogramme dont les diagonales ont la même longueur. D'après la question précédente, dont on reprend les notations, les racines de P forment un rectangle si et seulement si $b = 0$ et $|z_1| = |z_2|$. On cherche donc à quelle condition les racines de Q ont même module. En notant ω une racine carrée de $\Delta = a^2 - 4c$, on souhaite avoir $|-a-\omega| = |-a+\omega|$, ce qui équivaut à $a\overline{\omega} + \overline{a}\omega = 0$, à $\overline{a}\omega$ imaginaire pur et donc à $\overline{a}^2\omega^2 = \overline{a^2}\Delta$ réel négatif. Ceci est réalisé si $a = 0$. Sinon, on écrit

$$\overline{a^2}\Delta = |a|^2\frac{\Delta}{a^2} = |a|^2\left(1 - \frac{4c}{a^2}\right).$$

Cette expression est un réel négatif si et seulement si $\dfrac{c}{a^2}$ est un réel supérieur ou égal à $\dfrac{1}{4}$.

Conclusion. Les racines de P forment un rectangle si et seulement si $b = 0$ et soit $a = 0$, soit $\dfrac{c}{a^2}$ est un réel supérieur ou égal à $\dfrac{1}{4}$. ◁

5.30. Un calcul de $\zeta(2)$

1. Soit $n \in \mathbb{N}$. Montrer qu'il existe un polynôme P_n tel que, pour tout $t \in \left]0, \dfrac{\pi}{2}\right[$,

$$P_n(\operatorname{cotan}^2 t) = \frac{\sin(2n+1)t}{\sin^{2n+1} t}.$$

2. Expliciter les racines de P_n et calculer leur somme.

3. En observant que l'on a $\operatorname{cotan}^2 t \leqslant \dfrac{1}{t^2} \leqslant 1 + \operatorname{cotan}^2 t$ pour tout $t \in \left]0, \dfrac{\pi}{2}\right[$, déterminer la valeur de $\zeta(2) = \displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^2}$.

(École polytechnique)

▷ **Solution.**

1. On applique la formule de Moivre pour calculer $\sin(2n+1)t$ pour tout $t \in \left]0, \frac{\pi}{2}\right[$. On a

$$\sin(2n+1)t = \operatorname{Im}(\cos t + i \sin t)^{2n+1} = \sum_{k=0}^{n} \mathrm{C}_{2n+1}^{2k+1} (-1)^k \sin^{2k+1} t \cos^{2(n-k)} t.$$

En divisant par $\sin^{2n+1} t \neq 0$, on obtient bien $\dfrac{\sin(2n+1)t}{\sin^{2n+1} t} = \mathrm{P}_n(\operatorname{cotan}^2 t)$, où P_n est le polynôme $\mathrm{P}_n(\mathrm{X}) = \sum\limits_{k=0}^{n} \mathrm{C}_{2n+1}^{2k+1} (-1)^k \mathrm{X}^{n-k}$.

Le polynôme P_n est unique car si Q répond également au problème, on a $\mathrm{P}_n(x) = \mathrm{Q}(x)$ pour tout $x > 0$, puisque x peut s'écrire $x = \operatorname{cotan}^2 t$ avec $t = \operatorname{arccotan}(\sqrt{x}) \in \left]0, \frac{\pi}{2}\right[$.

2. Le polynôme P_n est de degré n et il résulte de la première question que pour tout $k \in [\![1, n]\!]$, $x_k = \operatorname{cotan}^2\left(\dfrac{k\pi}{2n+1}\right)$ est racine de P_n. Ces n racines étant deux à deux distinctes, il s'agit des n racines de P_n. La somme des racines de P_n est l'opposé du coefficient de X^{n-1} divisé par le coefficient dominant. Ainsi,

$$x_1 + \cdots + x_n = \frac{\mathrm{C}_{2n+1}^{3}}{\mathrm{C}_{2n+1}^{1}} = \frac{n(2n-1)}{3}.$$

3. La double inégalité proposée découle de l'encadrement bien connu $\sin t \leqslant t \leqslant \tan t$ valable pour tout $t \in \left[0, \frac{\pi}{2}\right[$. Si on doit le prouver on peut soit faire une étude de fonction, soit invoquer un argument de convexité. On écrit alors l'inégalité pour $t = \dfrac{k\pi}{2n+1}$ et on somme pour k variant de 1 à n. Il vient à l'aide de la question précédente

$$\frac{n(2n-1)}{3} \leqslant \sum_{k=1}^{n} \frac{(2n+1)^2}{\pi^2 k^2} \leqslant n + \frac{n(2n-1)}{3}.$$

On divise alors par $\dfrac{(2n+1)^2}{\pi^2}$ et on fait tendre n vers l'infini. On trouve un résultat sans doute bien connu du lecteur : $\boxed{\zeta(2) = \sum\limits_{n=1}^{+\infty} \dfrac{1}{n^2} = \dfrac{\pi^2}{6}}$. ◁

Parmi les fonctions polynomiales symétriques en n variables les plus utilisées, figurent les sommes de Newton $\mathrm{S}_p = \sum\limits_{i=1}^{n} x_i^p$. Les formules de Newton sont des relations entre les sommes de Newton et les fonctions symétriques élémentaires.

5.31. Formules de Newton (1707)

Soit n un entier $\geqslant 2$, K un corps commutatif, $x_1, \ldots, x_n$ des éléments de K. On considère, pour $p \in \mathbb{N}$, la somme $S_p = \sum_{i=1}^{n} x_i^p$. On note $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires de $x_1, \ldots, x_n$, définies par

$$\sigma_k = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n} x_{i_1} x_{i_2} \ldots x_{i_n}.$$

Démontrer qu'on a les relations suivantes :

1. $S_p - \sigma_1 S_{p-1} + \cdots + (-1)^{n-1}\sigma_{n-1} S_{p-n} + (-1)^n \sigma_n S_{p-n} = 0$ pour $p \geqslant n$.

2. $S_p - \sigma_1 S_{p-1} + \cdots + (-1)^{p-1}\sigma_{p-1} S_1 + (-1)^p p\sigma_p = 0$ pour $1 \leqslant p \leqslant n-1$.

(École polytechnique)

▷ **Solution.**

1. Considérons le polynôme $P = \prod_{i=1}^{n} (X - x_i) \in K[X]$. Il a pour expression

$$P = X^n + \sum_{i=1}^{n} (-1)^i \sigma_i X^{n-i}.$$

Pour $1 \leqslant i \leqslant n$ et $p \geqslant n$, on a $P(x_i) = x_i^n - \sigma_1 x_i^{n-1} + \cdots + (-1)^p \sigma_p = 0$ et donc en multipliant par x_i^{p-n},

$$x_i^p - \sigma_1 x_i^{p-1} + \cdots + (-1)^n \sigma_n x_i^{p-n} = 0.$$

En additionnant, pour $1 \leqslant i \leqslant n$, on obtient

$$\boxed{S_p - \sigma_1 S_{p-1} + \cdots + (-1)^n \sigma_n S_{p-n} = 0}.$$

2. Soit p entier tel que $1 \leqslant p \leqslant n-1$. Ce second cas est nettement plus difficile. Pour commencer, on compare S_p et $\sigma_1 S_{p-1}$. On obtient

$$S_p = \sigma_1 S_{p-1} - \sum_{\substack{1 \leqslant i_1, i_2 \leqslant n \\ i_1 \neq i_2}} x_{i_1} x_{i_2}^{p-1}.$$

On compare ensuite cette dernière somme et $\sigma_2 S_{p-2}$. On a, cette fois,

$$\sigma_2 S_{p-2} = \sum_{\substack{1 \leqslant i_1, i_2 \leqslant n \\ i_1 \neq i_2}} x_{i_1} x_{i_2}^{p-1} + \sum_{\substack{1 \leqslant i_1 < i_2 \leqslant n \\ i_3 \neq i_1, i_2}} x_{i_1} x_{i_2} x_{i_3}^{p-2}.$$

Plus généralement, on pose, pour $0 \leqslant k \leqslant p-1$,

$$A_k = \sum_{\substack{1 \leqslant i_1 < \cdots < i_k \leqslant n \\ i_{k+1} \neq i_1, i_2, \ldots, i_k}} x_{i_1} \ldots x_{i_k} x_{i_{k+1}}^{p-k}.$$

On remarque qu'en particulier $A_0 = S_p$ et $A_{p-1} = p\sigma_p$. On obtient alors, pour $1 \leqslant k \leqslant p-1$,

$$\sigma_k S_{p-k} = A_{k-1} + A_k.$$

En multipliant la première relation par -1, la seconde par $(-1)^2$, ... et la $(p-1)$-ième par $(-1)^{p-1}$, on trouve

$$\sum_{k=1}^{p-1} (-1)^k \sigma_k S_{p-k} = -A_0 + (-1)^{p-1} A_{p-1} = -S_p + (-1)^{p-1} p\sigma_p,$$

ce qui, si on fait tout passer dans le membre de gauche de l'égalité, nous donne le résultat voulu.

De ce résultat, nous proposons une preuve alternative fondée sur les séries génératrices.

Soit $\alpha \in \mathbb{C}$. On peut écrire le développement en série entière

$$\frac{1}{1-\alpha x} = \sum_{p=0}^{+\infty} \alpha^p x^p,$$

valable pour $|\alpha x| < 1$. Si on écrit ce développement pour $\alpha = x_i$, pour $1 \leqslant i \leqslant n$ et si on somme les relations obtenues, on obtient

$$\sum_{i=1}^{n} \frac{1}{1-x_i x} = \sum_{p=0}^{+\infty} S_p x^p,$$

développement valable dans un voisinage de 0. La somme $\sum_{i=1}^{n} \frac{1}{1-X_i x}$ est le développement en éléments simples d'une fraction rationnelle, que nous allons déterminer. On sait que si on pose $P = (X-x_1)\ldots(X-x_n)$, on obtient

$$\frac{P'}{P} = \sum_{i=1}^{n} \frac{1}{X-x_i} \quad \text{et donc} \quad \frac{XP'}{P} = \sum_{i=1}^{n} \frac{1}{1-x_i/X},$$

puis en substituant $1/X$ à X,

$$\sum_{i=1}^{n} \frac{1}{1-x_i X} = \frac{P'(1/X)}{XP(1/X)} = \frac{X^{n-1}P'(1/X)}{X^n P(1/X)}.$$

Puisque $P = \sum_{k=0}^{n} (-1)^k \sigma_k X^{n-k}$ et $P' = \sum_{k=0}^{n-1} (-1)^k (n-k)\sigma_k X^{n-k-1}$ (en posant $\sigma_0 = 1$), on obtient

$$\sum_{i=1}^{n} \frac{1}{1 - x_i \mathrm{X}} = \frac{\sum\limits_{k=0}^{n-1} (-1)^k (n-k) \sigma_k \mathrm{X}^k}{\sum\limits_{k=0}^{n} (-1)^k \sigma_k \mathrm{X}^k}.$$

Par conséquent, pour x voisin de 0, on peut écrire

$$\left(\sum_{k=0}^{n-1} (-1)^k (n-k) \sigma_k x^k \right) = \left(\sum_{p=0}^{+\infty} \mathrm{S}_p x^p \right) \left(\sum_{k=0}^{n} (-1)^k \sigma_k x^k \right).$$

D'après l'unicité des coefficients d'une série entière et la règle du produit de Cauchy, le coefficient de x^p (pour $1 \leqslant p \leqslant n-1$) vaut

$$\begin{aligned} (-1)^p \sigma_p (n-p) &= \sum_{k=0}^{p} \mathrm{S}_k (-1)^{p-k} \sigma_{p-k} \\ &= \mathrm{S}_p - \sigma_1 \mathrm{S}_{p-1} + \sigma_2 \mathrm{S}_{p-2} - \cdots + (-1)^p \sigma_p \underbrace{\mathrm{S}_0}_{=n} \end{aligned}$$

et finalement

$$\boxed{\mathrm{S}_p - \sigma_1 \mathrm{S}_{p-1} + \cdots + (-1)^{p-1} \sigma_{p-1} \mathrm{S}_1 + (-1)^p p \sigma_p = 0}. \lhd$$

Ces formules permettent de déterminer les sommes de Newton de proche en proche. Inversement, si le corps est de caractéristique nulle (il faut pouvoir diviser par les entiers), la connaissance des sommes de Newton permet de déterminer les fonctions symétriques élémentaires. Une utilisation de cela est faite dans l'exercice 5.27.

L'exercice suivant est l'occasion de rappeler que toute expression rationnelle et symétrique de $x_1, x_2, \ldots, x_n$ peut s'exprimer rationnellement[5] *en fonction de $\sigma_1, \ldots, \sigma_n$, fonctions symétriques élémentaires de $x_1, \ldots, x_n$. Ici, on se contente de le constater sur un exemple particulier.*

5.32. Polynômes réels scindés

On considère E l'ensemble des polynômes réels scindés sur $\mathbb{R}$ et à coefficients dans $\{0, -1, 1\}$. On souhaite décrire E.

1. Montrer qu'il suffit de connaître les éléments de E unitaires et qui ne s'annulent pas en 0.

5. Le lecteur pourra trouver une preuve de ce théorème dans ARNAUDIÈS (J.-M.) & BRAYSSE (H.), *Cours de Mathématiques, Algèbre 1*, Dunod, 1987, Chapitre X.

2. Pour n réels strictement positifs $a_1, \ldots, a_n$, démontrer l'inégalité $\sum_{1 \leqslant i,j \leqslant n} \frac{a_i}{a_j} \geqslant n^2$.

3. Soit P un polynôme unitaire non constant dans E tel que $P(0) \neq 0$. Démontrer que $\deg P \leqslant 3$. En déduire P.

(**École normale supérieure**)

▷ **Solution.**

1. Il est évident que P est dans E si et seulement si $-P$ est dans E. Il nous suffit donc de connaître les éléments unitaires de E. Si 0 est racine de $P \in E$ avec une multiplicité k, on peut écrire $P = X^k Q$ avec $Q \in \mathbb{R}[X]$. Or, Q est scindé et ses coefficients sont aussi dans $\{0, -1, 1\}$. Réciproquement, si Q est dans E, alors $X^k Q \in E$ pour tout entier k.

En résumé, les éléments non nuls de E s'écrivent $\pm X^k Q$, où $k \in \mathbb{N}$ et où Q est un élément unitaire de E n'ayant pas 0 comme racine.

2. Cette inégalité résulte du fait que, si x, y sont des réels strictement positifs, on a $\frac{x}{y} + \frac{y}{x} \geqslant 2$. Dans la somme $\sum_{1 \leqslant i,j \leqslant n} \frac{a_i}{a_j}$, on regroupe alors le terme (i, j) avec le terme (j, i) pour $i \neq j$. Comme le quotient vaut 1 lorsque $i = j$, il vient

$$\sum_{1 \leqslant i,j \leqslant n} \frac{a_i}{a_j} \geqslant n + 2C_n^2 = n^2.$$

3. Notons n le degré de P. Écrivons $P = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n$ où les σ_k sont les fonctions symétriques élémentaires des racines de P. Notons $x_1, \ldots, x_n$ ces racines distinctes ou confondues. Par hypothèse, elles sont toutes réelles et non nulles.

L'inégalité de la question précédente appliquée aux x_i^2 donne

$$S = \sum_{1 \leqslant i,j \leqslant n} \frac{x_i^2}{x_j^2} \geqslant n^2.$$

Or S est une expression rationnelle des x_i et elle va s'exprimer à l'aide des σ_k. Comme ces derniers sont majorés par 1, on pourra en déduire une majoration de n. Plus précisément, on a

$$\begin{aligned} S &= \sum_{1 \leqslant i,j \leqslant n} \frac{x_i^2}{x_j^2} = \left(\sum_{i=1}^n x_i^2\right)\left(\sum_{i=1}^n \frac{1}{x_i^2}\right) \\ &= (\sigma_1^2 - 2\sigma_2)\left(\left(\frac{\sigma_{n-1}}{\sigma_n}\right)^2 - 2\frac{\sigma_{n-2}}{\sigma_n}\right). \end{aligned}$$

On a alors clairement $S \leqslant 3 \times 3 = 9$ et donc $n \leqslant 3$. On peut alors mener une recherche exhaustive.

⋆ Pour $n = 1$, $X - 1$ et $X + 1$ conviennent pour P.

⋆ Pour $n = 2$ on obtient $X^2 - 1$, $X^2 + X - 1$, $X^2 - X - 1$.

⋆ Pour $n = 3$, l'étude du cas d'égalité dans la majoration obtenue plus haut donne $\sigma_1 = \pm 1$, $\sigma_2 = -1$, $\sigma_3 = \pm 1$ et $\sigma_1 = -\sigma_3$. On obtient alors les polynômes $X^3 + X^2 - X - 1$ et $X^3 - X^2 - X + 1$, qui conviennent tous les deux. ◁

Le théorème rappelé avant l'exercice précédent se généralise aux polynômes à coefficients dans un anneau. Ainsi, si P *est un polynôme symétrique en* $x_1, \ldots, x_n$ *à coefficients dans* $\mathbb{Z}$, *il existe* Q *à coefficients dans* $\mathbb{Z}$ *tel que* $P(x_1, \ldots, x_n) = Q(\sigma_1, \ldots, \sigma_n)$. *On pourra exploiter cela dans l'exercice qui suit.*

5.33. Un théorème de Kronecker

Soit P un polynôme unitaire de $\mathbb{Z}[X]$ dont les racines complexes sont toutes de module inférieur ou égal à 1. On suppose $P(0) \neq 0$. Montrer que toutes les racines de P sont des racines de l'unité.

(**École normale supérieure**)

▷ **Solution.**

• Notons $z_1, z_2, \ldots, z_n$ les racines de P comptées avec leur multiplicité, $n \geqslant 1$ désignant le degré de P, et $\sigma_1, \ldots, \sigma_n$ les fonctions symétriques élémentaires des z_i. On a donc

$$P(X) = X^n - \sigma_1 X^{n-1} + \cdots + (-1)^n \sigma_n$$

et les σ_i sont dans $\mathbb{Z}$. Comme $|z_i| \leqslant 1$ pour tout $i \in [\![1, n]\!]$, on obtient, pour $1 \leqslant p \leqslant n$, la majoration

$$|\sigma_p| = \left| \sum_{I \in \mathcal{P}_p([\![1,n]\!])} \prod_{i \in I} z_i \right| \leqslant \sum_{I \in \mathcal{P}_p([\![1,n]\!])} 1 = \operatorname{Card} \mathcal{P}_p([\![1, n]\!]) = C_n^p.$$

Ceci montre que l'ensemble Ω_n des polynômes unitaires de $\mathbb{Z}[X]$, de degré n, dont les racines complexes sont de module inférieur ou égal à 1 est fini.

• L'idée est alors de considérer pour tout $k \in \mathbb{N}^*$ les polynômes $P_k(X) = (X - z_1^k)(X - z_2^k) \ldots (X - z_n^k)$. Ce sont des polynômes unitaires de degré n dont les racines z_i^k sont de module inférieur ou égal à 1. Pour tout $r \in [\![1, n]\!]$, le coefficient de X^{n-r} dans P_k est $(-1)^r \sigma_r(z_1^k, \ldots, z_n^k)$. Il s'agit d'un polynôme symétrique en $z_1, z_2, \ldots, z_n$ à coefficients dans $\mathbb{Z}$. Il est donc égal à un polynôme à coefficients entiers en les fonctions symétriques élémentaires des z_i. Il en résulte que, pour tout entier k, on a $P_k \in \mathbb{Z}[X]$ et donc que $P_k \in \Omega_n$.

Comme Ω_n est fini, et que chaque élément de Ω_n admet au plus n racines complexes distinctes, l'ensemble des racines des éléments de Ω_n est aussi fini. En particulier, pour tout $i \in [\![1, n]\!]$, l'application $k \longmapsto z_i^k$ ne peut pas être injective. Il existe donc deux entiers $k \neq \ell$ tels que $z_i^k = z_i^\ell$. Comme z_i est supposé non nul, il s'agit d'une racine de l'unité. ◁

Si $P \in \mathbb{C}[X]$ *est unitaire on appelle mesure de Mahler*[6] *de* P *et on note* M(P), *le produit* $\prod_{P(z)=0} \max(1, |z|)$. *Le théorème de Kronecker montre donc que si* $P \in \mathbb{Z}[X]$ *est un polynôme unitaire de mesure égale à* 1, *ses racines sont des racines de l'unité (ou* 0*). Un célèbre problème de Mahler consiste à chercher s'il existe* $\varepsilon > 0$ *tel que le résultat reste vrai pour les polynômes de mesure inférieure à* $1 + \varepsilon$.

Dans $\mathbb{C}[X]$ *tout polynôme est scindé. Il n'en est rien dans* $\mathbb{R}[X]$ *et c'est l'objet de nombreux exercices, des plus simples aux plus sophistiqués, de chercher combien de racines réelles possède un polynôme réel et s'il est scindé. Il apparaît, dans les exercices suivants, que la recherche des racines réelles d'un polynôme de* $\mathbb{R}[X]$ *fait essentiellement appel à des techniques d'analyse.*

5.34. Racines réelles de $nX^n - X^{n-1} - \cdots - X - 1$

Combien $P_n = nX^n - X^{n-1} - \cdots - X - 1$ possède-t-il de racines réelles ?

(École normale supérieure)

▷ **Solution.**

On observe que 1 est racine de P_n pour tout $n \in \mathbb{N}^*$. Pour $n \geqslant 2$, on met en facteur $X - 1$ pour obtenir

$$P_n = (X-1)(nX^{n-1} + (n-1)X^{n-2} + \cdots + 2X + 1) = (X-1)Q_n'$$

avec $Q_n = X^n + X^{n-1} + \cdots + X + 1$. On a $Q_n = \dfrac{X^{n+1} - 1}{X - 1}$ de sorte qu'en dérivant, il vient

$$Q_n' = \frac{nX^{n+1} - (n+1)X^n + 1}{(X-1)^2}.$$

L'étude des variations du numérateur est enfantine et montre que Q_n' admet exactement une racine réelle (négative) si n est pair et n'admet aucune racine réelle si n est impair.

6. Le lecteur trouvera dans l'exercice 5.47 une inégalité (due à Landau) qui fournit une majoration de M(P).

Conclusion. Si n est pair, P_n admet 2 racines réelles (dont 1) et si n est impair, 1 est l'unique racine réelle de P_n. ◁

5.35. Un polynôme scindé sur $\mathbb{R}$

Montrer que, pour tous $n \geqslant 1$ et $\theta \in \mathbb{R}$ non multiple de π, le polynôme $P = \sum_{k=0}^{n} C_n^k \sin k\theta X^k$ a toutes ses racines réelles.

(École polytechnique)

▷ **Solution.**

Compte tenu de la factorisation $X^n - Y^n = \prod_{k=0}^{n-1} (X - e^{\frac{2ik\pi}{n}} Y)$, on peut écrire

$$\begin{aligned}
2iP(X) &= \sum_{k=0}^{n} C_n^k 2i \sin k\theta X^k = \sum_{k=0}^{n} C_n^k \left((e^{i\theta}X)^k - (e^{-i\theta}X)^k\right) \\
&= \left(1 + e^{i\theta}X\right)^n - \left(1 + e^{-i\theta}X\right)^n \\
&= \prod_{k=0}^{n-1} \left(1 + e^{i\theta}X - e^{i\frac{2k\pi}{n}}(1 + e^{-i\theta}X)\right) \\
&= \prod_{k=0}^{n-1} \left(1 - e^{i\frac{2k\pi}{n}} + (e^{i\theta} - e^{i\frac{2k\pi}{n}} e^{-i\theta})X\right).
\end{aligned}$$

On en déduit que si x, nombre complexe, est racine de P, l'un des facteurs $\left(1 - e^{i\frac{2k\pi}{n}} + (e^{i\theta} - e^{i\frac{2k\pi}{n}} e^{-i\theta})x\right)$ est nul. On a nécessairement $e^{i\theta} \neq e^{i\frac{2k\pi}{n}} e^{-i\theta}$, car sinon $1 = e^{i\frac{2k\pi}{n}}$ et $e^{i\theta} = e^{-i\theta}$, autrement dit $\theta \in \pi\mathbb{Z}$. On est donc en droit d'écrire

$$x = \frac{e^{i\frac{2k\pi}{n}} - 1}{e^{i\theta} - e^{i\frac{2k\pi}{n}} e^{-i\theta}} = \frac{e^{i\frac{k\pi}{n}} - e^{-i\frac{k\pi}{n}}}{e^{i\left(\theta - \frac{k\pi}{n}\right)} - e^{i\left(-\theta + \frac{k\pi}{n}\right)}} = \frac{\sin \dfrac{k\pi}{n}}{\sin\left(\theta - \dfrac{k\pi}{n}\right)}.$$

Le polynôme P n'a donc que des racines réelles. ◁

Le théorème de Rolle est un instrument efficace pour trouver des racines aux polynômes réels, comme l'illustre l'exercice suivant.

5.36. Dénombrement de racines réelles

Soit $P \in \mathbb{R}[X]$, un polynôme admettant n racines réelles simples strictement supérieures à 1. On pose

$$Q(X) = (1 + X^2)P(X)P'(X) + X(P(X)^2 + P'(X)^2).$$

Montrer que Q a au moins $2n - 1$ racines réelles distinctes.

(École polytechnique)

▷ **Solution.**

On a $Q = PP'X^2 + (P^2 + P'^2)X + PP'$, expression qui se factorise en

$$Q = (XP + P')(XP' + P)$$

(regarder Q comme un «polynôme du second degré en X»).

• Le polynôme $XP' + P$ est le polynôme dérivé de XP. Ce dernier admet comme racines celles de P, que l'on note $1 < x_1 < x_2 < \cdots < x_n$, et la racine $x_0 = 0$. Le théorème de Rolle nous assure de l'existence d'une racine de $XP' + P$ dans chaque intervalle $]x_i, x_{i+1}[$, $i \in [\![0, n-1]\!]$. Cela nous donne déjà n racines distinctes.

• Pour le second facteur, on introduit la fonction définie sur $\mathbb{R}$ par $f(x) = e^{x^2/2}P(x)$. Elle est de classe C^∞ et $f'(x) = e^{x^2/2}(P'(x) + xP(x))$. Le théorème de Rolle nous donne donc ici aussi $n - 1$ racines distinctes pour $XP + P'$ (une dans chaque intervalle $]x_i, x_{i+1}[$, $i \in [\![1, n-1]\!]$).

• Il reste enfin à vérifier que ces dernières racines diffèrent des précédentes. Or si $P(x) + xP'(x) = 0$ et $P'(x) + xP(x) = 0$, il vient $(1 - x^2)P(x) = 0$. Mais par construction les racines obtenues ci-dessus ne sont ni des racines de P, ni égales à ± 1. D'où le résultat : Q admet au moins $2n - 1$ racines réelles distinctes. ◁

On retiendra le résultat classique redémontré dans l'exercice suivant : si $P \in \mathbb{R}[X]$ est scindé sur $\mathbb{R}$, alors il en est de même de P'.

5.37. Dérivation et polynômes réels scindés

Soit $(P, Q) \in \mathbb{R}[X]^2$, $Q = \sum a_k X^k$. On pose $R = \sum a_k P^{(k)}$. Montrer que si P et Q sont scindés sur $\mathbb{R}$, alors R est scindé sur $\mathbb{R}$.

(École normale supérieure)

▷ **Solution.**

Si D désigne l'opérateur de dérivation sur $\mathbb{R}[X]$, on observe qu'en fait $R = Q(D)(P)$. Si Q est constant le résultat est trivial. Dans la suite, Q sera donc supposé de degré $p \geqslant 1$ et unitaire (ce qui ne nuit

nullement à la généralité). Il s'écrit donc $Q(X) = (X - \lambda_1)\dots(X - \lambda_p)$ (les λ_i n'étant pas nécessairement deux à deux distincts). On obtient alors $Q(D) = (D - \lambda_1 Id) \circ \cdots \circ (D - \lambda_p Id)$ dans l'algèbre $\mathcal{L}(\mathbb{R}[X])$. Il suffit donc de prouver le résultat suivant : pour tout $P \in \mathbb{R}[X]$ scindé et tout réel λ, $P' - \lambda P$ est aussi scindé.

Si P est constant, c'est clair. Supposons donc $n = \deg P \geqslant 1$ et notons $x_1 < \cdots < x_k$ les racines distinctes de P, de multiplicités respectives $\alpha_1, \dots, \alpha_k$.

• Le cas $\lambda = 0$ est classique : les x_i sont racines de P' d'ordre $\alpha_i - 1$, ce qui fournit $\sum_{i=1}^{k}(\alpha_i - 1) = n - k$ racines de P' comptés avec multiplicités. De plus, si $k > 1$, l'application du théorème de Rolle sur chacun des intervalles $[x_i, x_{i+1}]$, $1 \leqslant i \leqslant k - 1$, fournit $k - 1$ autres racines de P', deux à deux distinctes et distinctes des précédentes. Ce qui fait le bon compte.

• Le cas λ quelconque se traite de même : x_i est toujours racine de $P' - \lambda P$ de multiplicité $\alpha_i - 1$. Considérons alors la fonction définie sur $\mathbb{R}$ par $f(x) = P(x)e^{-\lambda x}$. On a $f'(x) = (P'(x) - \lambda P(x))e^{-\lambda x}$ et le théorème de Rolle qui s'applique encore sur les intervalles $[x_i, x_{i+1}]$ donne à nouveau $k-1$ racines supplémentaires. On a donc $(n-k)+(k-1) = n-1$ racines comptées avec multiplicité pour $P' - \lambda P$. Ce polynôme étant de degré n, il est nécessairement scindé (le facteur qui reste étant de degré 1).

Remarquons que si P est à racines simples, $P' - \lambda P$ l'est également. Il en résulte que si P est scindé à racines simples, R l'est aussi. ◁

5.38. Un théorème de Laguerre

> Soit P et Q deux polynômes non nuls de $\mathbb{R}[X]$, scindés sur $\mathbb{R}$. On suppose que les racines de Q ne sont pas dans l'intervalle $[0, \deg P]$. On note $P = \sum_{k=0}^{n} a_k X^k$ et $R = \sum_{k=0}^{n} a_k Q(k) X^k$. Montrer que R est scindé sur $\mathbb{R}$.
>
> **(École polytechnique)**

▷ **Solution.**

Sans perte de généralité, on peut supposer P et Q unitaires. On note n le degré de P et q celui de Q.

Une première constatation est qu'il suffit de montrer le résultat pour un polynôme Q de degré 1 (c'est trivial si Q est constant), car le résultat s'étend ensuite facilement par récurrence sur q. En effet, supposons le résultat vrai au rang $q - 1$. On écrit $Q = (X - \alpha)S$, où $S \in \mathbb{R}[X]$ est de degré $q - 1$ et α est une racine de Q. D'après l'hypothèse de récurrence,

le polynôme $\mathrm{T} = \sum_{k=0}^{n} a_k \mathrm{S}(k)\mathrm{X}^k$ est scindé sur $\mathbb{R}$ et d'après le cas $q = 1$, le polynôme $\mathrm{R} = \sum_{k=0}^{n} (a_k \mathrm{S}(k))(k-\alpha)\mathrm{X}^k = \sum_{k=0}^{n} a_k \mathrm{Q}(k)\mathrm{X}^k$ est scindé sur$\mathbb{R}$.

On suppose donc dans la suite que $\mathrm{Q} = \mathrm{X} - \alpha$, où par hypothèse $\alpha \notin [0, \deg \mathrm{P}] = [0, n]$. On a alors, avec $\mathrm{P} = \sum a_k \mathrm{X}^k$,

$$\mathrm{R} = \sum_{k=0}^{n} a_k (k-\alpha)\mathrm{X}^k = \sum_{k=0}^{n} a_k k \mathrm{X}^k - \alpha \sum_{k=0}^{n} a_k \mathrm{X}^k = \mathrm{XP}' - \alpha \mathrm{P}.$$

Le coefficient de X^n dans R est $a_n(n-\alpha) \neq 0$ de sorte que R est un polynôme de degré n.

On observe qu'une racine non nulle x_0 d'ordre k de P est racine d'ordre $k-1$ de R. En revanche, si 0 est racine d'ordre k de P, 0 reste racine d'ordre k de R. En effet, si $\mathrm{P} = \mathrm{X}^k \mathrm{P}_1$ avec $\mathrm{P}_1(0) \neq 0$, on obtient $\mathrm{P}' = \mathrm{X}^{k-1}(k\mathrm{P}_1 + \mathrm{XP}_1')$ et $\mathrm{R} = \mathrm{X}^k[(k-\alpha)\mathrm{P}_1 + \mathrm{XP}_1']$ et le polynôme entre crochets ne s'annule pas en 0 car $\alpha \neq k$.

On considère donc l'ensemble des racines de P auquel on rajoute, s'il n'est pas racine, le réel 0. On note $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ les éléments de cet ensemble et i_0 l'entier entre 1 et r tel que $\alpha_{i_0} = 0$. On note s_i l'ordre de α_i comme racine de P pour tout i compris entre 1 et r. Si $i \neq i_0$, on a $s_i \geqslant 1$, mais s_{i_0} peut être nul.

D'après ce qui est dit plus haut, pour $i \neq i_0$, α_i est racine d'ordre $s_i - 1$ de R ; $0 = \alpha_{i_0}$ est racine d'ordre s_{i_0} de R. Comme $s_1 + \cdots + s_r = n$, pour que R soit scindé sur $\mathbb{R}$, il suffit de trouver $r-1$ autres racines de R, distinctes des α_i, puisque

$$(s_1 - 1) + \cdots + s_{i_0} + \cdots + (s_r - 1) + (r-1) = n.$$

On remarque que $\mathrm{R} = \mathrm{XP}\left(\dfrac{\mathrm{P}'}{\mathrm{P}} - \dfrac{\alpha}{\mathrm{X}}\right)$. En écrivant

$$\mathrm{P}' = \sum_{i=1}^{r} s_i (\mathrm{X} - \alpha_i)^{s_i - 1} \prod_{k \neq i} (\mathrm{X} - \alpha_k)^{s_k} \quad \text{et} \quad \frac{\mathrm{P}'}{\mathrm{P}} = \sum_{i=1}^{r} \frac{s_i}{\mathrm{X} - \alpha_i},$$

on obtient

$$\mathrm{R} = \mathrm{XP}\left(\frac{s_1}{\mathrm{X} - \alpha_1} + \cdots + \frac{s_{i_0} - \alpha}{\mathrm{X}} + \cdots + \frac{s_r}{\mathrm{X} - \alpha_r}\right).$$

Il suffit donc de prouver que la fonction

$$f : x \longmapsto \left(\frac{s_1}{x - \alpha_1} + \cdots + \frac{s_{i_0} - \alpha}{x} + \cdots + \frac{s_r}{x - \alpha_r}\right)$$

s'annule $r-1$ fois sur son domaine de définition $\mathrm{D} = \mathbb{R} \backslash \{\alpha_1, \ldots, \alpha_r\}$. Nous distinguons deux cas.

⋆ Premier cas : $\alpha < 0$.

La fonction f est continue sur D. Comme les s_i sont strictement positifs ainsi que $s_{i_0} - \alpha$, on a, pour $1 \leqslant i \leqslant r-1$,

$$\lim_{\alpha_i^+} f = +\infty \quad \text{et} \quad \lim_{\alpha_{i+1}^-} f = -\infty$$

et d'après le théorème des valeurs intermédiaires, f s'annule sur $]\alpha_i, \alpha_{i+1}[$. D'où $r-1$ autres racines : c'est ce qu'on voulait.

⋆ Deuxième cas : $\alpha > n$.

On a $s_{i_0} - \alpha < 0$. Comme dans le premier cas, f s'annule sur $]\alpha_i, \alpha_{i+1}[$ pour $i \neq i_0 - 1$ et $i \neq i_0$. Mais on ne peut plus affirmer que f s'annule sur $]\alpha_{i_0-1}, \alpha_{i_0}[$ et sur $]\alpha_{i_0}, \alpha_{i_0+1}[$. Par contre, on a

$$f(x) \underset{-\infty}{\sim} \frac{s_1 + \cdots + s_{i_0} - \alpha + \cdots + s_r}{x} = \frac{n-\alpha}{x} \to 0^+ \quad \text{et} \quad \lim_{\alpha_1^-} f = -\infty,$$

si $\alpha_1 \neq 0$, *i.e.* $i_0 \neq 1$. D'après le théorème des valeurs intermédiaires, f s'annule sur $]-\infty, \alpha_1[$ si $i_0 \neq 1$. De manière analogue, f s'annule sur $]\alpha_r, +\infty[$ si $i_0 \neq r$. On a donc encore $r-1$ nouvelles racines (si $i_0 = 1$ ou r, f s'annule sur $r-2$ intervalles $]\alpha_i, \alpha_{i+1}[$).

Dans les deux cas, nous avons en tout $r-1$ racines nouvelles et R est scindé. ◁

5.39. Plans vectoriels de polynômes scindés

Soit (P, Q) un couple de polynômes réels.

1. On suppose que P et Q sont scindés à racines simples et que leurs racines sont entrelacées, c'est-à-dire que si α et β sont deux racines de l'un ($\alpha < \beta$), il y a au moins une racine de l'autre dans l'intervalle $]\alpha, \beta[$. Montrer que le polynôme $\lambda\mathrm{P} + \mu\mathrm{Q}$ reste scindé à racines simples lorsque (λ, μ) décrit $\mathbb{R}^2$.

2. Montrer que si pour tout $(\lambda, \mu) \in \mathbb{R}^2$, le polynôme $\lambda\mathrm{P}+\mu\mathrm{Q}$ est scindé à racines simples, alors les racines de P et Q sont entrelacées.

(École normale supérieure)

▷ **Solution.**

1. • De l'hypothèse, on déduit qu'entre deux racines consécutives de P (resp. Q) il y a exactement une racine de Q (resp. P) et donc que P et Q n'ont aucune racine commune. Ceci montre que, soit les degrés de P et Q sont égaux, soit ils diffèrent de 1. Supposons que $\deg(\mathrm{P}) \leqslant \deg(\mathrm{Q})$, notons n le degré de Q et $x_1, \ldots, x_n$ ses racines ($x_1 < \cdots < x_n$). On peut supposer P et Q unitaires. La propriété à démontrer est évidente

si $\lambda = 0$ ou $\mu = 0$; on suppose désormais $\lambda\mu \neq 0$. Le polynôme $\lambda P + \mu Q$ est alors de degré n sauf si $\deg(P) = \deg(Q) = n$ et si $\lambda + \mu = 0$.

• α est racine de $\lambda P + \mu Q$ si $Q(\alpha) \neq 0$ et $\dfrac{P(\alpha)}{Q(\alpha)} = -\dfrac{\mu}{\lambda}$. Nous allons donc étudier l'équation $F(x) = 0$, où F est la fraction rationnelle $\dfrac{P}{Q}$.

Par hypothèse, pour $1 \leqslant i \leqslant n-1$, Q ne change pas de signe et P change une fois de signe sur l'intervalle $]x_i, x_{i+1}[$. La fraction F change donc également de signe sur $]x_i, x_{i+1}[$. Puisque x_i et x_{i+1} sont des pôles simples de F, on en déduit que

$$\left(\lim_{x_i^+} F = -\infty \text{ et } \lim_{x_{i+1}^-} F = +\infty\right) \text{ ou } \left(\lim_{x_i^+} F = +\infty \text{ et } \lim_{x_{i+1}^-} F = -\infty\right).$$

Dans tous les cas, pour tout $i \in [\![1, n-1]\!]$, la fonction F prend une fois la valeur $-\dfrac{\mu}{\lambda}$ sur $]x_i, x_{i+1}[$, d'après le théorème des valeurs intermédiaires. La fraction F prend déjà $n-1$ fois la valeur $-\dfrac{\mu}{\lambda}$.

De plus, on a d'une part $\lim\limits_{x_1^-} F = -\infty$ et $\lim\limits_{x_n^+} F = +\infty$ ou $\lim\limits_{x_1^-} F = +\infty$ et $\lim\limits_{x_n^+} F = -\infty$, et d'autre part $\lim\limits_{-\infty} F = \lim\limits_{+\infty} F = 0$ (si $\deg P = n-1$) ou $\lim\limits_{-\infty} F = \lim\limits_{+\infty} F = 1$ (si $\deg P = n$). Si $\deg P = n-1$, alors F prend une fois la valeur $-\dfrac{\mu}{\lambda} \neq 0$, soit sur $]-\infty, x_1[$, soit sur $]x_n, +\infty[$, toujours d'après le théorème des valeurs intermédiaires. Cela reste vrai quand $\deg P = n$, sauf si $-\dfrac{\mu}{\lambda} = 1$.

Concluons. Si $\deg P = n-1$ ou $-\dfrac{\mu}{\lambda} \neq 1$, le polynôme $\lambda P + \mu Q$ possède n racines réelles distinctes. Il est donc scindé. Si $\deg P = n$ et si $-\dfrac{\mu}{\lambda} = 1$, le polynôme $\lambda P + \mu Q$ est de degré $n-1$ et possède $n-1$ racines distinctes. Il est encore scindé. Dans tous les cas, $\lambda P + \mu Q$ est scindé à racines simples.

2. • On voit en prenant $(\lambda, \mu) = (1, 0)$ ou $(0, 1)$ que P et Q sont scindés à racines simples. Montrons qu'ils n'ont aucune racine commune, en raisonnant par l'absurde. Si α est une racine commune à P et Q, il existe des polynômes P_1 et Q_1 tels que $P = (X-\alpha)P_1$ et $Q = (X-\alpha)Q_1$. On a alors, pour tout $(\lambda, \mu) \in \mathbb{R}^2$, $\lambda P + \mu Q = (X-\alpha)(\lambda P_1 + \mu Q_1)$. Mais α n'est racine ni de P_1, ni de Q_1. Si on choisit λ et μ tels que $\dfrac{\lambda}{\mu} = -\dfrac{Q_1(\alpha)}{P_1(\alpha)}$, alors α est racine double de $\lambda P + \mu Q$, ce qui est contraire à l'hypothèse.

• Montrons que les racines de P et Q sont entrelacées en raisonnant par l'absurde. Supposons par exemple qu'il existe deux racines consécutives de P, x et x' telles que Q ne s'annule pas sur le segment $[x, x']$ (on sait déjà qu'il ne s'annule ni en x ni en x'). La fonction $F = \dfrac{P}{Q}$ est donc définie et dérivable sur $[x, x']$; elle s'annule en x et x'. D'après le théorème de Rolle, il existe $\xi \in]x, x'[$, tel que $F'(\xi) = 0$. Alors ξ est

racine multiple de la fraction rationnelle $F - F(\xi)$. En multipliant par Q, on obtient que ξ est racine multiple de $P - F(\xi)Q$. C'est contraire à l'hypothèse. Les racines de P et Q sont donc entrelacées. $\lhd$

L'exercice suivant étudie dans un cas simple la question de la continuité des racines d'un polynôme par rapport à ses coefficients.

5.40. L'ouvert des polynômes scindés à racines simples sur $\mathbb{R}$ dans l'ensemble des polynômes unitaires de degré n

Soit $P = X^n + a_1X^{n-1} + \cdots + a_n$, un polynôme à coefficients réels scindé sur $\mathbb{R}$, à racines simples. Soit $Q = X^n + b_1X^{n-1} + \cdots + b_n$ un polynôme à coefficients réels. Montrer que si les b_i sont proches des a_i, alors Q est scindé sur $\mathbb{R}$, à racines simples.

(École polytechnique)

$\rhd$ **Solution.**

Notons $x_1, \ldots, x_n$ les n racines, rangées par ordre croissant, du polynôme P. Celui-ci s'annule et change de signe en $x_1, \ldots, x_n$, puisque ces racines sont simples. Considérons des réels $y_1, \ldots, y_n, y_{n+1}$ tels que $y_1 < x_1 < y_2 < \cdots < x_n < y_{n+1}$. On a alors $P(y_k)P(y_{k+1}) < 0$ pour tout $k \in [\![1, n]\!]$. La fonction

$$\Phi : (b_1, \ldots, b_n) \in \mathbb{R}^n \longmapsto (Q(y_1)Q(y_2), \ldots, Q(y_n)Q(y_{n+1})) \in \mathbb{R}^n$$

est continue puisque polynomiale. Par hypothèse, $\Phi(a_1, \ldots, a_n)$ appartient à $(\mathbb{R}_-^*)^n$. Cet ensemble étant un ouvert, on aura, pour $(b_1, \ldots, b_n)$ proche de $(a_1, \ldots, a_n)$ (pour une norme quelconque de $\mathbb{R}^n$, celles-ci étant équivalentes), $\Phi(b_1, \ldots, b_n) \in (\mathbb{R}_-^*)^n$, c'est-à-dire $Q(y_k)Q(y_{k+1}) < 0$ pour tout $k \in [\![1, n]\!]$. Alors la fonction Q change de signe, donc s'annule, entre y_k et y_{k+1}, pour tout $k \in [\![1, n]\!]$. Le polynôme Q s'annule donc n fois : il est scindé sur $\mathbb{R}$, à racines simples. $\lhd$

En choisissant y_k et y_{k+1} tels que $y_{k+1} - y_k \leqslant \varepsilon$, on montre que, pour $b_1, \ldots, b_n$ proche de $a_1, \ldots, a_n$, Q possède une racine z_k telle que $|x_k - z_k| \leqslant \varepsilon$. Ceci démontre que, pour $k \in [\![1, n]\!]$, la fonction, définie sur un voisinage de $(a_1, \ldots, a_n)$, qui à $(b_1, \ldots, b_n)$ associe la k-ième racine de Q (celles-ci étant rangées par ordre croissant) est continue.

Si cette démonstration ne s'applique plus, le théorème reste vrai dans $\mathbb{C}[X]$. On peut utiliser par exemple le discriminant (cf exercice 5.10) : celui-ci est une fonction polynomiale, donc continue, des coefficients de P ; si P n'a que des racines simples, son discriminant n'est pas nul et si les coefficients de Q sont proches de ceux de P, son discriminant reste non nul.

On ne saurait mieux terminer cette série d'exercices sur les polynômes scindés que par l'étude d'une famille de polynômes scindés sur $\mathbb{R}$, *aux riches propriétés : les polynômes de Tchebychev.*

5.41. Polynômes de Tchebychev

Soit $n \in \mathbb{N}^*$.

1. Montrer qu'il existe un unique polynôme $T_n \in \mathbb{R}[X]$ tel que, pour tout réel x, $T_n(\cos x) = \cos(nx)$. Calculer $T_{n+1} + T_{n-1}$.

Les polynômes T_n sont appelés *polynômes de Tchebychev de première espèce.*

2. Montrer que $T_n \in \mathbb{Z}[X]$, préciser son degré, son coefficient dominant. Déterminer les racines de T_n ainsi que les extrema de la fonction $x \longmapsto T_n(x)$ sur $[-1, 1]$.

3. Montrer que pour tout polynôme P à coefficients réels unitaire et de degré n, on a $\sup\limits_{x\in[-1,1]} |P(x)| \geqslant \dfrac{1}{2^{n-1}}$, avec égalité si et seulement si $P = \dfrac{1}{2^{n-1}} T_n$.

(École normale supérieure)

▷ **Solution.**

1. L'existence de T_n peut s'obtenir à l'aide de la formule de Moivre et de celle du binôme de Newton. On obtient

$$\cos(nx) = \mathrm{Re}(\cos x + i \sin x)^n = \sum_{0\leqslant 2k\leqslant n} C_n^{2k}(-1)^k \cos^{n-2k} x\ (1-\cos^2 x)^k,$$

ce qui prouve l'existence et donne l'expression suivante de T_n

$$T_n(X) = \sum_{k=0}^{E(n/2)} C_n^{2k}(X^2-1)^k X^{n-2k}.$$

Pour l'unicité, il suffit de dire que si R_n est un second polynôme qui convient, on a $(T_n - R_n)(\cos x) = 0$ pour tout réel x. Il en résulte que $T_n - R_n$ est identiquement nul sur $[-1, 1]$. C'est donc le polynôme nul.

Les formules de trigonométrie montrent que, pour tout $x \in \mathbb{R}$,

$$\begin{aligned}(T_{n+1} + T_{n-1})(\cos x) &= \cos(n+1)x + \cos(n-1)x \\ &= 2\cos x \cos nx = 2\cos x T_n(\cos x).\end{aligned}$$

Donc le polynôme $T_{n+1} - 2XT_n + T_{n-1}$ est identiquement nul sur $[-1, 1]$. Il en résulte qu'il est nul et on a la relation de récurrence :

$$\boxed{T_{n+1} - 2XT_n + T_{n-1} = 0}.$$

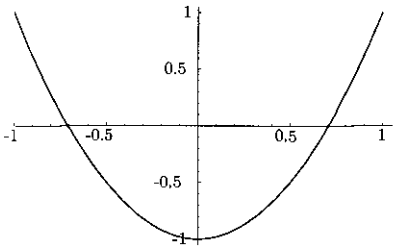
2. • On voit sur l'expression trouvé ci-dessus que $T_n \in \mathbb{Z}[X]$ et que $\deg(T_n) \leqslant n$. Comme le coefficient de X^n vaut $\sum_{k=0}^{E(n/2)} C_n^{2k} = 2^{n-1}$, on a $\deg(T_n) = n$.

On peut aussi montrer ces résultats par récurrence à l'aide de la relation de récurrence obtenue en 1.

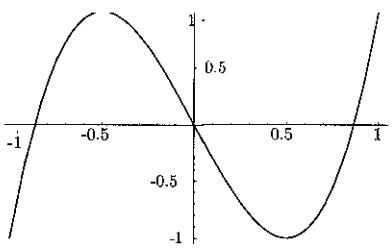
• Posons pour $k \in \mathbb{Z}$, $\theta_k = \dfrac{\pi}{2n} + \dfrac{k\pi}{n}$. On a évidemment $\cos(n\theta_k) = 0$ pour tout k. Il en résulte que $x_k = \cos\theta_k$ est une racine de T_n. Quand k décrit $\mathbb{Z}$, x_k prend n valeurs distinctes, obtenues en faisant varier k de 0 à $n-1$ par exemple. Comme $\deg(T_n) = n$, on dispose de toutes les racines de T_n, qui est donc scindé à racines simples sur $\mathbb{R}$. Notons que l'on a $-1 < x_{n-1} < \cdots < x_1 < x_0 < 1$.

• Comme $T_n(\cos\theta) = \cos n\theta$, on a $|T_n(z)| \leqslant 1$ pour tout $z \in [-1, 1]$. Il y a égalité si et seulement si z est de la forme $z_k = \cos\left(\dfrac{k\pi}{n}\right)$, avec $0 \leqslant k \leqslant n$. Plus précisément, $T_n(z_k) = 1$ si k est pair et $T_n(z_k) = -1$ si k est impair. Notons qu'en particulier, $T_n(1) = 1$ et $T_n(-1) = (-1)^n$.

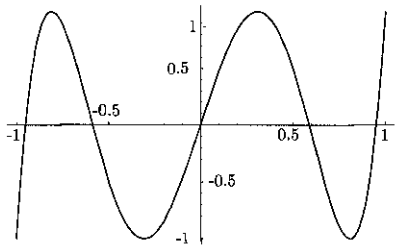
On voit que $-1 = z_n < x_{n-1} < z_{n-1} < \cdots < z_1 < x_0 < z_0 = 1$ et que la fonction T_n est strictement monotone entre deux z_k consécutifs. On a tracé les graphes sur $[-1, 1]$ de quelques polynômes.



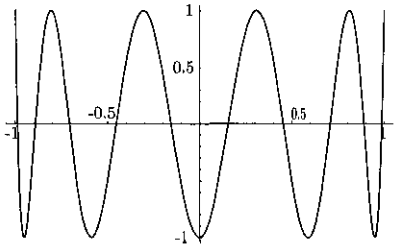
$n = 2$



$n = 3$



$n = 5$



$n = 10$

3. Pour tout polynôme P, on pose $\|P\| = \sup_{x \in [-1,1]} |P(x)|$. On considère

le polynome $P_n = \frac{1}{2^{n-1}} T_n$. Il est bien unitaire et de degré n. On a, d'après la question précédente, $\|P_n\| = 2^{1-n}$.

• Supposons qu'il existe un polynôme unitaire P de degré n tel que $\|P\| < \|P_n\|$. Étudions le polynôme $Q = P_n - P$. On a $\deg Q \leqslant n-1$ car P_n et P sont tous les deux unitaires de degré n. L'idée est de regarder les valeurs prises par Q aux points z_k (définis dans la question précédente). On a $Q(z_0) = P_n(z_0) - P(z_0) = \frac{1}{2^{n-1}} - P(z_0) > 0$ car $\|P\| < \|P_n\| = \frac{1}{2^{n-1}}$. De même $Q(z_1) < 0$, $Q(z_2) > 0$... Il résulte alors du théorème des valeurs intermédiaires que Q s'annule au moins une fois dans chaque intervalle $]z_{k+1}, z_k[$ pour $0 \leqslant k \leqslant n-1$. Ce qui donne n racines distinctes de Q. Comme Q est de degré $\leqslant n-1$, on a $Q = 0$, ce qui est absurde. On a donc $\|P\| \geqslant \|P_n\|$ pour tout polynôme P unitaire de degré n.

• On montre maintenant qu'il n'y a égalité dans $\|P\| \geqslant \|P_n\|$ que pour $P = P_n$. Reprenons le raisonnement précédent. Soit P unitaire de degré n tel que $\|P\| = \|P_n\|$ et $Q = P_n - P$. On a $\deg(Q) \leqslant n-1$ et $Q(z_0) \geqslant 0$, $Q(z_1) \leqslant 0$, $Q(z_2) \geqslant 0$... (on doit remplacer les inégalités strictes par des inégalités larges). Si toutes les inégalités sont strictes, Q est nul comme précédemment.

La situation est plus délicate si l'un des $Q(z_k)$ est nul. Si $1 \leqslant k \leqslant n-1$ et $Q(z_k) = 0$, alors $P(z_k) = \pm\frac{1}{2^{n-1}}$ et z_k est un extremum local de P. On a donc $P'(z_k) = 0$ et comme $P_n'(z_k) = 0$, on trouve $Q'(z_k) = 0$: z_k est une racine multiple de Q.

Montrons par récurrence sur $k \in [\![0, n-1]\!]$ que Q possède au moins k (resp. $k+1$) racines comptées avec leur multiplicité dans l'intervalle $[z_k, z_0] = [z_k, 1]$ si $Q(z_k) \neq 0$ (resp. $Q(z_k) = 0$). Il n'y a rien à prouver si $k = 0$. Supposons $k \geqslant 1$.

⋆ Si $Q(z_k) = 0$, z_k est une racine au moins double et comme il y en a au moins $k-1$ dans $[z_{k-1}, 1]$ (par hypothèse de récurrence), on en trouve donc au moins $k+1$ dans $[z_k, 1]$.

⋆ Si $Q(z_k) \neq 0$ et $Q(z_{k-1}) = 0$, l'hypothèse de récurrence assure l'existence de k zéros dans $[z_{k-1}, 1] \subset [z_k, 1]$.

⋆ Si $Q(z_k) \neq 0$ et $Q(z_{k-1}) \neq 0$, on a $Q(z_k)Q(z_{k-1}) < 0$ et Q s'annule sur $]z_k, z_{k-1}[$. Dans ce cas encore, on a donc au moins k racines dans $[z_k, 1]$.

La récurrence est achevée. Si $Q(z_{n-1}) = 0$, Q a donc au moins n racines dans $[-1, 1]$. Dans le cas contraire, $Q(-1)Q(z_{n-1}) \leqslant 0$ et Q s'annule sur $[-1, z_{n-1}[$. Comme on a déjà $n-1$ racines dans $[z_{n-1}, 1]$, on obtient dans ce cas aussi n racines dans $[-1, 1]$. Le polynôme Q est donc nul ce qui donne le résultat. ◁

La démonstration faite dans cet exercice peut se généraliser. On dit

qu'une fonction continue g équi-oscille sur $n+1$ points de $[a,b]$, s'il existe des points $z_0 < z_1 < \cdots < z_n$ de $[a,b]$ tels que, pour tout $i \in [\![0,n]\!]$, $|g(z_i)| = \|g\| = \sup_{t\in[a,b]} |g(t)|$ et $g(z_{i+1}) = -g(z_i)$ si $i < n$. On a vu que le polynôme T_n équi-oscille sur $n+1$ points de $[-1,1]$. On peut démontrer le théorème suivant : pour $f \in \mathcal{C}([a,b],\mathbb{R})$, il existe un polynôme unique (dit de meilleure approximation) qui réalise le minimum de distance de f à $\mathbb{R}_{n-1}[\mathrm{X}]$ au sens de la norme uniforme. Cet unique polynôme q est caractérisé par le fait que la fonction $f-q$ équi-oscille sur au moins $n+1$ points de $[a,b]$. L'exercice a montré que si on prend $[a,b]=[-1,1]$, alors $q = \frac{\mathrm{T}_n}{2^{n-1}} - \mathrm{X}^n$ réalise le minimum de distance de X^n à $\mathbb{R}_{n-1}[\mathrm{X}]$.

On peut démontrer, comme dans la première question de l'exercice précédent, que, pour $n \in \mathbb{N}$, il existe $\mathrm{U}_n \in \mathbb{R}[\mathrm{X}]$ de degré n tel que, pour tout $\theta \in \mathbb{R}$, $\sin(n+1)\theta = \sin\theta \mathrm{U}_n(\cos\theta)$. Le polynôme U_n est appelé n-ième polynôme de Tchebychev de seconde espèce. En dérivant la relation de définition de T_n, on obtient $\mathrm{T}'_n = n\mathrm{U}_{n-1}$.

La résolution de l'exercice suivant nécessite la connaissance des polynômes de Tchebychev.

5.42. Inégalités de Bernstein et de Markov

1. *Inégalité de Schur (1919).* Soit $\mathrm{P} \in \mathbb{R}_{n-1}[\mathrm{X}]$. Montrer que

$$[\forall x \in [-1,1],\ \sqrt{1-x^2}|\mathrm{P}(x)| \leqslant 1] \Longrightarrow [\forall x \in [-1,1],\ |\mathrm{P}(x)| \leqslant n].$$

(Indication : $x_0, x_1, \ldots, x_{n-1}$ étant les racines du n-ième polynôme de Tchebychev T_n, décomposer P dans la base des polynômes interpolateurs relatifs aux x_i.)

2. *Inégalité de Bernstein (1912).* Soit

$$\mathrm{Q}(\theta) = \sum_{k=0}^{n} (\lambda_k \cos k\theta + \mu_k \sin k\theta),$$

où les λ_k et μ_k sont réels. On suppose que $\sup_{\theta\in\mathbb{R}} |\mathrm{Q}(\theta)| \leqslant 1$. Montrer que $\sup_{\theta\in\mathbb{R}} |\mathrm{Q}'(\theta)| \leqslant n$.

3. *Inégalité de Markov (1889).* Soit $\mathrm{P} \in \mathbb{R}_n[\mathrm{X}]$. On suppose que $\sup_{|x|\leqslant 1} |\mathrm{P}(x)| \leqslant 1$. Montrer que $\sup_{|x|\leqslant 1} |\mathrm{P}'(x)| \leqslant n^2$.

(École normale supérieure)

▷ **Solution.**

1. Le n-ième polynôme de Tchebychev est de degré n et ses racines sont les $x_i = \cos\left(\dfrac{(2i+1)\pi}{2n}\right)$, où $i \in [\![0, n-1]\!]$. Notons $\theta_i = \dfrac{(2i+1)\pi}{2n}$. Les polynômes interpolateurs de base pour le n-uplet $(x_0, \ldots, x_{n-1})$ sont (cf. les rappels précédant l'exercice 5.25) les polynômes

$$\mathrm{L}_i(\mathrm{X}) = \frac{\Phi(\mathrm{X})}{\Phi'(x_i)(\mathrm{X} - x_i)} \ (0 \leqslant i \leqslant n-1), \text{ où } \Phi = \prod_{i=0}^{n-1}(\mathrm{X} - x_i).$$

On a donc

$$\mathrm{P} = \sum_{i=0}^{n-1} \mathrm{P}(x_i)\frac{\Phi}{\Phi'(x_i)(\mathrm{X} - x_i)} = \sum_{i=0}^{n-1} \mathrm{P}(x_i)\frac{\mathrm{T}_n}{\mathrm{T}'_n(x_i)(\mathrm{X} - x_i)},$$

puisque T_n est proportionnel à Φ. On va calculer les valeurs $\mathrm{T}'_n(x_i)$.

Par définition de T_n, on a, pour tout θ, $\mathrm{T}_n(\cos\theta) = \cos n\theta$ et donc, en dérivant, $-\sin\theta \mathrm{T}'_n(\cos\theta) = -n\sin n\theta$. On en déduit $\mathrm{T}'_n(x_i) = n\dfrac{\sin n\theta_i}{\sin\theta_i}$. On obtient

$$\sin n\theta_i = \sin\left((2i+1)\frac{\pi}{2}\right) = (-1)^i \quad \text{et} \quad \sin\theta_i = \sqrt{1 - x_i^2},$$

car θ_i est dans $]0, \pi[$, et donc $\mathrm{T}'_n(x_i) = \dfrac{(-1)^i n}{\sqrt{1 - x_i^2}}$, pour tout i de $[\![0, n-1]\!]$. On obtient finalement

$$\mathrm{P} = \mathrm{T}_n \sum_{i=0}^{n-1} \frac{\mathrm{P}(x_i)}{\mathrm{T}'_n(x_i)(\mathrm{X} - x_i)} = \frac{\mathrm{T}_n}{n} \sum_{i=0}^{n-1} (-1)^i \sqrt{1 - x_i^2}\,\frac{\mathrm{P}(x_i)}{\mathrm{X} - x_i}.$$

De l'égalité précédente, on déduit que, pour tout $x \in [-1, 1] \setminus \{x_0, \ldots, x_{n-1}\}$, on a

$$|\mathrm{P}(x)| \leqslant \frac{|\mathrm{T}_n(x)|}{n} \sum_{i=0}^{n-1} \sqrt{1 - x_i^2}\,\frac{|\mathrm{P}(x_i)|}{|x - x_i|} \leqslant \frac{|\mathrm{T}_n(x)|}{n} \sum_{i=0}^{n-1} \frac{1}{|x - x_i|}.$$

Si $x \in [-1, x_{n-1}[\cup]x_0, 1]$, alors tous les $x - x_i$ ont même signe. On peut donc écrire

$$|\mathrm{P}(x)| \leqslant \frac{|\mathrm{T}_n(x)|}{n} \left| \sum_{i=0}^{n-1} \frac{1}{x - x_i} \right|.$$

Mais $x_0, \ldots, x_{n-1}$ étant les n racines de T_n, on reconnaît dans la somme ci-dessus $\dfrac{\mathrm{T}'_n(x)}{\mathrm{T}_n(x)}$. On a donc $|\mathrm{P}(x)| \leqslant \dfrac{1}{n}|\mathrm{T}'_n(x)|$. Or on a vu que, pour

tout $\theta \in \mathbb{R}$ tel que $\sin\theta \neq 0$, on a $T_n'(\cos\theta) = \dfrac{n\sin n\theta}{\sin\theta}$. De l'inégalité, valable pour tout $\theta \in \mathbb{R}$, $|\sin n\theta| \leqslant n|\sin\theta|$ (qui se montre facilement par récurrence sur n), on déduit que $|T_n'(\cos\theta)| \leqslant n^2$. On obtient enfin, pour tout $x \in [-1, x_{n-1}[\cup]x_0, 1]$,

$$|P(x)| \leqslant \frac{1}{n}|T_n'(x)| \leqslant n,$$

ce qui est l'inégalité voulue.

Reste à examiner le cas où $x \in [x_{n-1}, x_0] = \left[-\cos\dfrac{\pi}{2n}, \cos\dfrac{\pi}{2n}\right]$. On a alors

$$|P(x)| \leqslant \frac{1}{\sqrt{1-x^2}} \leqslant \frac{1}{\sin\dfrac{\pi}{2n}}.$$

L'inégalité $|P(x)| \leqslant n$ est vérifiée si on a $\sin\dfrac{\pi}{2n} \geqslant \dfrac{1}{n}$. C'est vrai car on a, plus généralement, pour tout $x \in \left[0, \dfrac{\pi}{2}\right]$, $\sin x \geqslant \dfrac{2}{\pi}x$; cette inégalité résulte de la concavité de la fonction sinus sur $\left[0, \dfrac{\pi}{2}\right]$.

2. On va appliquer la question 1 à un polynôme P approprié. Soit θ un réel. Pour majorer $|Q'(\theta)|$, on utilise la définition de la dérivée comme limite du taux d'accroissement, mais on considère $Q(\theta+h) - Q(\theta-h)$, plutôt que $Q(\theta+h) - Q(\theta)$, pour des raisons de symétrie. Les formules de trigonométrie usuelles donnent, pour $h \in \mathbb{R}$,

$$\begin{aligned} Q(\theta+h) - Q(\theta-h) &= \sum_{k=0}^{n} \lambda_k(\cos(k(\theta+h)) - \cos(k(\theta-h)) \\ &\quad + \mu_k(\sin(k(\theta+h)) - \sin(k(\theta-h)) \\ &= 2\sum_{k=1}^{n} (-\lambda_k \sin k\theta + \mu_k \cos k\theta)\sin kh. \end{aligned}$$

On sait que, pour $k \in \mathbb{N}^*$ et $h \in \mathbb{R}$, on a $\sin kh = \sin h U_{k-1}(\cos h)$, où U_{k-1} est le $(k-1)$-ième polynôme de Tchebychev de seconde espèce ; il est de degré $k-1$. On a donc, θ étant fixé, pour tout réel h,

$$\begin{aligned} Q(\theta+h) - Q(\theta-h) &= 2\sin h \left(\sum_{k=1}^{n} (-\lambda_k \sin k\theta + \mu_k \cos k\theta)\, U_{k-1}(\cos h)\right) \\ &= 2\sin h\, P(\cos h), \end{aligned}$$

où P appartient à $\mathbb{R}_{n-1}[X]$.

Montrons que P vérifie l'hypothèse de la question 1.

Pour tout $x \in [-1, 1]$, il existe $h \in [0, \pi]$ tel que $x = \cos h$. On a alors

$$\sqrt{1-x^2}|P(x)| = |\sin h\, P(\cos h)| = \frac{1}{2}|Q(\theta+h) - Q(\theta-h)| \leqslant 1,$$

d'après l'hypothèse sur Q. Le polynôme vérifie donc l'hypothèse de la question 1. On en déduit que, pour tout $x \in [-1, 1]$, on a $|P(x)| \leqslant n$. En particulier, pour tout $h \in \mathbb{R}$ tel que $\sin h \neq 0$, on a

$$\left|\frac{Q(\theta + h) - Q(\theta - h)}{2 \sin h}\right| = |P(\cos h)| \leqslant n.$$

Sachant que

$$Q'(\theta) = \lim_{h \to 0} \frac{Q(\theta + h) - Q(\theta - h)}{2h} = \lim_{h \to 0} \frac{Q(\theta + h) - Q(\theta - h)}{2 \sin h},$$

on en déduit, en faisant tendre h vers 0, que $|Q'(\theta)| \leqslant n$. Ceci étant vrai pour tout réel θ, on a l'inégalité voulue.

3. On utilise la question précédente, en posant $Q(\theta) = P(\cos\theta)$ pour tout $\theta \in \mathbb{R}$. Montrons que Q a la même forme que dans la question précédente. Cela résulte de la linéarisation de $\cos^n \theta$, pour $n \in \mathbb{N}$, à l'aide de la formule du binôme et de la formule de Moivre. On a, pour tout $n \in \mathbb{N}$,

$$\cos^n \theta = \left(\frac{e^{i\theta} + e^{-i\theta}}{2}\right)^n = \frac{1}{2^n}\left(\sum_{k=0}^{n} C_n^k e^{i(n-2k)\theta}\right).$$

En regroupant les termes conjugués, on obtient

$$\cos^n \theta = \begin{cases} \dfrac{1}{2^{n-1}} \displaystyle\sum_{k=0}^{\frac{n-1}{2}} C_n^k \cos((n-2k)\theta) & \text{si } n \text{ est impair,} \\ \dfrac{1}{2^{n-1}} \displaystyle\sum_{k=0}^{\frac{n}{2}-1} C_n^k \cos((n-2k)\theta) + \dfrac{1}{2^n} & \text{si } n \text{ est pair.} \end{cases}$$

Chaque $\cos^k \theta$, pour $0 \leqslant k \leqslant n$, étant une combinaison linéaire à coefficients réels de $1, \cos\theta, \cos 2\theta, \ldots, \cos k\theta$, $P(\cos\theta)$ sera une combinaison linéaire de $1, \cos\theta, \cos 2\theta, \ldots, \cos n\theta$. Il existe donc des constantes réelles $\lambda_0, \lambda_1, \ldots, \lambda_n$ telles que, pour tout $\theta \in \mathbb{R}$, $Q(\theta) = \sum_{k=0}^{n} \lambda_k \cos k\theta$ et ainsi Q a la forme voulue.

On a, par hypothèse, pour tout $\theta \in \mathbb{R}$, $|Q(\theta)| = |P(\cos\theta)| \leqslant 1$. On en déduit, d'après la question 2 que, pour tout réel θ, $|Q'(\theta)| \leqslant n$. De l'égalité $Q'(\theta) = -\sin\theta P'(\cos\theta)$, on tire $|\sin\theta P'(\cos\theta)| \leqslant n$. En posant $x = \cos\theta$, on obtient alors, pour tout $x \in [-1, 1]$,

$$|\sqrt{1 - x^2} P'(x)| \leqslant n.$$

La fonction $\frac{1}{n} P'$ vérifie les hypothèses de la question 1. On en déduit que pour tout $x \in [-1, 1]$, on a $\frac{1}{n}|P'(x)| \leqslant n$ et donc $|P'(x)| \leqslant n^2$. $\lhd$

Par homogénéité, on en déduit pour tout polynôme trigonométrique Q *de degré inférieur ou égal à* n, $\sup_{\theta\in\mathbb{R}} |Q'(\theta)| \leqslant n \sup_{\theta\in\mathbb{R}} |Q(\theta)|$, *c'est-à-dire* $\|Q'\|_\infty \leqslant n\|Q\|_\infty$. *On a de même, pour* P *dans* $\mathbb{R}_n[X]$, $\|P'\| \leqslant n^2\|P\|$, *où* $\|P\| = \sup_{|x|\leqslant 1} |P(x)|$.

Les exercices qui suivent traitent du problème de la localisation des racines. Le premier démontre le très classique théorème de Gauss-Lucas et en donne quelques applications posées lors de différents oraux.

5.43. Théorème de Gauss-Lucas

1. Soit $P \in \mathbb{C}[X]$ non constant. Montrer que les racines de P' sont dans l'enveloppe convexe des racines de P.

2. Déterminer le plus grand entier $n \geqslant 2$ tel que les racines non nulles de $(X+1)^n - X^n - 1$ soient de module 1.

3. Soit P un polynôme non constant de $\mathbb{C}[X]$, Δ une droite du plan complexe, H_1 et H_2 les deux demi-plans ouverts limités par Δ. On suppose que P' a une racine dans H_1. Montrer que $P(H_1) = \mathbb{C}$.

(**École normale supérieure**)

▷ **Solution.**

1. On écrit $P = \lambda \prod_{k=1}^{r} (X-\lambda_k)^{n_k}$ où $r \geqslant 1$, $\lambda \in \mathbb{C}^*$, $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$ sont les racines deux à deux distinctes de P et $n_1, \ldots, n_r$ leur ordre respectif. Comme

$$P' = \lambda \sum_{k=1}^{r} n_k (X-\lambda_k)^{n_k-1} \prod_{l\neq k} (X-\lambda_l)^{n_l},$$

on a classiquement la décomposition en éléments simples de P'/P :

$$\frac{P'}{P} = \sum_{k=1}^{r} \frac{n_k}{X-\lambda_k}.$$

Prenons une racine z de P'. Si z est l'une des racines λ_k, elle est évidemment dans l'enveloppe convexe des racines de P. Sinon, on peut écrire

$$0 = \frac{P'(z)}{P(z)} = \sum_{k=1}^{r} \frac{n_k}{z-\lambda_k} = \sum_{k=1}^{r} n_k \frac{\overline{z-\lambda_k}}{|z-\lambda_k|^2},$$

ce qui donne en passant au conjugué $\sum_{k=1}^{r} n_k \frac{z-\lambda_k}{|z-\lambda_k|^2} = 0$ puis

$$z = \frac{\displaystyle\sum_{k=1}^{r} \frac{n_k}{|z-\lambda_k|^2}\lambda_k}{\displaystyle\sum_{k=1}^{r} \frac{n_k}{|z-\lambda_k|^2}}.$$

Comme chaque $\dfrac{n_k}{|z-\lambda_k|^2}$ est strictement positif, cette formule exprime le fait que z est un barycentre à coefficients strictement positifs des λ_k. La racine z de P' est donc dans l'enveloppe convexe des racines de P.

2. Si $n = 2$, P a une seule racine 0. Soit $n \geqslant 3$ et $P = (X+1)^n - X^n - 1$. On a alors $P' = n(X+1)^{n-1} - nX^{n-1}$. Si z une racine de P', on remarque que z ne peut être nul et donc

$$\left(\frac{z+1}{z}\right)^{n-1} = 1.$$

Il existe donc $k \in [\![0, n-2]\!]$ tel que $\dfrac{z+1}{z} = e^{\frac{2ik\pi}{n-1}}$. En fait, $k \neq 0$ puisque $z+1 \neq z$. On en déduit que les $n-2$ racines de P' sont les nombres complexes

$$z_k = \frac{e^{\frac{-ik\pi}{n-1}}}{2i\sin\dfrac{k\pi}{n-1}} \quad (1 \leqslant k \leqslant n-2).$$

Si toutes les racines de P sont de module 1, les racines de P' sont nécessairement dans le disque unité, puisque ce sont des barycentres à coefficients positifs des racines de P. Le module de z_1 est $\dfrac{1}{2\sin\frac{\pi}{n-1}} > 0$ et pour $n \geqslant 8$, on a

$$2\sin\frac{\pi}{n-1} < 2\sin\frac{\pi}{6} = 1 \quad \text{et} \quad |z_1| > 1,$$

donc un entier $n \geqslant 8$ ne convient pas.

Regardons $P_0 = (X+1)^7 - X^7 - 1$. Visiblement, -1 et 0 sont racines de P_0 qui s'écrit

$$P_0 = X(X+1)(7X^4 + 14X^3 + 21X^2 + 14X + 7).$$

Le polynôme $Q = 7X^4 + 14X^3 + 21X^2 + 14X + 7$, qui est un polynôme réciproque, peut se mettre sous la forme $X^2R\left(X + \dfrac{1}{X}\right)$ où $R \in \mathbb{R}[X]$. En effet, en posant $Y = X + \dfrac{1}{X}$, on a

$$\begin{aligned} Q &= X^2\left(7\left(X^2 + \frac{1}{X^2}\right) + 14\left(X + \frac{1}{X}\right) + 21\right) \\ &= X^2\left(7Y^2 - 14 - 14Y + 21\right) \\ &= 7X^2(Y-1)^2. \end{aligned}$$

Un racine z de P_0 distincte de 0 et -1 doit vérifier $z + \frac{1}{z} - 1 = 0$, ce qui équivaut à $z^2 - z + 1 = 0$ et donc à $z = -j$ ou $z = -j^2$. L'ensemble des racines de P_0 est donc $\{0, -1, -j, -j^2\}$ qui est contenu dans le disque unité.

Conclusion. Le plus grand entier n pour lequel $(X+1)^n - X^n - 1$ a toutes ses racines non nulles de module 1 est $n_0 = 7$.

3. Supposons que $P(H_1) \neq \mathbb{C}$. Considérons $z \in \mathbb{C}$ tel que $z \notin P(H_1)$. Les racines du polynôme $P - z$ appartiennent donc à $\mathbb{C} \setminus H_1 = \overline{H_2}$, adhérence de H_2. Comme $\overline{H_2}$ est convexe, le résultat rappelé ci-dessus montre que les racines de P' sont encore dans $\overline{H_2}$. Cela contredit l'existence d'une racine de P' dans H_1. On a donc $P(H_1) = \mathbb{C}$. $\lhd$

On pourra encore utiliser le théorème de Gauss-Lucas dans la seconde question de l'exercice suivant.

5.44. Polynôme à racines réelles

Soit $P \in \mathbb{C}[X]$. On suppose que P admet deux racines réelles distinctes et que P'' divise P.

1. Montrer que les racines de P sont toutes simples.

2. Montrer que les racines de P sont toutes réelles.

(École normale supérieure)

$\rhd$ **Solution.**

1. Notons $n \geqslant 2$ le degré de P. On peut supposer P unitaire sans perte de généralité et l'écrire sous la forme

$$P(X) = \prod_{i=1}^{p}(X - z_i) \prod_{j=1}^{q}(X - w_j)^{\alpha_j}$$

où les nombres complexes $z_1, \ldots, z_p, w_1, \ldots, w_q$ sont deux à deux distincts et où les exposants α_j sont tous supérieurs ou égaux à 2 (on a simplement factorisé P en isolant les racines simples). Le but est de montrer que $q = 0$. Chaque w_j est encore racine de P'' avec un ordre de multiplicité $\alpha_j - 2$. On peut donc écrire

$$P''(X) = R(X) \prod_{j=1}^{q}(X - w_j)^{\alpha_j - 2},$$

où R est un polynôme qui, par hypothèse, doit diviser $\prod_{i=1}^{p}(X - z_i)$.

Regardons ce que cela donne sur les degrés. On a $n = p + \sum_{j=1}^{q} \alpha_j$ et

$$n - 2 = \deg \mathrm{P}'' = r + \sum_{j=1}^{q} (\alpha_j - 2) = r + n - p - 2q,$$

où $r = \deg \mathrm{R} \leqslant p$. On en déduit que $(p - r) + 2q = 2$ ce qui laisse peu de possibilités (car $p - r \geqslant 0$). On veut montrer que $q = 0$ de sorte qu'il suffit d'exclure la solution $q = 1$, $p = r$. On aurait dans ce cas,

$$\begin{cases} \mathrm{P} = (\mathrm{X} - z_1) \dots (\mathrm{X} - z_p)(\mathrm{X} - w_1)^{\alpha_1} \\ \mathrm{P}'' = n(n-1)(\mathrm{X} - z_1) \dots (\mathrm{X} - z_p)(\mathrm{X} - w_1)^{\alpha_1 - 2}. \end{cases}$$

Il faut noter que cela serait parfaitement possible avec $p = 0$. Mais par hypothèse, P admet au moins deux racines distinctes et on a donc $p \geqslant 1$. Posons $\mathrm{S} = (\mathrm{X} - z_1) \dots (\mathrm{X} - z_p)$. On a $\mathrm{P} = (\mathrm{X} - w_1)^{\alpha_1} \mathrm{S}$ et en dérivant cela deux fois on obtient

$$\mathrm{P}'' = (\mathrm{X} - w_1)^{\alpha_1 - 2} [\alpha_1(\alpha_1 - 1)\mathrm{S} + 2\alpha_1(\mathrm{X} - w_1)\mathrm{S}' + (\mathrm{X} - w_1)^2 \mathrm{S}''].$$

Le polynôme entre crochets doit être égal à $\mathrm{R} = n(n-1)\mathrm{S}$. Mais sachant que $1 \leqslant \alpha_1 < n$ (car p n'est pas nul), on obtient une contradiction en évaluant en w_1, car on obtient alors que w_1 est racine de S.

Conclusion. Le cas $q = 1$ est impossible : on a $q = 0$ et $p = n$ de sorte que P est à racines simples dans $\mathbb{C}$.

2. Nous allons utiliser ici le théorème de Gauss-Lucas (voir l'exercice précédent) : si $\mathrm{Q} \in \mathbb{C}[\mathrm{X}]$, les racines de Q' qui ne sont pas racines de Q sont des barycentres à coefficients strictement positifs des racines de Q ; en particulier, elles se trouvent dans l'enveloppe convexe de l'ensemble des racines de Q. Nous allons appliquer cela à P et P'. D'après la question précédente le polynôme P admet n racines simples $z_1, \dots, z_n$ et le polynôme P'' qui divise P admet donc $n - 2$ racines simples à prendre parmi les z_i. L'enveloppe convexe de $z_1, \dots, z_n$ est un polygone convexe K du plan complexe. Quitte à renuméroter les z_i on peut supposer que $z_1, \dots, z_k$ sont les sommets de ce polygone. Imaginons que $k \geqslant 3$ c'est-à-dire que K n'est pas un segment. Les racines de P' sont alors nécessairement dans l'intérieur de K d'après le résultat que nous venons de rappeler. Et une nouvelle application de ce théorème montre qu'il en est de même des racines de P''. Mais il y a au plus $n - 3$ racines de P dans l'intérieur de K ce qui donne une contradiction. On a donc $k = 2$, c'est-à-dire que K est un segment. Comme par hypothèse P a deux racines réelles distinctes, le segment K est inclus dans $\mathbb{R}$ et on peut donc affirmer que toutes les racines de P sont réelles. $\lhd$

5.45. Théorème d'Eneström-Kakeya

Soit $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{R}[X]$ avec $a_k > 0$ pour tout k dans $[\![0, n]\!]$.

1. Montrer que si $a_0 \geqslant a_1 \geqslant \cdots \geqslant a_n$, alors les racines complexes de P sont toutes de module $\geqslant 1$.

2. Montrer, dans le cas général, que les racines complexes de P sont situées dans la couronne

$$\left\{z \in \mathbb{C},\ \min_{0\leqslant k\leqslant n-1} \frac{a_k}{a_{k+1}} \leqslant |z| \leqslant \max_{0\leqslant k\leqslant n-1} \frac{a_k}{a_{k+1}}\right\}.$$

(École polytechnique)

▷ **Solution.**

1. Soit z une racine de P. On a

$$(1-z)P(z) = 0 = -a_nz^{n+1} + (a_n - a_{n-1})z^n + \cdots + (a_1 - a_0)z + a_0,$$

de sorte que $a_0 = (a_0 - a_1)z + \cdots + (a_{n-1} - a_n)z^n + a_nz^{n+1}$. Supposons par l'absurde que $|z| < 1$. En passant au module dans cette égalité et en majorant par inégalité triangulaire, on obtient

$$a_0 = |a_0| < (a_0 - a_1) + (a_1 - a_2) + \cdots + (a_{n-1} - a_n) + a_n = a_0.$$

Contradiction.

2. Posons $r = \min\limits_{0\leqslant k\leqslant n-1} \dfrac{a_k}{a_{k+1}}$ et $R = \max\limits_{0\leqslant k\leqslant n-1} \dfrac{a_k}{a_{k+1}}$ et considérons le polynôme Q défini par

$$Q(X) = P(rX) = a_0 + ra_1X + \cdots + r^na_nX^n.$$

Alors Q satisfait les conditions de la question précédente. Si z est une racine de P, $\dfrac{z}{r}$ est une racine de Q. On a donc $\left|\dfrac{z}{r}\right| \geqslant 1$, soit $|z| \geqslant r$.

Pour la minoration, considérons

$$\widetilde{P} = X^nP\left(\frac{1}{X}\right) = a_0X^n + a_1X^{n-1} + \cdots + a_n.$$

Comme $\dfrac{a_{k+1}}{a_k} \geqslant \dfrac{1}{R}$, pour $0 \leqslant k \leqslant n-1$, d'après ce qu'on vient de démontrer, tout racine de $\widetilde{P}$ est de module $\geqslant \dfrac{1}{R}$. Si z est une racine de P, on a $z \neq 0$ puisque $a_0 > 0$ et $P(z) = z^n\widetilde{P}\left(\dfrac{1}{z}\right) = 0$. Ainsi, $\dfrac{1}{z}$ est une racine de $\widetilde{P}$, $\dfrac{1}{|z|} \geqslant \dfrac{1}{R}$ et finalement, $|z| \leqslant R$. ◁

5.46. Construction d'un polynôme satisfaisant des conditions sur le module de ses valeurs

Soit $P \in \mathbb{C}[X]$ non nul ayant une racine z_0 telle que $|z_0| < 1$. Montrer qu'il existe $Q \in \mathbb{C}[X]$ de degré inférieur ou égal à celui de P, tel que pour tout z de module 1 on ait $|Q(z)| = |P(z)|$ et pour tout z de module strictement inférieur à 1 on ait $|Q(z)| > |P(z)|$.

(École polytechnique)

▷ **Solution.**

On peut supposer P unitaire.

• Commençons par étudier le cas où $\deg P = 1$. On a alors $P = X - z_0$. Montrons que le polynôme $Q = 1 - \overline{z_0}X$ convient. L'hypothèse sur le degré est remplie et on a pour tout $z \in \mathbb{C}$,

$$\begin{aligned}|Q(z)|^2 - |P(z)|^2 &= (1 + |z|^2|z_0|^2 - z\overline{z_0} - \overline{z}z_0) - (|z|^2 + |z_0|^2 - z\overline{z_0} - \overline{z}z_0)\\ &= (1 - |z|^2)(1 - |z_0|^2).\end{aligned}$$

Le résultat en découle, car $1 - |z_0|^2 > 0$.

• Passons au cas général. Notons $z_0, z_1, \ldots, z_k$ les racines de P qui sont de module strictement inférieur à 1, comptées avec leur ordre de multiplicité. On peut écrire

$$P(X) = (X - z_0)\cdots(X - z_k)R(X),$$

où R est un polynôme qui ne s'annule pas dans le disque unité ouvert. Posons

$$Q(X) = (1 - \overline{z_0}X)\cdots(1 - \overline{z_k}X)R(X).$$

Il résulte du point précédent que si $|z| = 1$, alors $|Q(z)| = |P(z)|$ et que si $|z| < 1$, alors $|Q(z)| > |P(z)|$, car $|R(z)| > 0$. ◁

5.47. Inégalité de Landau

Pour $P = \sum_{i=0}^{n} a_i X^i \in \mathbb{C}[X]$, on pose $\|P\| = \left(\sum_{i=0}^{n} |a_i|^2\right)^{\frac{1}{2}}$.

1. Soit $R \in \mathbb{C}[X]$ et $z \in \mathbb{C}^*$. Montrer que

$$\|(1 - \overline{z}X)R\| = \|(X - z)R\|.$$

2. Soit $P \in \mathbb{C}[X]$ unitaire et de degré n. On note $M(P)$ le module du produit des racines hors du disque unité de $\mathbb{C}$ ($M(P) = 1$ s'il n'y en a pas). Montrer que $M(P) \leqslant \|P\|$.

(École polytechnique)

Solution.

1. Si $P \in \mathbb{C}[X]$, on a $\|P\|^2 = \frac{1}{2\pi}\int_0^{2\pi} P(e^{i\theta})\overline{P(e^{i\theta})}d\theta$: c'est la formule de Parseval appliquée à la fonction 2π-périodique $\theta \longmapsto P(e^{i\theta})$. Cette constatation conduit à une preuve particulièrement courte de l'égalité demandée. En effet, on a

$$\|(X-z)R\|^2 = \frac{1}{2\pi}\int_0^{2\pi}(e^{i\theta}-z)R(e^{i\theta})(e^{-i\theta}-\overline{z})\overline{R(e^{i\theta})}d\theta$$

et

$$\|(1-\overline{z}X)R\|^2 = \frac{1}{2\pi}\int_0^{2\pi}(1-\overline{z}e^{i\theta})R(e^{i\theta})(1-ze^{-i\theta})\overline{R(e^{i\theta})}d\theta$$

Il suffit de constater que $(e^{i\theta}-z)(e^{-i\theta}-\overline{z}) = (1-\overline{z}e^{i\theta})(1-ze^{-i\theta})$ pour tout θ. Notons qu'un calcul direct des quantités $\|(1-\overline{z}X)R\|$ et $\|(X-z)R\|$ permet de conclure également.

2. On suppose que P possède des racines de module strictement supérieur à 1 : sinon, $M(P) = 1$ et l'inégalité est vérifiée car $\|P\| \geqslant 1$ puisque P est unitaire. Notons $z_1, \ldots, z_r$ les racines de P de module inférieur ou égal à 1 et $z_{r+1}, \ldots, z_n$ les racines de module strictement supérieur à 1. On a donc $M(P) = \prod_{i=r+1}^{n} |z_i|$.

La question précédente montre que si on remplace dans P un facteur $(X - z_i)$ par $(1 - \overline{z_i}X)$ la norme ne change pas. On va effectuer cette substitution pour toutes les racines $z_1, \ldots, z_r$. Posons

$$Q = \prod_{i=1}^{r}(1-\overline{z_i}X)\prod_{j=r+1}^{n}(X-z_j).$$

On a $\|P\| = \|Q\|$. Mais le coefficient constant de Q est $\prod_{j=r+1}^{n} z_j$. On a donc $M(P) \leqslant \|Q\| = \|P\|$. ◁

5.48. Critère de Routh-Hurwitz pour le degré 3

Soit $P = X^3 + aX^2 + bX + c \in \mathbb{R}[X]$. Montrer que, pour que toutes les racines complexes de P aient une partie réelle strictement négative il faut et il suffit que $a > 0$, $b > 0$, $c > 0$ et $ab - c > 0$.

(**École normale supérieure**)

▷ **Solution.**

• P étant de degré impair, il possède au moins une racine réelle. Il existe donc $(\alpha, \beta, \gamma) \in \mathbb{R}^3$ tel que $P = (X + \alpha)(X^2 + \beta X + \gamma)$. Les racines de P ont toutes une partie réelle strictement négative si $\alpha > 0$ et si les parties réelles des racines x_1 et x_2 du polynôme $Q = X^2 + \beta X + \gamma$ sont strictement négatives.

Si le polynôme Q a deux racines réelles, c'est-à-dire si $\beta^2 \geqslant 4\gamma$, on doit avoir $x_1 x_2 = \gamma > 0$ et $x_1 + x_2 = -\beta < 0$, soit $\beta > 0$. S'il possède deux racines complexes conjuguées, c'est-à-dire si $\beta^2 < 4\gamma$, on a alors $\mathrm{Re}(x_1) = \mathrm{Re}(x_2) = \frac{1}{2}(x_1 + x_2) = \frac{-\beta}{2}$. Il faut donc $\beta > 0$; on remarque qu'on a, de plus, $\gamma > \frac{1}{4}\beta^2 > 0$. Dans tous les cas, il faut $\beta > 0$ et $\gamma > 0$.

Réciproquement, si les conditions $\beta > 0$ et $\gamma > 0$ sont réalisées, soit Q possède deux racines réelles et alors elles sont toutes deux négatives d'après ce qui précède, soit Q possède deux racines complexes conjuguées et leur partie réelle est négative puisque $\beta > 0$.

Les racines de P ont donc une partie réelle strictement négative si et seulement si $\alpha > 0, \beta > 0, \gamma > 0$.

• On remarque alors que $a = \alpha + \beta, b = \alpha\beta + \gamma, c = \alpha\gamma$. On en déduit que si $\alpha > 0$, $\beta > 0$ et $\gamma > 0$, alors $a > 0$, $b > 0$ et $c > 0$. Et on a de plus $ab - c = \beta(\alpha^2 + \alpha\beta + \gamma) > 0$.

Réciproquement, si on a $a > 0, b > 0, c > 0, ab - c > 0$, on obtient

$$\alpha + \beta > 0,\ \alpha\beta + \gamma > 0,\ \alpha\gamma > 0 \ \text{ et } \ \beta(\alpha^2 + \alpha\beta + \gamma) > 0.$$

On en déduit que $\alpha^2 + \alpha\beta + \gamma \geqslant \alpha\beta + \gamma > 0$; la dernière inégalité donne alors $\beta > 0$. D'autre part, α et γ sont de même signe ; s'ils étaient tous deux négatifs, on aurait $\alpha\beta + \gamma < 0$. On a donc $\alpha > 0, \beta > 0, \gamma > 0$, et d'après ce qui précède, les racines complexes du polynôme P ont toutes une partie réelle strictement négative.

Conclusion. Les racines complexes du polynôme $X^3 + aX^2 + bX + c$ ont une partie réelle strictement négative si et seulement si

$$\boxed{a > 0, b > 0, c > 0, ab - c > 0}. \ \triangleleft$$

La règle de Descartes et le théorème de Sturm ramènent l'étude du nombre de racines sur un intervalle d'un polynôme à coefficients réels à l'évaluation d'une fonction simple — un nombre de changements de signe — en deux points. Ce sont des méthodes aisément programmables et présentes dans les logiciels de calcul formel (fonctions sturm, sturmseq, realroot de Maple).

5.49. Règle de Descartes

On considère un polynôme P à coefficients réels de degré n. Pour tout réel x, on considère la suite $(P^{(k)}(x))_{k\in[\![0,n]\!]}$. On note $V(x)$ le nombre de changements de signe stricts de cette suite : $V(x)$ est le cardinal de

$$\{(i,j), 0\leqslant i<j\leqslant n,\ P^{(i)}(x)P^{(j)}(x)<0 \text{ et } P^{(k)}(x)=0 \text{ si } i<k<j\}.$$

1. Soit a et b tels que $P(a)P(b)\neq 0$ et $\mu(a,b)$ le nombre de racines de P dans l'intervalle $[a,b]$, comptées avec leur ordre de multiplicité. Montrer que

$$\mu(a,b)\leqslant V(a)-V(b) \quad \text{et} \quad \mu(a,b)\equiv V(a)-V(b) \pmod 2.$$

2. On note $P=a_0+a_1X+\cdots+a_nX^n$, $\nu(P)$ le nombre de changements de signe dans la suite $(a_0,\ldots,a_n)$ et $\mu(P)$ le nombre de racines de P dans $\mathbb{R}_+^*$ comptées avec leur ordre de multiplicité.

Montrer que $\mu(P)\leqslant\nu(P)$ et que $\mu(P)\equiv\nu(P) \pmod 2$.

(**École normale supérieure**)

Solution.

1. Il s'agit d'étudier comment varie V sur l'intervalle $[a,b]$.

Remarquons que la fonction V est constante sur chaque intervalle contenu dans $[a,b]$ sur lequel aucune fonction $P^{(k)}$ $(0\leqslant k\leqslant n)$ ne s'annule.

Il suffit donc de voir comment varie $V(x)$ quand x «traverse» en croissant une racine d'un des polynômes $P^{(k)}$ $(0\leqslant k\leqslant n)$.

Le raisonnement qui suit est basé sur la remarque simple que voici. Supposons que c soit une racine d'un polynôme A, non nul. La fonction polynôme A^2 présente en c un minimum strict. Sa dérivée $2AA'$ est négative, puis positive, sur un voisinage de c. Ainsi, pour $h\neq 0$ assez petit, $A(c+h)A'(c+h)$ a le signe de h.

• Supposons que c est une racine de P d'ordre m : c annule donc les polynômes $P, P', \ldots, P^{(m-1)}$, mais pas $P^{(m)}$. On en déduit que, pour $h\neq 0$ assez petit et $0\leqslant i\leqslant m-1$, $P^{(i)}(c+h)P^{(i+1)}(c+h)$ a le signe de h et donc est négatif, puis positif. On en déduit qu'en traversant c, $V(x)$ diminue de m, ordre de multiplicité de c.

• Supposons maintenant que c est une racine de $P^{(k)}$ d'ordre m (on suppose $P^{(k-1)}(c)\neq 0$). Le même raisonnement que précédemment montre qu'on a une diminution de $V(x)$ de m, car les produits $P^{(i)}(x)P^{(i+1)}(x)$, pour $k\leqslant i\leqslant k+m-1$ de négatifs deviennent positifs quand x traverse c.

Mais une variation supplémentaire de $V(x)$ peut être due au changement de signe de $P^{(k-1)}(x)P^{(k)}(x)$. On a, par hypothèse, $P^{(k-1)}(c) \neq 0$ et donc $P^{(k-1)}$ garde un signe constant dans un voisinage de c. Quant à $P^{(k)}$, il change de signe en c si m est impair.

Si m est pair, $V(x)$ diminue donc de m ; si m est impair, $V(x)$ diminue donc de $m-1$ ou $m+1$ selon que $P^{(k-1)}(x)P^{(k)}(x)$ est positif ou négatif avant c. Dans tous les cas, $V(x)$ diminue ici d'un nombre pair.

• Quant on fait la somme de toutes les diminutions obtenues de la fonction V entre a et b, on trouve la somme des ordres de multiplicité des racines de P sur $]a,b[$, et donc sur $[a,b]$, car $P(a)P(b) \neq 0$, c'est-à-dire $\mu(a,b)$, à quoi s'ajoute un entier naturel pair. Il existe donc $N \in \mathbb{N}$ tel que $V(a) - V(b) = \mu(a,b) + 2N$. On en déduit que

$$\mu(a,b) \leqslant V(a) - V(b) \text{ et } \mu(a,b) \equiv V(a) - V(b) \pmod 2.$$

2. Quitte à diviser le polynôme P par X^k, où k est sa valuation, ce qui ne modifie ni $\mu(P)$, ni $\nu(P)$, on peut supposer que $a_0 \neq 0$.

En 0, on obtient $P^{(i)}(0) = i!\,a_i$, pour $0 \leqslant i \leqslant n$. On en déduit que $V(0) = \nu(P)$.

D'autre part, étant donné un polynôme quelconque A, pour x assez grand $A(x)$ garde un signe constant, celui de son coefficient dominant. On peut donc trouver $\alpha \in \mathbb{R}_+^*$ tel que, pour $x \geqslant \alpha$, $P(x), P'(x), \ldots, P^{(n)}(x)$ ont le signe de a_n. On en déduit que, pour $x \geqslant \alpha$, on a $V(x) = 0$.

Nous obtenons donc finalement $V(0) - V(\alpha) = \nu(P)$.

Nous voyons, d'autre part, que toutes les racines positives de P et de ses dérivées non nulles appartiennent à l'intervalle $]0,\alpha[$. De la première question, appliquée à l'intervalle $[0,\alpha]$, nous déduisons donc que

$$\mu(P) \leqslant \nu(P) \text{ et } \mu(P) \equiv \nu(P) \pmod 2. \lhd$$

5.50. Théorème de Sturm

Soit $P \in \mathbb{R}[X]$. On pose $S_0 = P, S_1 = P'$, puis, aussi longtemps que c'est possible, $S_{i-1} = A_i S_i - S_{i+1}$, avec $\deg(S_{i+1}) < \deg(S_i)$.

Pour x réel, on note $V(x)$ le nombre de changements de signes (stricts) de la suite $S_0(x), \ldots, S_p(x)$, lorsque $S_{p+1} = 0$. Ainsi, $V(x)$ est le cardinal de l'ensemble

$$\{(i,j), 0 \leqslant i < j \leqslant p, S_i(x)S_j(x) < 0 \text{ et } S_k(x) = 0 \text{ si } i < k < j\}.$$

Soit $a < b$. On suppose que $P(a)P(b) \neq 0$. Montrer que le nombre de racines distinctes de P dans $[a,b]$ est égal à $V(a) - V(b)$.

(École normale supérieure)

Solution.

• S_{i+1} est l'opposé du reste dans la division euclidienne de S_{i-1} par S_i. Celle-ci est possible tant que S_i n'est pas nul. La suite $S_0, \ldots, S_p, S_{p+1}$ est donc au signe près la suite des restes obtenus en calculant le pgcd de P et P′ par l'algorithme d'Euclide. Par construction, on a donc, pour tout $i \in [\![0, p]\!]$,

$$\mathrm{pgcd}(S_i, S_{i+1}) = S_p.$$

On se ramène à un polynôme n'ayant que des racines simples en posant, pour tout $i \in [\![0, p]\!]$,

$$T_i = \frac{S_i}{S_p}.$$

Alors, pour tout $i \in [\![0, p]\!]$, les polynômes T_i et T_{i+1} sont premiers entre eux et n'ont donc pas de racine commune ; on note que $T_p = 1$.

Les racines de T_0 sont les racines de P, mais toutes les racines de T_0 sont simples. En effet, si α est racine de P d'ordre m, alors α est racine d'ordre $m-1$ de P′ et $(X-\alpha)^{m-1}$ est en facteur dans S_p.

• Notons que si $S_p(x) \neq 0$, $V(x)$ est égal au nombre $V_1(x)$ de changements de signes (stricts) de la suite $T_0(x), \ldots, T_p(x)$. C'est vrai en particulier si $x = a$ ou b (car $P(x) \neq 0$ implique $S_p(x) \neq 0$). On a donc

$$V(a) - V(b) = V_1(a) - V_1(b).$$

• Il s'agit de démontrer que $V_1(a) - V_1(b)$ est égal au nombre de racines de P (ou de T_0) sur $[a, b]$.

On remarque d'abord que la fonction V_1 est constante sur tout intervalle contenu dans $[a, b]$ sur lequel aucune des fonctions T_i ne s'annule.

Comme les fonctions T_i n'ont qu'un nombre fini de racines, il suffit de démontrer que V_1 possède les deux propriété suivantes :

(*i*) $V_1(x)$ diminue de 1 quand x «traverse» une racine de T_0, c'est-à-dire une racine de P ;

(*ii*) $V_1(x)$ ne change pas lorsque x «traverse» un point α tel que $T_0(\alpha)$ est non nul et $T_i(\alpha) = 0$ pour au moins un indice $i \geqslant 1$.

• Supposons que α soit une racine de P. La fonction P^2 présente en α un minimum. Sa dérivée $2PP'$ est donc négative, puis positive. Ainsi, pour $h \neq 0$ assez petit $P(\alpha+h)P'(\alpha+h)$ a le signe de h et donc $T_0(\alpha+h)T_1(\alpha+h)$ a le signe de h (car $(S_p(\alpha+h))^2 > 0$ si $P(\alpha+h) \neq 0$). Ce qui montre qu'après la traversée de α, il y a un changement de signe de moins entre les termes d'indice 0 et 1.

• Supposons maintenant que α soit une racine de T_i, avec $i \geqslant 1$; on a nécessairement $i < p$. De l'égalité $S_{i-1} = A_i S_i - S_{i+1}$, on déduit $T_{i-1} = A_i T_i - T_{i+1}$, puis $T_{i-1}(\alpha) = -T_{i+1}(\alpha)$. Mais α n'est pas racine de T_{i-1}, ni de T_{i+1}. On a donc $T_{i-1}(\alpha)T_{i+1}(\alpha) < 0$. Par continuité, on

on déduit qu'on a encore $T_{i-1}(x)T_{i+1}(x) < 0$, pour x dans un voisinage de α. Le nombre de changements de signe entre les termes d'indices $i-1$ et $i+1$ ne change pas, il reste égal à 1 (quel que soit le signe de $T_i(x)$ sur ce voisinage de α).

Ceci achève la démonstration. ◁

Les exercices suivants traitent de fractions rationnelles. Le premier est une classique décomposition en éléments simples. Rappelons que si α est un pôle simple de la fraction rationnelle $F = \dfrac{P}{Q}$, la partie polaire de F relative à α est $\dfrac{P(\alpha)}{(X-\alpha)Q'(\alpha)}$.

5.51. Décomposition en éléments simples

Soit P un polynôme de $\mathbb{C}[X]$ n'admettant que des racines simples non nulles $x_1, \ldots, x_n$.

Montrer que $\displaystyle\sum_{i=1}^{n} \frac{1}{x_i P'(x_i)} = -\frac{1}{P(0)}$. Que vaut $\displaystyle\sum_{i=1}^{n} \frac{1}{P'(x_i)}$?

(École polytechnique)

▷ **Solution.**

• On décompose en éléments simples $F(X) = \dfrac{1}{P(X)}$. Les pôles de F sont les x_i et ils sont tous simples par hypothèse. Puisque la partie entière de F est nulle on a

$$F(X) = \frac{1}{P(X)} = \sum_{k=1}^{n} \frac{1}{\prod_{k \neq i}(x_i - x_k)} \frac{1}{X - x_i} = \sum_{k=1}^{n} \frac{1}{P'(x_i)(X - x_i)}. \quad (*)$$

L'identité demandée s'obtient en évaluant cette égalité en 0.

• Pour calculer la somme $\displaystyle\sum_{i=1}^{n} \frac{1}{P'(x_i)}$, on multiplie $(*)$ par X, on évalue en x réel et on fait tendre x vers l'infini : $\displaystyle\sum_{i=1}^{n} \frac{1}{P'(x_i)}$ vaut 1 si $n = 1$ et 0 si $n > 1$. ◁

L'exercice qui suit offre, à partir d'une relation remarquable entre P *et* P′*, une preuve très simple d'une inégalité de Bernstein. Elle a été trouvée en 1973 par P.J. O'Hara.*

5.52. Inégalité de Bernstein

1. Soit $n \in \mathbb{N}^*$ et $z_1, \ldots, z_n$ les racines de $X^n + 1$. Démontrer que pour tout polynôme P de $\mathbb{C}_n[X]$, on a

$$XP'(X) = \frac{n}{2}P(X) + \frac{2}{n}\sum_{k=1}^{n} \frac{z_k P(z_k X)}{(z_k - 1)^2}.$$

2. Si $P \in \mathbb{C}[X]$ on pose $\|P\| = \sup_{|z|=1} |P(z)|$. Montrer que pour tout $P \in \mathbb{C}_n[X]$ on a $\|P'\| \leqslant n\|P\|$.

(**École Polytechnique**)

▷ **Solution.**

1. Par linéarité, il suffit de vérifier l'identité pour $P = X^\ell$, lorsque ℓ est dans $[\![0, n]\!]$. Il s'agit donc de calculer

$$\alpha = \sum_{k=1}^{n} \frac{z_k z_k^\ell}{(z_k - 1)^2} = \sum_{k=1}^{n} \frac{z_k^{\ell+1}}{(z_k - 1)^2}$$

et de vérifier la relation $\ell = \frac{n}{2} + \frac{2}{n}\alpha$. Le carré au dénominateur fait penser à une dérivée. On considère donc $F = \frac{X^\ell}{X^n + 1}$ que l'on va dériver. Décomposons F en éléments simples dans $\mathbb{C}(X)$: il s'agit de trouver $\mu_1, \ldots, \mu_n$ dans $\mathbb{C}$ tels que

$$F = \sum_{k=1}^{n} \frac{\mu_k}{X - z_k} + E(F),$$

où $E(F)$ désigne la partie entière de F qui vaut 0 si $\ell < n$ et 1 si $\ell = n$. Fixons $k \in [\![1, n]\!]$, on a alors

$$\mu_k = \left(X^\ell \frac{X - z_k}{X^n + 1}\right)(z_k) = \frac{z_k^\ell}{\prod_{j \neq k}(z_k - z_j)} = \frac{z_k^\ell}{T'(z_k)},$$

où $T = X^n + 1$. Ainsi, on obtient $\mu_k = \frac{z_k^\ell}{n z_k^{n-1}} = -\frac{z_k^{\ell+1}}{n}$ car $z_k^n = -1$. Il en résulte

$$F = -\frac{1}{n}\sum_{k=1}^{n} \frac{z_k^{\ell+1}}{(X - z_k)} \quad \text{et} \quad F' = \frac{1}{n}\sum_{k=1}^{n} \frac{z_k^{\ell+1}}{(X - z_k)^2}.$$

On a donc $F'(1) = \frac{\alpha}{n} = \frac{2\ell - n}{4}$ puisque $F' = \frac{\ell X^{\ell-1}(X^n + 1) - nX^{n-1}X^\ell}{(X^n + 1)^2}$. Dans ces conditions, on obtient

$$\frac{n}{2} + \frac{2}{n}\alpha = \frac{n}{2} + \frac{2\ell - n}{2} = \ell.$$

C'est ce qu'on voulait.

2. Soit $P \in \mathbb{C}_n[X]$. Appliquons la formule précédente en un point z de module 1. Par inégalité triangulaire, il vient

$$|P'(z)| \leqslant \left(\frac{n}{2} + \frac{2}{n}\sum_{k=1}^{n} \frac{|z_k|}{|z_k - 1|^2}\right) \|P\|$$

car les z_k sont tous de module 1. Il nous suffit donc de prouver que $\sum_{k=1}^{n} \frac{|z_k|}{|z_k - 1|^2} \leqslant \frac{n^2}{4}$. Le point clé est que si $z = e^{i\theta}$ est un nombre complexe de module 1 distinct de 1, alors

$$\frac{z}{(z-1)^2} = \frac{e^{i\theta}}{(e^{i\theta} - 1)^2} = \frac{1}{(e^{i\theta/2} - e^{-i\theta/2})^2} = \frac{-1}{4\sin^2\frac{\theta}{2}}$$

est un réel négatif. C'est en particulier le cas pour les z_k. On a donc

$$\sum_{k=1}^{n} \frac{|z_k|}{|z_k - 1|^2} = -\sum_{k=1}^{n} \frac{z_k}{(z_k - 1)^2} = \frac{n^2}{4}$$

d'après la question 1 appliquée avec le polynôme constant $P = 1$. D'où le résultat. ◁

5.53. Inversion de la matrice de Hilbert

Soit $(a_1, \ldots, a_n)$, $(b_1, \ldots, b_n)$ et $(c_1, \ldots, c_n)$ dans $\mathbb{R}^n$. On suppose que les a_i sont deux à deux distincts de même que les b_j. On suppose de plus que $a_i + b_j \neq 0$ pour tout $(i, j) \in [\![1, n]\!]^2$.

1. Résoudre le système : $\forall j \in [\![1, n]\!]$, $\sum_{i=1}^{n} \frac{x_i}{a_i + b_j} = c_j$.

2. Soit $H = (h_{ij}) \in \mathcal{M}_n(\mathbb{R})$ avec $h_{ij} = \frac{1}{i + j - 1}$. Montrer que H est inversible et que H^{-1} est à coefficients entiers.

(École normale supérieure)

▷ **Solution.**

1. Pour $(x_1, \ldots, x_n) \in \mathbb{R}^n$, on considère la fraction $F = \sum_{i=1}^{n} \frac{x_i}{a_i + X}$. Si l'on note P le polynôme $(X+a_1)\ldots(X+a_n)$, alors il existe un polynôme Q de $\mathbb{R}_{n-1}[X]$ tel que $F = \frac{Q}{P}$ puisque $\deg F \leqslant -1$.

Le système considéré équivaut à : pour tout $j \in [\![1, n]\!]$,

$$F(b_j) = c_j, \text{ c'est-à-dire } Q(b_j) = P(b_j)c_j.$$

Les n réels $b_1, \ldots, b_n$ étant distincts, ces conditions déterminent un polynôme unique Q de $\mathbb{R}_{n-1}[X]$, qui s'exprime en fonction des polynômes interpolateurs de Lagrange relatifs au système $(b_1, \ldots, b_n)$, c'est-à-dire les polynômes $L_j = \dfrac{\prod\limits_{k \neq j}(X - b_k)}{\prod\limits_{k \neq j}(b_j - b_k)}$, par $Q = \sum\limits_{j=1}^{n} P(b_j)c_jL_j$. La fraction rationnelle $F = \dfrac{Q}{P}$ est donc entièrement déterminée. On en déduit que le système considéré admet une solution unique. En effet, F se décompose de manière unique en $F = \sum\limits_{i=1}^{n} \dfrac{x_i}{a_i + X}$. On obtient, pour tout $i \in [\![1, n]\!]$.

$$x_i = \frac{Q(-a_i)}{P'(-a_i)} = \frac{1}{P'(-a_i)} \sum_{j=1}^{n} P(b_j)c_jL_j(-a_i).$$

On note que

$$P'(-a_i) = \prod_{k \neq i}(a_k - a_i),$$

et que

$$L_j(-a_i) = \frac{\prod\limits_{k \neq j}(-a_i - b_k)}{\prod\limits_{k \neq j}(b_j - b_k)} = \prod_{k=1}^{n}(a_i + b_k)\frac{1}{(a_i + b_j)\prod\limits_{k \neq j}(b_k - b_j)}.$$

On obtient finalement

$$x_i = \frac{\prod\limits_{k=1}^{n}(a_i + b_k)}{\prod\limits_{k \neq i}(a_k - a_i)} \sum_{j=1}^{n} c_j \frac{\prod\limits_{k \neq i}(a_k + b_j)}{\prod\limits_{k \neq j}(b_k - b_j)}.$$

2. Avec les notations de la question précédente, si on note A la matrice de $\mathcal{M}_n(\mathbb{R})$ dont le coefficient d'indice (i, j) est $\dfrac{1}{a_i + b_j}$ (matrice de Cauchy), le système devient $AX = C$, où $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$ et $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$.

Nous avons démontré que ce système a une solution unique pour tout $C \in \mathbb{R}^n$. La matrice A est donc inversible et l'expression des x_i en fonction des c_j donne les coefficients de A^{-1}.

Le coefficient d'indice (i,j) de A^{-1} est

$$a'_{i,j} = \frac{\prod\limits_{k=1}^{n}(a_i+b_k)}{\prod\limits_{k\neq i}(a_k-a_i)}\,\frac{\prod\limits_{k\neq i}(a_k+b_j)}{\prod\limits_{k\neq j}(b_k-b_j)}.$$

La matrice H (matrice de Hilbert) est un cas particulier de matrice de Cauchy avec, pour tout $i \in [\![1,n]\!]$, $a_i = b_i = i - \frac{1}{2}\cdot$ Le coefficient d'indice (i,j) de H^{-1} est donc

$$h'_{i,j} = \frac{\prod\limits_{k=1}^{n}(i+k-1)}{\prod\limits_{k\neq i}(k-i)}\,\frac{\prod\limits_{k\neq i}(k+j-1)}{\prod\limits_{k\neq j}(k-j)}.$$

On remarque que

$$\prod_{k=1}^{n}(i+k-1) = \frac{(i+n-1)!}{(i-1)!} \quad \text{et} \quad \prod_{k\neq i}(k-i) = (-1)^{i-1}(i-1)!(n-i)!.$$

On en déduit que

$$h'_{i,j} = (-1)^{i+j}\frac{(i+n-1)!(j+n-1)!}{((i-1)!)^2((j-1)!)^2(n-i)!(n-j)!(i+j-1)}.$$

L'égalité $\dfrac{1}{(i-1)!(j-1)!} = \dfrac{C_{i+j-2}^{i-1}}{(i+j-2)!}$ permet d'écrire

$$\begin{aligned} h'_{i,j} &= (-1)^{i+j}(C_{i+j-2}^{i-1})^2\frac{(i+n-1)!(j+n-1)!}{(n-i)!(n-j)!(i+j-2)!(i+j-1)!} \\ &= (-1)^{i+j}(i+n-1)(C_{i+j-2}^{i-1})^2C_{i+n-2}^{n-j}C_{j+n-1}^{n-i}. \end{aligned}$$

Cela montre que H^{-1} est à coefficients entiers. $\lhd$

5.54. Automorphismes de K(X)

1. Déterminer les automorphismes de la K-algèbre K[X].

2. Déterminer les automorphismes de la K-algèbre K(X) des fractions rationnelles à une indéterminée.

(École polytechnique)

▷ **Solution.**

1. Soit Φ un automorphisme de la K-algèbre K[X]. Notons $P = \Phi(X)$. Alors $\Phi(X^n) = P^n$ pour tout $n \in \mathbb{N}$ et si $Q = \sum_{k\in\mathbb{N}} a_k X^k \in K[X]$,

$$\Phi(Q) = \sum_{k\in\mathbb{N}} a_k \Phi(X^k) = \sum_{k\in\mathbb{N}} a_k P^k = Q \circ P.$$

Pour que Φ soit surjective, il est nécessaire que P ne soit pas constant. Si $Q \neq 0$, $\deg(\Phi(Q)) = \deg P \times \deg Q$. La surjectivité de Φ impose $\deg P = 1$. Il existe donc $(a, b) \in K^* \times K$ tel que $\Phi(Q) = Q(aX + b)$ pour tout $Q \in K[X]$.

Réciproquement, si $(a, b) \in K^* \times K$, $Q \longmapsto Q(aX + b)$ est un automorphisme de la K-algèbre K[X] dont l'automorphisme réciproque est l'application $Q \longmapsto Q\left(\dfrac{X - b}{a}\right)$.

2. • Soit Φ un morphisme d'algèbres de K(X). Posons $F = \Phi(X)$. On démontre alors, comme dans la question 1, que, pour tout $P \in K[X]$, on a $\Phi(P) = P \circ F$. Si $G \in K(X)$ s'écrit $G = \dfrac{P}{Q}$, avec P et Q dans K[X], on obtient

$$\Phi(G) = \Phi\left(\frac{P}{Q}\right) = \frac{\Phi(P)}{\Phi(Q)} = \frac{P \circ F}{Q \circ F} = G \circ F.$$

Il est clair, réciproquement, que pour tout $F \in K(X)$, l'application

$$\Phi_F : G \in K(X) \longmapsto G \circ F \in K(X)$$

est un morphisme de K-algèbre. Reste à trouver à quelle condition sur F l'application Φ_F est un automorphisme.

• Si Φ_F est un automorphisme, il est surjectif et en particulier il existe $G \in K(X)$ tel que $\Phi(G) = G \circ F = X$. Soit A, B, P, Q quatre polynômes tels que $\dfrac{A}{B}$ et $\dfrac{P}{Q}$ soient des représentants irréductibles de F et G. On note p et q les degrés respectifs de P et Q, $a_0, \ldots, a_p$ et $b_0, \ldots, b_q$ les scalaires tels que $P = \sum_{j=0}^{p} a_j X^j$ et $Q = \sum_{k=0}^{q} b_k X^k$. La relation $G \circ F = X$ équivaut à $P \circ F = X(Q \circ F)$, c'est-à-dire à

$$\sum_{j=0}^{p} a_j F^j = X \sum_{k=0}^{q} b_k F^k, \text{ soit } \sum_{j=0}^{p} a_j \frac{A^j}{B^j} = X \sum_{k=0}^{q} b_k \frac{A^k}{B^k}.$$

Si on note $m = \max(p, q)$, on obtient

$$\sum_{j=0}^{p} a_j A^j B^{m-j} = X \sum_{k=0}^{q} b_k A^k B^{m-k}.$$

Tous les polynômes qui interviennent dans cette égalité sont divisibles par A, sauf ceux qui correspondent à $j = 0$ et $k = 0$. On en déduit que A divise $a_0 B^m - b_0 X B^m$. Le polynôme A étant premier avec B et donc avec B^m, on en déduit que A divise $a_0 - b_0 X$. Le couple (a_0, b_0) n'est pas égal à $(0,0)$ sinon $\frac{P}{Q}$ ne serait pas irréductible, donc le polynôme $a_0 - b_0 X$ est de degré $\leqslant 1$. On en déduit que $\deg(A) \leqslant 1$.

Intéressons-nous maintenant aux polynômes divisibles par B dans l'égalité précédente. Si $m = p = q$, B divise $(a_p - b_p X)A^p$ et donc $a_p - b_p X$, puisqu'il est premier avec A^p. Le polynôme $a_p - b_p X$ est de degré 1 car $b_p \neq 0$. On en déduit que $\deg(B) \leqslant 1$. Si $m = q > p$, on montre que B divise $b_q X$ et si $m = p > q$, B divise a_p. Dans tous les cas, la conclusion est la même : $\deg(P) \leqslant 1$.

Nous avons donc démontré qu'il existe $(a, b, c, d) \in K^4$ tel que

$$F = \frac{aX + b}{cX + d}.$$

Il est clair que F ne peut pas être constant ; il faut donc $ad - bc \neq 0$.

• Réciproquement, étant donnés quatre éléments a, b, c, d de K tels que $ad - bc \neq 0$, notons $\Phi_{a,b,c,d}$ le morphisme de K(X) défini par

$$\Phi_{a,b,c,d}(X) = \frac{aX + b}{cX + d}.$$

On montre facilement que $\Phi_{1,0,0,1} = \mathrm{Id}_{K(X)}$ et que si (a, b, c, d) et (a', b', c', d') sont deux quadruplets tels que $ad - bc \neq 0$ et $a'd' - b'c' \neq 0$, alors

$$\Phi_{a,b,c,d} \circ \Phi_{a',b',c',d'} = \Phi_{a'',b'',c'',d''},$$

où a'', b'', c'', d'' sont tels que $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$.

La matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est inversible. Si $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}$, alors

$$\Phi_{a,b,c,d} \circ \Phi_{a',b',c',d'} = \Phi_{a',b',c',d'} \circ \Phi_{a,b,c,d} = \mathrm{Id}_{K(X)}.$$

Le morphisme $\Phi_{a,b,c,d}$ est inversible : c'est un automorphisme de K(X).

Conclusion. Les automorphismes d'algèbre de K(X) sont les applications

$$G \in K(X) \longmapsto G\left(\frac{aX + b}{cX + d}\right) \in K(X),$$

avec $(a, b, c, d) \in K^4$ et $ad - bc \neq 0$. De plus l'application qui à la matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(K)$ associe $\Phi_{a,b,c,d}$ est un morphisme de groupes. Son noyau est le sous-groupe des matrices scalaires non nulles. $\lhd$

Les nombres algébriques sur $\mathbb{Q}$ sont les racines des polynômes à coefficients entiers. On s'intéresse ici à l'approximation des nombres algébriques par des rationnels.

5.55. Approximation d'un irrationnel algébrique par des rationnels

Soit $P \in \mathbb{Z}[X]$ non nul et a une racine irrationnelle de P.

1. Théorème de Liouville : montrer qu'il existe des réels $c > 0$ et $r \geqslant 0$ tels que $\left|a - \frac{p}{q}\right| \geqslant \frac{c}{q^r}$ pour tout couple $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$.

2. Montrer qu'il existe $d > 0$ tel que $\left|a - \frac{p}{q}\right| \leqslant \frac{d}{q^2}$ pour une infinité de couples $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$.

3. Montrer que l'ordre de a comme racine de P est inférieur ou égal à $\frac{n}{2}$ où n est le degré de P.

(École normale supérieure)

▷ **Solution.**

1. On décompose P en produit de facteurs irréductibles dans $\mathbb{Q}[X]$ et on considère $Q \in \mathbb{Q}[X]$ irréductible, divisant P et tel que $Q(a) = 0$. On note $r \geqslant 2$ le degré de Q. Soit $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. Comme $a \neq \frac{p}{q}$, en vertu du théorème des accroissements finis, il existe $d \in \left]\frac{p}{q}, a\right[$ tel que

$$Q\left(\frac{p}{q}\right) = Q\left(\frac{p}{q}\right) - Q(a) = Q'(d)\left(\frac{p}{q} - a\right).$$

En passant à la valeur absolue, on obtient $\left|Q\left(\frac{p}{q}\right)\right| = |Q'(d)|\left|a - \frac{p}{q}\right|$. Il existe $A \in \mathbb{Z}^*$ tel que $AQ \in \mathbb{Z}[X]$. Il s'ensuit que $Aq^rQ\left(\frac{p}{q}\right)$ est dans $\mathbb{Z}$ et même dans $\mathbb{Z}^*$, puisque Q n'a pas de racine rationnelle (en effet, il est irréductible sur $\mathbb{Q}$ et n'est pas de degré 1 puisque $a \notin \mathbb{Q}$ est racine). Par conséquent, on a $\left|Aq^rQ\left(\frac{p}{q}\right)\right| \geqslant 1$ et

$$|Q'(d)|\left|a - \frac{p}{q}\right| = \frac{1}{Aq^r}\left|Aq^rQ\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{Aq^r}.$$

Cherchons à majorer $|Q'(d)|$: la fonction Q' est continue sur $[a-1, a+1]$, donc il existe $K > 0$ tel que, si $x \in [a-1, a+1]$, $|Q'(x)| \leqslant K$. Ainsi on a, si $\frac{p}{q} \in [a-1, a+1]$,

$$K\left|a - \frac{p}{q}\right| \geqslant \frac{1}{Aq^r} \quad \text{et} \quad \left|a - \frac{p}{q}\right| \geqslant \frac{c}{q^r}$$

en ayant posé $c = \dfrac{1}{\mathrm{KA}} > 0$. Quitte à changer c en 1 si $c > 1$, on peut supposer $c \leqslant 1$. L'inégalité $\left|a - \dfrac{p}{q}\right| \geqslant \dfrac{c}{q^r}$ reste alors vraie si $\left|a - \dfrac{p}{q}\right| > 1$.

Conclusion. On a trouvé $r \geqslant 2$ et $c > 0$ tel que si $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$,

$$\boxed{\left|a - \frac{p}{q}\right| \geqslant \frac{c}{q^r}}.$$

2. Nous allons démontrer la propriété demandée avec $d = 1$.

• Montrons pour commencer le résultat suivant : étant donné N dans N^*, il existe $(p, q) \in \mathbb{Z}^2$ tel que $|qa - p| < \dfrac{1}{\mathrm{N}}$ et $0 < q \leqslant \mathrm{N}$. Pour cela, nous appliquons la méthode des tiroirs de Dirichlet. Considérons les $\mathrm{N} + 1$ nombres réels $a_k = ka - \mathrm{E}(ka)$ $(0 \leqslant k \leqslant \mathrm{N})$. Ils appartiennent à l'intervalle $[0, 1[$. Celui-ci est réunion des N «tiroirs» $\left[\dfrac{i}{\mathrm{N}}, \dfrac{i+1}{\mathrm{N}}\right[$, pour $0 \leqslant i \leqslant \mathrm{N} - 1$. Un de ces tiroirs doit contenir deux réels a_k. Il existe donc des entiers k_1 et k_2 tels que $0 \leqslant k_1 < k_2 \leqslant \mathrm{N}$ et $|a_{k_2} - a_{k_1}| < \dfrac{1}{\mathrm{N}}$. En posant $q = k_2 - k_1$ et $p = \mathrm{E}(k_2 a) - \mathrm{E}(k_1 a)$, on obtient $0 < q \leqslant \mathrm{N}$ et $|aq - p| < \dfrac{1}{\mathrm{N}}$.

• De ce résultat on déduit, en prenant un entier N strictement positif quelconque, que $\left|a - \dfrac{p}{q}\right| < \dfrac{1}{q\mathrm{N}} \leqslant \dfrac{1}{q^2}$, ce qui montre l'existence d'un couple (p, q) vérifiant l'inégalité voulue. Pour montrer qu'il en existe une infinité, on raisonne par l'absurde et on suppose qu'il n'en existe qu'un nombre fini $\dfrac{p_1}{q_1}, \ldots, \dfrac{p_m}{q_m}$. Puisque a est irrationnel, il existe un entier N strictement positif tel que, pour $1 \leqslant i \leqslant m$, on ait $\left|a - \dfrac{p_i}{q_i}\right| > \dfrac{1}{\mathrm{N}}$. Mais, d'après ce qui précède, il existe $(p, q) \in \mathbb{Z}^2$ tel que $|qa - p| < \dfrac{1}{\mathrm{N}}$ et $0 < q \leqslant \mathrm{N}$. On a alors $\left|a - \dfrac{p}{q}\right| \leqslant \dfrac{1}{q^2}$, mais aussi $\left|a - \dfrac{p}{q}\right| < \dfrac{1}{q\mathrm{N}} \leqslant \dfrac{1}{\mathrm{N}}$, ce qui montre que $\dfrac{p}{q}$ n'est pas un des $\dfrac{p_i}{q_i}$. D'où la contradiction cherchée.

3. Appelons d l'ordre de a comme racine de P et démontrons que $d \leqslant \dfrac{n}{2}$, par récurrence sur d. Considérons à nouveau $\mathrm{Q} \in \mathbb{Q}[\mathrm{X}]$, facteur irréductible de P, admettant a comme racine. Comme $a \notin \mathbb{Q}$, on a $\deg \mathrm{Q} = r \geqslant 2$.

• Si $d = 1$, alors $2 \leqslant \deg \mathrm{Q} \leqslant \deg \mathrm{P}$ et $n \geqslant 2d$.

• Supposons $d \geqslant 2$. Montrons que a est racine simple de Q. En effet, l'ensemble $\mathrm{I} = \{\mathrm{A} \in \mathrm{K}[\mathrm{X}], \mathrm{A}(a) = 0\}$ est un idéal de $\mathbb{Q}[\mathrm{X}]$. Il est donc principal et admet un générateur unitaire A non constant. Or $\mathrm{Q} \in \mathrm{I}$ donc A divise Q et $\mathrm{Q} \in \mathbb{Q}^*\mathrm{A}$, puisque Q est irréductible. Si a était une

racine double de Q, on aurait $Q'(a) = 0$ et $Q' \in I$. Alors Q diviserait Q', ce qui est exclu car $Q' \neq 0$ et $\deg Q' < \deg Q$.

Ainsi, a est une racine d'ordre $d-1$ du polynôme $P_1 = \dfrac{P}{Q}$. On a, par hypothèse de récurrence, $n - \deg Q = \deg P_1 \geqslant 2(d-1)$, d'où l'on déduit $n \geqslant 2(d-1) + \deg Q \geqslant 2d$. ◁

Le théorème démontré dans la première question de l'exercice permit à Liouville de donner les premiers exemples de nombres transcendants, c'est-à-dire non algébriques (en 1844). Supposons que a soit un réel irrationnel tel que, pour tout $k \in \mathbb{N}^*$, il existe $(p,q) \in \mathbb{Z} \times \mathbb{N}^*$, $q \geqslant 2$ tel que $\left|a - \dfrac{p}{q}\right| < \dfrac{1}{q^k}$. Alors, il ne peut exister c et r comme dans la question 1 de l'exercice. En effet, en prenant k assez grand, on arrive à une contradiction puisque $q \geqslant 2$. On montre ainsi que $a = \sum_{i=0}^{+\infty} \dfrac{1}{10^{i!}}$ est transcendant.

En 1863, Cantor, après avoir démontré que $\mathbb{R}$ n'est pas dénombrable, prouva l'existence d'une infinité de nombres transcendants en remarquant que l'ensemble des nombres algébriques est dénombrable. L'exercice suivant prouve la transcendance de e, résultat établi par Hermite en 1873.

5.56. Transcendance de e

1. Soit $P \in \mathbb{R}[X]$ et, pour $t \in \mathbb{R}$, $I(t) = \int_0^t e^{t-u}P(u)\,du$. Montrer que, si $\deg(P) = q$, $I(t) = e^t \sum_{i=0}^{q} P^{(i)}(0) - \sum_{i=0}^{q} P^{(i)}(t)$.

2. Supposons donnés des entiers relatifs $a_0, a_1, \ldots, a_n$ tels que $a_0 \neq 0$ et $a_0 + a_1 e + \cdots + a_n e^n = 0$. Soit $p \in \mathbb{N}$; on pose

$$P = X^{p-1}(X-1)^p(X-2)^p \cdots (X-n)^p$$

et

$$J = a_0 I(0) + a_1 I(1) + \cdots + a_n I(n).$$

Montrer que J est un entier. Montrer que $(p-1)!$ divise J et enfin que, pour tout entier premier p assez grand, $J \neq 0$.

3. Montrer qu'il existe $C \in \mathbb{R}$ tel que, pour tout $p \in \mathbb{N}$, $|J| \leqslant C^p$ et trouver une minoration de $|J|$. En déduire que e est transcendant.

(**École polytechnique**)

▷ **Solution.**

1. On définit $D(P) = \sum_{i=0}^{q} P^{(i)}$ et la fonction f par $f(u) = e^{-u}D(P)(u)$. On note que $D(P)' = D(P) - P$, car $P^{(q+1)} = 0$; on en déduit que, pour tout $u \in \mathbb{R}$, on a

$$f'(u) = -e^{-u}\mathrm{D(P)}(u) + e^{-u}\mathrm{D(P)}'(u) = -e^{-u}\mathrm{P}(u).$$

On obtient alors

$$\mathrm{I}(t) = e^t \int_0^t e^{-u}\mathrm{P}(u)\mathrm{d}u = e^t \left[-e^{-u}\mathrm{D(P)}(u)\right]_0^t = e^t\mathrm{D(P)}(0) - \mathrm{D(P)}(t),$$

c'est-à-dire

$$\mathrm{I}(t) = e^t \sum_{i=0}^{q} \mathrm{P}^{(i)}(0) - \sum_{i=0}^{q} \mathrm{P}^{(i)}(t).$$

2. • Avec les notations précédentes, on a, pour tout entier $k \in \mathbb{N}$,

$$\mathrm{I}(k) = e^k\mathrm{D(P)}(0) - \mathrm{D(P)}(k).$$

On en déduit que

$$\mathrm{J} = \left(\sum_{k=0}^{n} a_k e^k\right)\mathrm{D(P)}(0) - \sum_{k=0}^{n} a_k\mathrm{D(P)}(k) = -\sum_{k=0}^{n} a_k\mathrm{D(P)}(k).$$

Le polynôme P est à coefficients entiers, donc D(P) également ; les a_k étant entiers, on en déduit que J est un entier.

• Montrons, que pour $k \in [\![0, n]\!]$, $\mathrm{D(P)}(k)$ est divisible par $(p-1)!$. Le polynôme P s'écrit $\mathrm{X}^{p-1}\mathrm{Q}$, avec $\mathrm{Q} \in \mathbb{Z}[\mathrm{X}]$. Pour $i \in \mathbb{N}$, on calcule $\mathrm{P}^{(i)}$ par la formule de Leibniz. Les termes qui apportent une contribution non nulle à $\mathrm{P}^{(i)}(0)$ sont ceux pour lesquels on aura dérivé $p-1$ fois X^{p-1}. La dérivée $(p-1)$-ième de X^{p-1} étant $(p-1)!$, on en déduit que, pour tout entier i, $\mathrm{P}^{(i)}(0)$ est divisible par $(p-1)!$. Il en est donc de même de $\mathrm{D(P)}(0)$.

Pour $1 \leqslant k \leqslant n$, en écrivant $\mathrm{P} = (\mathrm{X}-k)^p\mathrm{R}$, avec $\mathrm{R} \in \mathbb{Z}[\mathrm{X}]$, on montre de la même manière que $\mathrm{D(P)}(k)$ est divisible par $p!$ et a fortiori par $(p-1)!$.

Finalement, chaque $\mathrm{D(P)}(k)$ étant divisible par $(p-1)!$, on conclut que J est divisible par $(p-1)!$.

• Montons que, si p est un nombre premier assez grand, J n'est pas divisible par $p!$. Avec les notations précédentes, on a, pour $i \geqslant 1$, $\mathrm{Q}^{(i)}(0)$ divisible par p, car il existe $\mathrm{Q}_1 \in \mathbb{Z}[\mathrm{X}]$ tel que $\mathrm{Q} = \mathrm{Q}_1^p$. On en déduit que, si $i \geqslant p$, alors $\mathrm{P}^{(i)}(0)$ est divisible par $p!$. Comme

$$\mathrm{P}^{(p-1)}(0) = (p-1)!\mathrm{Q}(0) = (p-1)!(-1)^{pn}\,(n!)^p\,,$$

il en résulte que

$$\mathrm{D(P)}(0) \equiv (p-1)!(-1)^{pn}\,(n!)^p \pmod{p!},$$

puis que

$$\mathrm{J} \equiv -a_0(p-1)!(-1)^{pn}\,(n!)^p \pmod{p!}.$$

Par hypothèse, a_0 est non nul. Si p est un entier premier supérieur à $|a_0|$ et à n, p ne divise ni a_0, ni $n!$ et donc $p!$ ne divise pas J. On en déduit qu'alors J n'est pas nul.

3. Pour majorer J, on majore $\mathrm{I}(k)$, pour $0 \leqslant k \leqslant n$, en revenant à l'expression initiale de $\mathrm{I}(t)$. On a, pour $k \in [\![0, n]\!]$,

$$|\mathrm{I}(k)| = \left| \int_0^k e^{t-u} \mathrm{P}(u) \mathrm{d}u \right| \leqslant \sup_{[0,k]} |\mathrm{P}| \int_0^k e^{k-u} \mathrm{d}u = (e^k - 1) \sup_{[0,k]} |\mathrm{P}|$$
$$\leqslant e^n \sup_{[0,n]} |\mathrm{P}|.$$

Or, pour tout $x \in [0, n]$, on a

$$|\mathrm{P}(x)| = x^{p-1} \left(|x-1||x-2| \cdots |x-n|\right)^p \leqslant n^{p-1} \left(n^n\right)^p.$$

On en déduit que, pour tout $k \in [\![0, n]\!]$,

$$|\mathrm{I}(k)| \leqslant e^n n^{p-1} \left(n^n\right)^p,$$

puis que, pour tout entier $p \in \mathbb{N}$,

$$|\mathrm{J}| \leqslant \sum_{k=0}^{n} |a_k| e^n n^{p-1} \left(n^n\right)^p.$$

Soit $a = \max\left(\sum_{k=0}^{n} |a_k| e^n, n\right)$. On a alors, pour tout $p \in \mathbb{N}$,

$$|\mathrm{J}| \leqslant a^p \left(n^n\right)^p \leqslant \left(a n^n\right)^p \quad \text{c'est-à-dire } |\mathrm{J}| \leqslant \mathrm{C}^p,$$

avec $\mathrm{C} = a n^n$.

Mais nous avons vu dans la question précédente que, si p est un entier premier assez grand, alors J est non nul et divisible par $(p-1)!$. On en déduit que $|\mathrm{J}| \geqslant (p-1)!$ et a fortiori, $\mathrm{C}^p \geqslant (p-1)!$. Or on a $\lim_{p \to +\infty} \dfrac{\mathrm{C}^p}{(p-1)!} = 0$. Pour p assez grand, on a donc $\mathrm{C}^p < (p-1)!$. D'où la contradiction cherchée. Il ne peut pas exister des entiers $a_0, a_1, \ldots, a_n$ appartenant à $\mathbb{Z}$ tels que $a_0 \neq 0$ et $a_0 + a_1 e + \cdots + a_n e^n = 0$.

On en déduit que e est transcendant. En effet, si e est algébrique sur $\mathbb{Q}$, il existe $\mathrm{P} \in \mathbb{Q}[\mathrm{X}]$, tel que $\mathrm{P}(e) = 0$. En multipliant P par un entier, on peut supposer que $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$. Il existe donc des entiers $a_0, a_1, \ldots, a_n$ appartenant à $\mathbb{Z}$ tels que $a_0 + a_1 e + \cdots + a_n e^n = 0$. On peut supposer que $a_0 \neq 0$, car si l'ordre de 0 comme racine de P est p, on divise P par X^p.

Les derniers exercices du chapitre traitent des polynômes à plusieurs variables. Le premier est une généralisation du résultat de l'exercice 5.24 aux polynômes à plusieurs variables.

5.57. Polynômes à plusieurs variables à valeurs entières

1. Soit $P \in \mathbb{R}[X]$ avec $\deg P \leqslant n$. Montrer que $P(\mathbb{Z}) \subset \mathbb{Z}$ si et seulement si $P(0), P(1), \ldots, P(n)$ sont dans $\mathbb{Z}$.

2. Soit $Q(X_1, \ldots, X_\ell)$ un polynôme à ℓ variables à coefficients dans $\mathbb{R}$. Donner une condition nécessaire et suffisante pour que l'on ait $P(\mathbb{Z}^\ell) \subset \mathbb{Z}$.

3. Montrer que pour tout $(m_1, \ldots, m_\ell) \in \mathbb{Z}^\ell$, $\prod_{k=1}^{\ell-1} k!$ divise $\prod_{1 \leqslant i < j \leqslant \ell} (m_j - m_i)$.

(École normale supérieure)

▷ **Solution.**

1. Il est clair que si $P(\mathbb{Z}) \subset \mathbb{Z}$, alors $P(0), \ldots, P(n)$ sont dans $\mathbb{Z}$. Pour démontrer la réciproque, nous raisonnerons par récurrence sur n.

• Si $n = 0$, le polynôme P est constant et cette constante est entière, puisque $P(0) \in \mathbb{Z}$.

• Supposons la propriété établie pour les polynômes de degré $\leqslant n-1$. Soit P un polynôme de degré $\leqslant n$ tel que $P(0), P(1), \ldots, P(n)$ soient dans $\mathbb{Z}$. Considérons le polynôme $Q = P(X+1) - P(X)$. Il est de degré $\leqslant n-1$ et, pour $0 \leqslant k \leqslant n-1$, on a $Q(k) = P(k+1) - P(k) \in \mathbb{Z}$. On en déduit que $Q(\mathbb{Z}) \subset \mathbb{Z}$. On remarque que, pour tout $k \in \mathbb{N}$, on a $P(k+1) = P(k) + Q(k)$ et $P(-k-1) = P(-k) - Q(-k-1)$. Sachant que $P(0) \in \mathbb{Z}$, une récurrence banale sur k permet de conclure que, pour tout $k \in \mathbb{N}$, $P(k)$ et $P(-k)$ sont dans $\mathbb{Z}$. On conclut $P(\mathbb{Z}) \subset \mathbb{Z}$, ce qui achève la démonstration[7].

2. Montrons que si $Q \in \mathbb{R}[X_1, \ldots, X_\ell]$ et si le degré de Q en chacune des variables est inférieur ou égal à n, alors $Q(\mathbb{Z}^\ell) \subset \mathbb{Z}$ si et seulement si on a, pour tout $(x_1, \ldots, x_\ell) \in [\![0, n]\!]^\ell$, $Q(x_1, \ldots, x_\ell) \in \mathbb{Z}$. Là encore une des deux implications est évidente. On démontre que si on a, pour tout $(x_1, \ldots, x_\ell) \in [\![0, n]\!]^\ell$, $Q(x_1, \ldots, x_\ell) \in \mathbb{Z}$, alors $Q(\mathbb{Z}^\ell) \subset \mathbb{Z}$, en raisonnant par récurrence sur $\ell \in \mathbb{N}^*$

• Le cas $\ell = 1$ a été traité dans la question précédente.

• Supposons la propriété vérifiée au rang $\ell - 1 \geqslant 1$ et considérons un polynôme Q de ℓ variables et de degré $\leqslant n$ par rapport à chaque variable, tel que $Q(x_1, \ldots, x_\ell) \in \mathbb{Z}$ pour tout $(x_1, \ldots, x_\ell) \in [\![0, n]\!]^\ell$. Fixons x_ℓ dans $[\![0, n]\!]$ et considérons le polynôme $Q_1 \in \mathbb{R}[X_1, \ldots, X_{\ell-1}]$ défini par

$$Q_1(X_1, \ldots, X_{\ell-1}) = Q(X_1, \ldots, X_{\ell-1}, x_\ell).$$

Le polynôme Q_1 est de degré $\leqslant n$ par rapport à $X_1, \ldots, X_{\ell-1}$ et vérifie,

7. On a donné ici une preuve différente de celle que le lecteur trouvera dans l'exercice 5.24.

par hypothèse, pour tout $(x_1, \ldots, x_{\ell-1}) \in [\![0, n]\!]^{\ell-1}$,

$$Q_1(x_1, \ldots, x_{\ell-1}) = Q(x_1, \ldots, x_{\ell-1}, x_\ell) \in \mathbb{Z}.$$

De l'hypothèse de récurrence, on déduit que $Q_1(\mathbb{Z}^{\ell-1}) \subset \mathbb{Z}$. On a donc, pour tout $(x_1, \ldots, x_{\ell-1}) \in \mathbb{Z}^{\ell-1}$, $Q(x_1, \ldots, x_{\ell-1}, x_\ell) = Q_1(x_1, \ldots, x_{\ell-1})$ dans $\mathbb{Z}$, ceci pour tout $x_\ell \in [\![0, n]\!]$.

Fixons maintenant $(x_1, \ldots, x_{\ell-1})$, élément quelconque de $\mathbb{Z}^{\ell-1}$ et considérons le polynôme $Q_2 \in \mathbb{R}[X_\ell]$ défini par

$$Q_2 = Q(x_1, \ldots, x_{\ell-1}, X_\ell).$$

On a $\deg Q_2 \leqslant n$ et, d'après ce qui précède, $Q_2(x_\ell) \in \mathbb{Z}$ pour tout $x_\ell \in [\![0, n]\!]$. On en déduit que $Q(x_1, \ldots, x_{\ell-1}, x_\ell) = Q_2(x_\ell) \in \mathbb{Z}$, pour tout $x_\ell \in \mathbb{Z}$, d'après la question 1. Cela montre que $Q(\mathbb{Z}^\ell) \subset \mathbb{Z}$ et termine la démonstration par récurrence.

3. Considérons le polynôme $Q \in \mathbb{R}[X_1, \ldots, X_\ell]$ défini par

$$Q = \prod_{1 \leqslant i < j \leqslant \ell} \frac{X_j - X_i}{j - i}.$$

Montrons que $Q(\mathbb{Z}^\ell) \subset \mathbb{Z}$. Puisque Q est de degré $\ell - 1$ par rapport à chacune des variables, il suffit de vérifier, d'après la question 2 que $Q(x_1, \ldots, x_\ell) \in \mathbb{Z}$ pour tout $(x_1, \ldots, x_\ell) \in [\![0, \ell - 1]\!]^\ell$.

S'il existe deux indices distincts i et j tels que $x_i = x_j$, alors on a $Q(x_1, \ldots, x_\ell) = 0 \in \mathbb{Z}$. Sinon, on obtient $\{x_1, \ldots, x_\ell\} = \{0, 1, \ldots, \ell - 1\}$ et donc $\{x_1 + 1, \ldots, x_\ell + 1\} = \{1, 2, \ldots, \ell\}$. Il existe $\sigma \in \mathcal{S}_n$ tel que, pour tout $i \in [\![1, \ell]\!]$, $x_i + 1 = \sigma(i)$. On en déduit que

$$Q(x_1, \ldots, x_\ell) = \prod_{1 \leqslant i < j \leqslant \ell} \frac{\sigma(j) - \sigma(j)}{j - i} = \varepsilon(\sigma) \in \mathbb{Z}.$$

Calculons maintenant $N = \prod_{1 \leqslant i < j \leqslant \ell} (j - i)$. On obtient

$$N = \prod_{j=2}^{\ell} \left(\prod_{i=1}^{j-1} (j - i) \right) = \prod_{j=2}^{\ell} (j - 1)! = \prod_{j=1}^{\ell-1} j!.$$

D'après ce qui précède, on a pour tout $(m_1, \ldots, m_\ell) \in \mathbb{Z}^\ell$,

$$Q(m_1, \ldots, m_\ell) = \frac{\prod_{1 \leqslant i < j \leqslant \ell} (m_j - m_i)}{N} \in \mathbb{Z}.$$

Autrement dit, $N = \prod_{j=1}^{\ell-1} j!$ divise $\prod_{1 \leqslant i < j < \ell} (m_j - m_i)$. $\lhd$

Le lecteur trouvera dans l'exercice 1.8 du tome 2 d'algèbre une autre solution de cette dernière question, utilisant le déterminant de Vandermonde.

5.58. Applications de $\mathbb{R}^2$ dans $\mathbb{R}$ polynomiales par rapport à chaque variable

1. Soit $f : \mathbb{R}^2 \to \mathbb{R}$ telle que $y \mapsto f(x,y)$ est polynomiale pour tout $x \in \mathbb{R}$ et $x \mapsto f(x,y)$ est polynomiale pour tout $y \in \mathbb{R}$. Montrer que f est polynomiale.

2. Que se passe-t-il si on remplace le corps $\mathbb{R}$ par $\mathbb{Q}$?

(**École normale supérieure**)

▷ **Solution.**

1. Si f est polynomiale de degré n par rapport à y, pour tout $x \in \mathbb{R}$, l'application polynomiale $y \longmapsto f(x,y)$ est de degré inférieur ou égal à n. Cela incite à considérer, pour tout $d \in \mathbb{N}$, l'ensemble E_d des x pour lesquels l'application polynomiale $y \longmapsto f(x,y)$ est de degré $\leqslant d$. Comme $\mathbb{R} = \bigcup_{n\in\mathbb{N}} \mathrm{E}_d$, l'un des ensembles E_d est infini (sinon $\mathbb{R}$ serait dénombrable). Notons-le E_n. Pour tout $x \in \mathrm{E}_n$, l'application polynomiale $y \longmapsto f(x,y)$, qui est degré inférieure ou égale à n, est déterminée par les valeurs en $n+1$ points, disons $0, 1, \ldots, n$. En notant L_i $(0 \leqslant i \leqslant n)$ les polynômes interpolateurs élémentaires en ces $n+1$ valeurs, on obtient, pour $x \in \mathrm{E}_n$ et $y \in \mathbb{R}$,

$$f(x,y) = \sum_{i=0}^{n} f(x,i)\mathrm{L}_i(y).$$

Pour tout $i \in [\![0,n]\!]$, l'application $x \longmapsto f(x,i)$ est polynomiale. Ainsi l'application $g : (x,y) \longmapsto \sum_{i=0}^{n} f(x,i)\mathrm{L}_i(y)$ est polynomiale.

Soit $y \in \mathbb{R}$. L'application $x \longmapsto f(x,y)$ est polynomiale et pour tout $x \in \mathrm{E}_n$, $f(x,y) = g(x,y)$. Les applications polynomiales

$$x \longmapsto f(x,y) \quad \text{et} \quad x \longmapsto g(x,y)$$

qui coïncident pour une infinité de valeurs sont égales. On a donc, pour tout $(x,y) \in \mathbb{R}^2$, $f(x,y) = g(x,y)$ et $f = g$.

2. Si le corps de base est $\mathbb{Q}$ et plus généralement tout corps dénombrable, il est possible qu'aucun des ensembles E_d ne soit infini et la démonstration précédente tombe en défaut. Construisons un contre-exemple.

Le degré des applications $y \longmapsto f(x,y)$ ne doit pas être borné quand x décrit $\mathbb{Q}$; il en est de même des applications $y \longmapsto f(x,y)$. Ainsi f doit être une somme infinie de termes polynomiaux qui pour x ou y fixé sont presque tous nuls. Notons (r_i) une énumération de $\mathbb{Q}$ et pour tout

entier naturel i, L_i le polynôme interpolateur de degré i qui vaut 1 en r_i et 0 en $r_0, \ldots, r_{i-1}$. Posons, pour tout $(x, y) \in \mathbb{Q}^2$,

$$f(x, y) = \sum_{i=0}^{+\infty} L_i(x) L_i(y).$$

On note que $L_i(r_k) = 0$ si $k < i$. Ainsi la somme ne contient jamais qu'un nombre fini de termes et, pour tout $k \in \mathbb{N}$, $f(r_k, x) = \sum_{i=0}^{k} L_i(r_k) L_i(x)$. L'application $y \longmapsto f(x, y)$ est donc polynomiale pour tout $x \in \mathbb{Q}$. Il en est de même de l'application $x \longmapsto f(x, y)$ pour tout $y \in \mathbb{Q}$.

Mais f n'est pas polynomiale car pour tout $k \in \mathbb{N}$, $y \longmapsto f(r_k, x)$ est de degré k, donc l'ensemble des degrés des applications $y \longmapsto f(r_k, x)$ n'est pas borné. $\lhd$

La démonstration du théorème de Bezout qui suit illustre les grandes différences entre l'arithmétique de $K[X]$ *et celle de* $K[X_1, \ldots, X_n]$ *pour* $n \geqslant 2$. *Ce dernier n'est pas un anneau principal (d'après l'exercice 3.9) ; l'identité de Bezout ne s'y applique pas : par exemple* X *et* Y *sont premiers entre eux, mais l'identité* $AX + BY = 1$ *n'est pas possible pour* $(A, B) \in K[X, Y]^2$. *Néanmoins, c'est un anneau intègre ; c'est même un anneau factoriel, c'est-à-dire que tout polynôme peut s'écrire comme produit de polynômes irréductibles (voir 3.10 pour la définition précise).*

5.59. Un théorème de Bezout

Soit P et Q deux polynômes de $K[X, Y]$, premiers entre eux.

1. Montrer qu'il existe $(A, B) \in K[X, Y]$ et $\Delta \in K[X]$, non nul, tels que $\Delta = AP + BQ$.

2. Montrer que l'ensemble des couples $(x, y) \in K^2$ solutions de $P(x, y) = Q(x, y) = 0$ est fini.

(**École normale supérieure**)

$\rhd$ **Solution.**

1. • On souhaiterait appliquer le théorème de Bezout à P et Q, mais comme cela est dit dans le préambule, on ne peut pas le faire directement. On va donc se placer sur un anneau où le théorème de Bezout s'applique. On peut voir P et Q comme des polynômes en Y à coefficients dans $K[X]$. Comme $K[X]$ est contenu dans le corps commutatif $L = K(X)$, P et Q se révèlent être des éléments de $L[Y]$, domaine sur lequel s'applique le théorème de Bezout.

• P et Q sont premiers entre eux dans $K[X, Y]$. Montons qu'ils restent premiers entre eux dans $L(Y)$. Raisonnons par l'absurde et supposons qu'un irréductible D de $L(Y)$ divise à la fois P et Q dans $L(Y)$. Le polynôme D s'écrit

$$D = a_n(X)Y^n + a_{n-1}(X)Y^{n-1} + \cdots + a_1(X)Y + a_0(X),$$

avec $n \geqslant 1$ et les $a_i(X) \in K(X)$. Quitte à multiplier D par le produit des dénominateurs des fractions rationnelles $a_i(X)$ (ce produit est un élément de L non nul), on peut supposer que les $a_i(X)$ sont dans $K[X]$ et $D \in K[X, Y]$.

Résumons : $D \in K[X, Y]$ divise P et Q dans $L[Y] = K(X)[Y]$. Il existe donc F_1 et F_2 dans $L[Y]$ tels que $F_1D = P$ et $F_2D = Q$. Pour arriver à une contradiction, il suffit de montrer que F_1 et F_2 sont en fait dans $K[X][Y] = K[X, Y]$.

Pour cela, donnons quelques définitions (ce sont les mêmes que dans $\mathbb{Z}[X]$: on pourra se reporter à l'exercice 5.16 sur le critère d'Eisenstein). Pour tout $M \in K[X][Y]$ qui s'écrit $\alpha_p(X)Y^p + \cdots + \alpha_1(X)Y + \alpha_0(X)$ (avec $p \geqslant 0$ et les $\alpha_i(X)$ dans $K[X]$), on appelle *contenu* de M et on note $c_X(M)$ le pgcd des $\alpha_i(X)$ pour i variant de 0 à p. On dit qu'un polynôme M est *primitif* si $c_X(M) = 1$. En divisant tous les coefficients de M par leur pgcd, on trouve un polynôme primitif : ainsi M s'écrit $M = c_X(M)\tilde{M}$ avec $\tilde{M} \in K[X][Y]$ primitif.

Nous allons nous appuyer sur le lemme suivant.

Lemme. (Lemme de Gauss) *Soit* P *et* Q *dans* $K[X][Y]$.

(*i*) *Si* P *et* Q *sont primitifs, leur produit* PQ *l'est aussi.*

(*ii*) *On a* $c_X(PQ) = c_X(P) \times c_X(Q)$.

Démonstration.

(*i*) Supposons P et Q primitifs. Raisonnons par l'absurde et imaginons que PQ ne le soit pas. On écrit $P = \sum_{k=0}^{n} a_k(X)Y^k$, $Q = \sum_{k=0}^{m} b_k(X)Y^k$ et $PQ = \sum_{k=0}^{m+n} c_k(X)Y^k$. Puisque PQ n'est pas primitif, il existe $R \in K[X]$, irréductible, divisant tous les $c_k(X)$. Comme P et Q sont primitifs, il existe un plus petit entier k (resp. ℓ) tels que R ne divise pas $a_k(X)$ (resp. $b_\ell(X)$). Considérons alors

$$c_{k+\ell}(X) = a_0b_{k+\ell} + \cdots + a_{k-1}b_{\ell+1} + a_kb_\ell + a_{k+1}b_{\ell-1} + \cdots + a_{k+\ell}b_0.$$

Par définition de k, les k premiers termes sont divisibles par R puisque R divise a_i si $i < k$. De même, par définition de ℓ, les ℓ derniers termes sont divisibles par R. Comme $c_{k+\ell}$ est également divisible par R, il

s'ensuit que R divise le terme restant $a_k b_\ell$. Or, cela est impossible, en vertu du lemme d'Euclide, puisque ni a_k, ni b_ℓ ne sont divisibles par l'irréductible R.

On conclut donc que PQ est primitif.

(*ii*) On écrit $P = c_X(P)\widetilde{P}$, $Q = c_X(Q)\widetilde{Q}$. On a $PQ = c_X(P)c_X(Q)\widetilde{P}\widetilde{Q}$. D'après le 1, $\widetilde{P}\widetilde{Q}$ est primitif et donc le contenu de PQ est $c_X(P)c_X(Q)$. D'où l'égalité voulue. ◇

Comme $\widetilde{D}$ est également irréductible et divise P et Q dans L(Y), quitte à remplacer D par $\widetilde{D}$, on peut supposer D primitif. On peut multiplier $F_1 \in K(X)[Y]$ par un polynôme $R(X) \in K[X]$ afin de chasser les dénominateurs des coefficients de F_1 : $F_1 = \dfrac{F}{R(X)}$ et $F \in K[X][Y]$. On écrit ensuite $F = c_X(F)\widetilde{F}$ avec $\widetilde{F}$ primitif. Par conséquent, on obtient

$$D\frac{c_X(F)\widetilde{F}}{R(X)} = P \quad \text{ou encore} \quad Dc_X(F)\widetilde{F} = R(X)P.$$

Passons aux contenus : $c_X(F) = c_X(D)c_X(F) = c_X(Dc_X(F)\widetilde{F}) = Rc_X(P)$. Donc R divise $c_X(F)$ et finalement $F_1 = \dfrac{c_X(F)}{R}\widetilde{F} \in K[X][Y]$. Autrement dit, D divise P dans $K[X, Y]$. Il en est de même pour Q, par symétrie du problème. Comme P et Q sont premiers entre eux dans $K[X, Y]$, nous aboutissons à une contradiction.

• Nous avons donc démontré que P et Q sont premiers entre eux dans $K(X)[Y]$. Il existe A' et B' dans $K(X)[Y]$ tels que $1 = A'P + B'Q$. Soit $\Delta \in K[X]$ le produit des dénominateurs des coefficients de A et de B. On a alors

$$\Delta = AP + BQ \quad \text{avec} \quad A = \Delta A' \in K[X, Y] \text{ et } B = \Delta B' \in K[X, Y].$$

2. Soit maintenant $(x, y) \in K^2$ tel que $P(x, y) = Q(x, y) = 0$. En substituant dans l'égalité ci-dessus, il vient $\Delta(x) = 0$. Donc x est une racine de Δ. Il ne peut prendre qu'un nombre fini de valeurs puisque Δ est non nul. Par symétrie du problème en X et Y, y lui aussi ne peut prendre qu'un nombre fini de valeurs. Il en résulte que

$$V = \{(x, y) \in K^2,\ P(x, y) = Q(x, y) = 0\} \quad \text{est fini.}$$

Conclusion. Ce résultat s'interprète ainsi : l'intersection de deux courbes algébriques planes $P(x, y) = 0$ et $Q(x, y) = 0$ est finie si P et Q sont des polynômes de $K[X, Y]$ premiers entre eux. ◁

Bezout a en fait montré que si P *et* Q *sont de degrés respectifs* m *et* n, *le nombre de points d'intersection des deux courbes, comptés avec leur ordre de multiplicité d'intersection et en tenant compte des points à l'infini, est exactement* mn *lorsque* K *est algébriquement clos.*

Chapitre 6

Espaces vectoriels. Algèbres

Au XVIIIe *siècle se développent la résolution des systèmes linéaires et la théorie des déterminants. Les raisonnements suggèrent rapidement le concept d'espace à n dimensions. Mais il fallait oser un langage géométrique, alors qu'une interprétation sensible dans le plan ou l'espace faisait défaut pour $n > 3$.*

De manière indépendante, Cayley en Angleterre et Grassman en Allemagne franchissent le pas vers 1843-1845 et parlent d'espace à n dimensions. Le point de vue de Cayley est issu directement de la géométrie analytique : un vecteur d'un espace à n dimensions est un système de n réels ou n complexes. L'addition de deux vecteurs et la multiplication par un scalaire sont naturellement introduites par la généralisation de la dimension 3. Pour parvenir vraiment à la notion d'espace vectoriel, il faut dégager le concept de sous-espace et de dimension d'un sous-espace. C'est ce que fera Grassman (professeur de lycée autodidacte en marge des milieux de la recherche) en cherchant à développer une analyse géométrique portant sur des calculs intrinsèques indépendants du choix des coordonnées. Grassman introduit le produit extérieur de deux vecteurs, la définition de l'indépendance linéaire, de la dimension d'un espace et démontre la relation fondamentale

$$\dim \mathrm{V} + \dim \mathrm{W} = \dim(\mathrm{V} + \mathrm{W}) - \dim \mathrm{V} \cap \mathrm{W}.$$

Ces travaux eurent peu d'impact au début, mais ils furent repris par Henri Poincaré et Elie Cartan (notamment son «algèbre extérieure» en géométrie différentielle).

C'est en 1888 que Peano donnera la définition axiomatique d'un espace vectoriel réel. Jusqu'en 1930, le point de vue des matrices et des coordonnées prédomine par rapport au point de vue intrinsèque des espaces vectoriels.

Les premiers exercices portent sur les sous-espaces vectoriels.

6.1. Intersection de sous-espaces

Soit E un espace vectoriel de dimension n et $\mathrm{F}_1, \ldots, \mathrm{F}_k$ des sous-espaces de E. Montrer que si $\sum_{i=1}^{k} \dim \mathrm{F}_i > n(k-1)$ alors $\bigcap_{i=1}^{k} \mathrm{F}_i \neq \{0\}$.

(**École normale supérieure**)

▷ **Solution.**

• Il suffit d'observer que $\bigcap_{i=1}^{k} \mathrm{F}_i$ est isomorphe au noyau de l'application linéaire

$$\psi : \begin{array}{ccc} \mathrm{F}_1 \times \cdots \times \mathrm{F}_k & \longrightarrow & \mathrm{E}^{k-1} \\ (x_1, x_2, \ldots, x_k) & \longmapsto & (x_2 - x_1, x_3 - x_1, \ldots, x_k - x_1) \end{array}$$

En effet, $\psi(x_1, \ldots, x_k) = 0$ si et seulement si $(x_1, \ldots, x_k) = (x, x, \ldots, x)$ où x appartient à $\bigcap_{i=1}^{k} \mathrm{F}_i$. Le théorème du rang permet alors d'affirmer que

$$\dim(\mathrm{F}_1 \times \mathrm{F}_2 \times \cdots \times \mathrm{F}_k) = \sum_{i=1}^{k} \dim \mathrm{F}_i = \operatorname{rg} \psi + \dim \bigcap_{i=1}^{k} \mathrm{F}_i.$$

Comme $\operatorname{rg}(\psi) \leqslant \dim \mathrm{E}^{k-1} = n(k-1)$, on a $\dim \bigcap_{i=1}^{k} \mathrm{F}_i > 0$. ◁

On peut rédiger la solution à l'aide des espaces quotients. Prenons donc cet exercice comme prétexte pour fournir quelques rappels sur cette notion.

Soit E *un* K*-espace vectoriel,* F *un sous-espace de* E*. Comme* F *est un sous-groupe du groupe abélien* $(\mathrm{E}, +)$*, on peut considérer le groupe quotient* E/F*, défini à partir de la relation d'équivalence telle que, pour tout* $(x, y) \in \mathrm{E}^2$*,*

$$x \equiv y \pmod{\mathrm{F}} \iff y - x \in \mathrm{F}.$$

La loi de composition externe est compatible avec cette congruence, i.e. *si* $\lambda \in \mathrm{K}$ *et* $x \equiv y \pmod{\mathrm{F}}$*, alors* $\lambda x \equiv \lambda y \pmod{\mathrm{F}}$*, si bien que l'on peut munir* E/F *d'une loi de composition externe définie pour* $\lambda \in \mathrm{K}$ *et* $x \in \mathrm{E}$ *par* $\lambda \overline{x} = \overline{\lambda x}$ *(la classe de* λx *ne dépend pas du représentant* x *choisi dans* $\overline{x}$*). Dans ces conditions,* E/F *est un* K*-espace vectoriel (le lecteur est invité à faire les quelques vérifications d'usage) appelé quotient de* E *par* F*.*

Si E *est de dimension finie,* E/F *est aussi de dimension finie et l'on a* $\dim \mathrm{E/F} = \dim \mathrm{E} - \dim \mathrm{F}$*. En effet, c'est une conséquence du théorème du rang, puisque la surjection canonique* $s : x \in \mathrm{E} \longmapsto \overline{x} \in \mathrm{E/F}$ *est linéaire de noyau* F*.*

Revenons maintenant à l'exercice ci-dessus. Dire que $x \in \mathrm{F}_i$ *revient à dire que son image dans* $\mathrm{E/F}_i$ *par la surjection canonique est nulle. On considère donc*

$$\Psi : \begin{array}{ccc} \mathrm{E} & \longrightarrow & \mathrm{E/F}_1 \times \cdots \times \mathrm{E/F}_k \\ x & \longmapsto & (\overline{x}, \ldots, \overline{x}) \end{array}$$

Il s'agit juste de prouver que, sous l'hypothèse $\sum_{i=1}^{k} \dim \mathrm{F}_i > n(k-1)$, *cette application linéaire n'est pas injective. C'est vrai car* $\dim \mathrm{E} = n$ *et*

$$\dim\left(\mathrm{E}/\mathrm{F}_1 \times \cdots \times \mathrm{E}/\mathrm{F}_k\right) = nk - \sum_{i=1}^{k} \dim \mathrm{F}_i < n = \dim \mathrm{E}.$$

L'exercice suivant a trait à la notion de supplémentaire. En dimension finie, l'existence d'un supplémentaire à un sous-espace donné résulte du théorème de la base incomplète. Nous pourrons, dans certains exercices de ce chapitre, admettre qu'en dimension infinie, tout sous-espace vectoriel admet également un supplémentaire, résultat qui nécessite toutefois l'axiome du choix.

6.2. Supplémentaire commun

Soit K un corps infini, E un K-espace vectoriel de dimension finie.

1. Montrer qu'on ne peut avoir $\mathrm{E} = \mathrm{V}_1 \cup \mathrm{V}_2 \cup \cdots \cup \mathrm{V}_\mathrm{N}$, où les V_i sont des sous-espaces stricts de E. Que se passe-t-il si K est fini ?

2. Montrer que si $\mathrm{F}_1, \mathrm{F}_2, \ldots, \mathrm{F}_p$ sont des sous-espaces vectoriels de E de même dimension (finie), il existe G supplémentaire commun à tous les F_i.

(École normale supérieure)

▷ **Solution.**

1. Raisonnons par l'absurde et supposons que $\mathrm{E} = \mathrm{V}_1 \cup \mathrm{V}_2 \cup \cdots \cup \mathrm{V}_\mathrm{N}$, où les V_i sont des sous-espaces stricts de E. On a nécessairement $\mathrm{N} \geqslant 2$, sinon $\mathrm{E} = \mathrm{V}_1$. Quitte à retirer un certain nombre de sous-espaces, jusqu'à ce que le nombre N de sous-espaces dont la réunion est E soit minimal, on peut supposer qu'aucun sous-espace n'est contenu dans la réunion des $\mathrm{N}-1$ autres. Pour aboutir alors à une contradiction, nous proposons deux méthodes différentes.

La première utilise directement un argument de cardinalité. On peut trouver $x \in \mathrm{V}_\mathrm{N}$ tel que $x \notin \mathrm{V}_1 \cup \mathrm{V}_2 \cup \cdots \cup \mathrm{V}_{\mathrm{N}-1}$. D'autre part, on n'a pas $\mathrm{V}_1 \cup \mathrm{V}_2 \cup \cdots \cup \mathrm{V}_{\mathrm{N}-1} \subset \mathrm{V}_\mathrm{N}$, sinon on aurait $\mathrm{E} = \mathrm{V}_\mathrm{N}$. Il existe donc $y \in \mathrm{V}_1 \cup \mathrm{V}_2 \cup \cdots \cup \mathrm{V}_{\mathrm{N}-1}$ tel que $y \notin \mathrm{V}_\mathrm{N}$. Considérons, pour tout $\lambda \in \mathrm{K}$, le vecteur $y + \lambda x$. Il n'appartient pas à V_N, car sinon $y \in \mathrm{V}_\mathrm{N}$. Il appartient donc à $\mathrm{V}_1 \cup \mathrm{V}_2 \cup \cdots \cup \mathrm{V}_{\mathrm{N}-1}$ de sorte qu'il existe $i_\lambda \in [\![1, \mathrm{N}-1]\!]$ tel que $y + \lambda x \in \mathrm{V}_{i_\lambda}$. L'application $\varphi : \lambda \in \mathrm{K} \longmapsto i_\lambda \in [\![1, \mathrm{N}-1]\!]$ est injective. En effet, supposons qu'il existe λ et μ, dans K tels que $i_\lambda = i_\mu$. Les vecteurs $y + \lambda x$ et $y + \mu x$ sont dans V_{i_λ}, donc leur différence $(\lambda - \mu)x$

aussi. Comme $x \notin V_{i_\lambda}$ on a $\mu = \lambda$. On obtient donc une application injective de K, qui est un ensemble infini, dans $[\![1, N-1]\!]$ qui est un ensemble fini. C'est absurde : E ne peut pas être réunion d'une famille finie de sous-espace stricts.

Autre méthode. Quitte à remplacer chaque sous-espace V_i par un hyperplan le contenant, on peut supposer que les V_i sont des hyperplans. On considère alors, pour tout $i \in [\![1, N]\!]$, une forme linéaire φ_i sur E , telle que $V_i = \operatorname{Ker} \varphi_i$. On n'a pas $V_i \subset \bigcup_{\substack{1 \leqslant j \leqslant N \\ j \neq i}} V_j$. Il existe donc $x_i \in V_i \setminus \bigcup_{\substack{1 \leqslant j \leqslant N \\ j \neq i}} V_j$. Considérons, pour tout $i \in [\![1, N]\!]$, l'application $F_i : K^n \to K$ définie par $F_i(\lambda_1, \ldots, \lambda_N) = \varphi_i(\sum_{j=1}^{N} \lambda_j x_j)$. C'est une fonction polynomiale sur K^N. L'hypothèse $E = V_1 \cup V_2 \cup \cdots \cup V_N$ entraîne $\prod_{i=1}^{N} \varphi_i = 0$ et donc $\prod_{i=1}^{N} F_i = 0$. Le corps K étant infini, l'algèbre des fonctions polynomiales sur K^n est isomorphe à $K[X_1, \ldots, X_N]$, qui est un anneau intègre. Il existe donc un entier i_0 entre 1 et N tel que $F_{i_0} = 0$. Puisque $N \geqslant 2$, on peut considérer un indice $i \neq i_0$. On obtient alors $\varphi_{i_0}(x_i) = F_{i_0}(0, \ldots, 1, \ldots, 0) = 0$, ce qui contredit le fait que $x_i \notin V_{i_0}$.

Si le corps K est fini, on obtient $|K| \leqslant N - 1$ par la première démonstration. Ainsi E ne peut pas être réunion de $|K|$ sous-espaces stricts ou moins.

Le lecteur pourra montrer que $|K| + 1$ *sous-espaces stricts suffisent effectivement pour recouvrir* E.

2. Il existe des sous-espaces G de E tels que $F_i \cap G = \{0\}$ pour tout $i \in [\![1, p]\!]$, par exemple le sous-espace nul. Parmi ces sous-espaces, considérons-en un de dimension maximale que l'on note G. Soit r la dimension commune des F_i. Si $r + \dim G < \dim E$, les sous-espaces $F_i \oplus G$ sont des sous-espaces stricts de E. Il existe alors, d'après la première question, un vecteur x n'appartenant à aucun de ces espaces. Mais alors le sous-espace $G' = G \oplus Kx$ est en somme directe avec tous les F_i, contredisant ainsi la maximalité de G. On a donc $r + \dim G = \dim E$ et G est un supplémentaire commun à tous les F_i. $\lhd$

On peut montrer, plus généralement, que dans le cas où K *est infini,* E *ne peut pas être réunion d'une famille* $(F_i)_{i \in I}$ *de sous-espaces stricts avec* $|I| < |K|$. *Par exemple si* $K = \mathbb{R}$, E *ne peut pas être réunion d'une famille dénombrable de sous-espaces stricts. Nous donnerons une preuve topologique de ce résultat dans le tome 3 d'analyse, à l'aide du théorème de Baire.*

La deuxième question se généralise alors directement avec la même démonstration : pour toute famille $(F_i)_{i \in I}$ *de sous-espaces de même dimension avec* $|I| < |K|$ *il existe un supplémentaire commun à tous les* F_i.

On rappelle que si V *est un espace vectoriel de dimension* n*, un drapeau de* V *est une suite croissante pour l'inclusion de* $n+1$ *sous-espaces vectoriels* $V_0 \subset V_1 \subset \cdots \subset V_n$ *avec* $\dim V_k = k$ *pour tout* k*. Cette notion se présente naturellement dans l'étude de la trigonalisation : un endomorphisme* u *de* V *est trigonalisable si et seulement s'il existe un drapeau stable par* u *(c'est-à-dire* $u(V_k) \subset V_k$ *pour tout* k*, avec les notations ci-dessus). Le groupe linéaire opère naturellement sur les drapeaux et le lecteur vérifiera facilement que cette opération est transitive. Le difficile exercice qui suit étudie le nombre d'orbites pour l'action du groupe linéaire sur les couples de drapeaux.*

6.3. Drapeaux

Soit V un K-espace vectoriel de dimension n, d et d' deux drapeaux, respectivement $V_0 \subset V_1 \subset \cdots \subset V_n$ et $V'_0 \subset V'_1 \subset \cdots \subset V'_n$.

1. On pose $A_{ij} = V'_{i-1} + V_j$ pour $i \in [\![1, n+1]\!]$ et $j \in [\![0, n]\!]$ et

$$\sigma(i) = \min\{j,\ A_{ij} = A_{i+1,j}\} \ \text{ pour } \ i \in [\![1, n]\!].$$

Montrer que σ est une bijection de $[\![1, n]\!]$ sur $[\![1, n]\!]$ (on pourra considérer l'application σ' définie comme σ, mais en échangeant les rôles de d et d').

2. Par définition, une base $(e_1, \ldots, e_n)$ est adaptée à d si, pour tout $k \in [\![1, n]\!]$, $\mathrm{Vect}(e_1, \ldots, e_k) = V_k$. Trouver une base $(e_1, \ldots, e_n)$ adaptée à d et une permutation σ de $[\![1, n]\!]$ telle que $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ soit adaptée à d'.

3. On fait opérer naturellement GL(V) sur les couples de drapeaux de V. Quel est le nombre d'orbites ?

(**École normale supérieure**)

▷ **Solution.**

1. • Notons, pour commencer, que, pour $i \in [\![1, n]\!]$, on a $\sigma(i) \in [\![1, n]\!]$. En effet, pour tout $i \in [\![1, n]\!]$, on a $A_{i0} = V'_{i-1} + V_0 = V'_{i-1}$ et donc $A_{i0} \neq A_{i+1,0}$. Explicitons la définition de $\sigma(i)$. L'espace $A_{ij} = V'_{i-1} + V_j$ est toujours inclus dans $A_{i+1,j} = V'_i + V_j$. On a l'inclusion inverse si $V'_i \subset V'_{i-1} + V_j$. Ceci équivaut à $V'_i \subset V'_{i-1} + V'_i \cap V_j$, puisque si $x \in V'_i$ s'écrit $y + z$, avec $(y, z) \in V'_{i-1} \times V_j$, alors $z = x - y \in V'_i \cap V_j$, et donc à $V'_i = V'_{i-1} + V'_i \cap V_j$, puisque l'inclusion inverse est toujours réalisée. On obtient les équivalences suivantes :

$$A_{ij} = A_{i+1,j} \iff V'_i = V'_{i-1} + V'_i \cap V_j \iff V'_i \cap V_j \not\subset V'_{i-1},$$

la dernière équivalence résultant de $\dim(V'_i) = \dim(V'_{i-1}) + 1$. On peut donc caractériser $\sigma(i)$ par

$$\begin{cases} V'_i \cap V_{\sigma(i)-1} \subset V'_{i-1} \\ V'_i \cap V_{\sigma(i)} \not\subset V'_{i-1}, \end{cases}$$

puisque, si $V'_i \cap V_j \subset V'_{i-1}$, alors $V'_i \cap V_k \subset V'_i \cap V_j \subset V'_{i-1}$, pour tout $0 \leqslant k \leqslant j$.

• Pour montrer que σ est une permutation de $[\![1,n]\!]$, considérons, comme le suggère l'énoncé, l'application $\sigma' : [\![1,n]\!] \longmapsto [\![1,n]\!]$ définie comme σ, mais en échangeant les rôles de d et d' et montrons que σ et σ' sont réciproques l'une de l'autre. Par symétrie des rôles de d et d', il suffit de prouver que $\sigma' \circ \sigma = \mathrm{Id}_{[\![1,n]\!]}$. Soit $i \in [\![1,n]\!]$, $j = \sigma(i)$. Il faut prouver que $\sigma'(j) = i$, c'est-à-dire que

$$\begin{cases} V_j \cap V'_{i-1} \subset V_{j-1} \\ V_j \cap V'_i \not\subset V_{j-1}. \end{cases}$$

⋆ Si $V_j \cap V'_{i-1} \not\subset V_{j-1}$, alors $V_j = V_{j-1} + V_j \cap V'_{i-1}$. Considérons un élément x de $V'_i \cap V_j$. Il s'écrit $y + z$, avec $(y,z) \in V_{j-1} \times V_j \cap V'_{i-1}$. On a alors $y = x - z \in V'_i \cap V_{j-1} \subset V'_{i-1}$, puisque $\sigma(i) = j$; x est donc dans V'_{i-1}. On a donc $V'_i \cap V_j \subset V'_{i-1}$, ce qui est contradictoire avec $\sigma(i) = j$. On conclut que $V_j \cap V'_{i-1} \subset V_{j-1}$.

⋆ Si $V_j \cap V'_i \subset V_{j-1}$, on obtient

$$V_j \cap V'_i \subset V_{j-1} \cap V'_i \subset V'_{i-1},$$

ce qui est faux. On a donc $V_j \cap V'_i \not\subset V_{j-1}$, ce qui termine la démonstration.

2. Construisons une base $(e_1, \ldots, e_n)$ adaptée à d telle que, pour la permutation σ précédemment définie, on ait $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ adaptée à d'.

On a, pour $j \in [\![1,n]\!]$, $V_j = V_{j-1} + V_j \cap V'_{\sigma'(j)}$. Considérons, pour tout $j \in [\![1,n]\!]$, un vecteur e_j dans $V_j \cap V'_{\sigma'(j)} \setminus V_{j-1}$. La famille (e_1) est une base de V_1 et si on suppose que $(e_1, \ldots, e_{j-1})$ est une base de V_{j-1}, alors $(e_1, \ldots, e_j)$ est une base de V_j, puisque $\dim(V_j) = \dim(V_{j-1}) + 1$ et que $e_j \in V_j \setminus V_{j-1}$. On a donc montré que $(e_1, \ldots, e_n)$ est une base adaptée à d. On a, d'autre part, pour $i \in [\![1,n]\!]$,

$$e_{\sigma(i)} \in V_{\sigma(i)} \cap V'_{\sigma' \circ \sigma(i)} = V_{\sigma(i)} \cap V'_i \subset V'_i.$$

La famille $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$ est donc une base adaptée à d'.

3. Le groupe $\mathrm{GL}(V)$ agit naturellement sur les drapeaux : pour tout $f \in \mathrm{GL}(V)$ et tout drapeau $d = (V_0, \ldots V_n)$, $(f(V_0), \ldots f(V_n))$ est un drapeau (car f conserve la dimension et l'inclusion), noté $f(d)$. Si (d, d') est un couple de drapeaux, $(f(d), f(d'))$ est un couple de drapeaux. Nous allons montrer que les orbites de couples de drapeaux sous

cette action de groupe sont caractérisées par la valeur de la permutation σ définie dans la question 2.

• Commençons par démontrer que cette permutation est unique (mais pas la base $(e_1, \ldots, e_n)$). Soit donc deux drapeaux d et d', une permutation τ de $[\![1, n]\!]$ et une base $(e_1, \ldots, e_n)$ de V telle que $(e_1, \ldots, e_n)$ soit adaptée à d et $(e_{\tau(1)}, \ldots, e_{\tau(n)})$ adaptée à d'. On a alors, pour tout $i \in [\![1, n]\!]$,

$$e_{\tau(i)} \in \mathrm{V}_{\tau(i)},\ e_{\tau(i)} \notin \mathrm{V}_{\tau(i)-1},\ e_{\tau(i)} \in \mathrm{V}'_i,\ e_{\tau(i)} \notin \mathrm{V}'_{i-1}.$$

On en déduit que $\mathrm{V}'_i \cap \mathrm{V}_{\tau(i)} \not\subset \mathrm{V}'_{i-1}$, car $e_{\tau(i)}$ appartient au premier ensemble mais pas au second. D'autre part on a

$$\begin{aligned}\mathrm{V}'_i \cap \mathrm{V}_{\tau(i)-1} &= \mathrm{Vect}(e_{\tau(1)}, \ldots, e_{\tau(i-1)}, e_{\tau(i)}) \cap \mathrm{Vect}(e_1, \ldots, e_{\tau(i)-1}) \\ &\subset \mathrm{Vect}(e_{\tau(1)}, e_{\tau(2)}, \ldots, e_{\tau(i-1)}) \subset \mathrm{V}'_{i-1}.\end{aligned}$$

Il résulte de la question 1 que les inclusions

$$\begin{cases} \mathrm{V}'_i \cap \mathrm{V}_{\tau(i)-1} \subset \mathrm{V}'_{i-1} \\ \mathrm{V}'_i \cap \mathrm{V}_{\tau(i)} \not\subset \mathrm{V}'_{i-1} \end{cases}$$

permettent de conclure que $\tau(i) = \sigma(i)$. Ceci est vrai pour tout $i \in [\![1, n]\!]$. Il en résulte que $\tau = \sigma$, ce qui démontre l'unicité voulue.

• Dans la suite, fixons $d = (\mathrm{V}_0, \ldots, \mathrm{V}_n)$ et $d' = (\mathrm{V}'_0, \ldots, \mathrm{V}'_n)$ deux drapeaux de V, $\mathcal{B} = (e_1, \ldots, e_n)$ une base de V, σ la permutation de $[\![1, n]\!]$ telle que $\mathcal{B}$ soit une base adaptée à d et que $(e_{\sigma(1)}, \ldots, e_{\sigma(n)})$, que nous noterons désormais $\sigma(\mathcal{B})$, soit une base adaptée à d'.

⋆ Pour tout $f \in \mathrm{GL}(\mathrm{V})$, $\mathcal{B}' = (f(e_1), \ldots, f(e_n))$ est une base de V ; pour tout $i \in [\![1, n]\!]$, $(f(e_1), \ldots, f(e_i))$ est une base de $f(\mathrm{V}_i)$ et $(f(e_{\sigma(1)}), \ldots, f(e_{\sigma(i)}))$ est une base de $f(\mathrm{V}'_i)$. Ceci montre que $\mathcal{B}'$ est une base adaptée à $f(d)$ et $\sigma(\mathcal{B}')$ une base adaptée à $f(d')$. La même permutation σ qu'au couple (d, d') est donc associée au couple $(f(d), f(d'))$.

⋆ Réciproquement soit (d_1, d'_1) un couple de drapeaux pour lequel il existe une base $\mathcal{B}'$ de V, adaptée à d_1 et telle que $\sigma(\mathcal{B}')$ soit adaptée à d'_1. Notons $d_1 = (\mathrm{W}_0, \ldots, \mathrm{W}_n)$, $d'_1 = (\mathrm{W}'_0, \ldots, \mathrm{W}'_n)$ et $\mathcal{B}' = (\varepsilon_1, \ldots, \varepsilon_n)$ et considérons $f \in \mathrm{GL}(\mathrm{V})$ défini par $f(e_i) = \varepsilon_i$, pour tout $i \in [\![1, n]\!]$.

On a alors, pour tout $i \in [\![1, n]\!]$,

$$\begin{aligned} f(\mathrm{V}_i) &= \mathrm{Vect}(f(e_1), \ldots, f(e_n)) = \mathrm{Vect}(\varepsilon_1, \ldots, \varepsilon_i) = \mathrm{W}_i, \\ f(\mathrm{V}'_i) &= \mathrm{Vect}(f(e_{\sigma(1)}), \ldots, f(e_{\sigma(i)})) = \mathrm{Vect}(\varepsilon_{\sigma(1)}, \ldots, \varepsilon_{\sigma(i)}) = \mathrm{W}'_i. \end{aligned}$$

On a donc $f(d, d') = (d_1, d'_1)$. Le couple de drapeaux (d_1, d'_1) appartient donc à l'orbite de (d, d').

On peut donc conclure que deux couples de drapeaux sont dans la même orbite si et seulement si la permutation σ qui leur est associée est

la même. L'ensemble des orbites peut être mis en bijection avec $\mathcal{S}_n$. Il y a donc $n!$ orbites. $\lhd$

Le lecteur trouvera dans l'exercice 7.18 une autre démonstration du résultat de la dernière question par une méthode matricielle utilisant la décomposition de Bruhat.

Nous commençons une série d'exercices assez généraux sur les applications linéaires. Le premier énoncé porte sur les lemmes de factorisation.

6.4. Lemmes de factorisation

Soit E, F et G deux K-espaces vectoriels de dimension finie.

1. Soit $f : \mathrm{E} \to \mathrm{F}$ et $g : \mathrm{E} \to \mathrm{G}$ des applications linéaires. Donner une condition nécessaire et suffisante sur f et g pour qu'il existe $h : \mathrm{F} \longrightarrow \mathrm{G}$ linéaire telle que $g = h \circ f$.

2. Soit $g : \mathrm{E} \longrightarrow \mathrm{G}$ et $h : \mathrm{F} \longrightarrow \mathrm{G}$ des applications linéaires. Donner une condition nécessaire et suffisante sur g et h pour qu'il existe $f : \mathrm{E} \longrightarrow \mathrm{F}$ linéaire telle que $g = h \circ f$.

(École polytechnique)

$\rhd$ **Solution.**

1. • Condition nécessaire. Supposons qu'il existe $h : \mathrm{F} \longrightarrow \mathrm{G}$ linéaire tel que $g = h \circ f$. Alors pour tout $x \in \operatorname{Ker} f$, on a

$$g(x) = h(f(x)) = h(0) = 0.$$

On obtient donc $\operatorname{Ker} f \subset \operatorname{Ker} g$.

$$\begin{tikzcd} \mathrm{E} \arrow[r, "f"] \arrow[dr, "g"'] & \mathrm{F} \arrow[d, dotted, "h"] \\ & \mathrm{G} \end{tikzcd}$$

• Supposons réciproquement que $\operatorname{Ker} f \subset \operatorname{Ker} g$. Alors, pour tout $(x, x') \in \mathrm{E}^2$ tel que $f(x) = f(x')$, on a $x - x' \in \operatorname{Ker} f$, donc $x - x' \in \operatorname{Ker} g$ et $g(x) = g(x')$.

Pour $y \in \operatorname{Im} f$, on pose $h'(y) = g(x) \in \mathrm{G}$ où x est un antécédent quelconque de y par f. Cette définition est cohérente, car $g(x)$ ne dépend pas de l'antécédent x choisi, comme on vient de le voir.

Par construction, pour tout $x \in \mathrm{E}$, on a $h'(f(x)) = g(x)$. Ceci montre que $h' \circ f = g$.

Montrons que $h' : \operatorname{Ker} f \longrightarrow \mathrm{G}$ est linéaire. Soit $(y, y') \in (\operatorname{Im} f)^2$, $(\lambda, \mu) \in \mathrm{K}^2$ et $(x, x') \in \mathrm{E}^2$ tel que $f(x) = y$ et $f(x') = y'$. On obtient alors $f(\lambda x + \mu x') = \lambda y + \mu y'$ et $\lambda x + \mu x'$ est un antécédent de $\lambda y + \mu y'$ par f. On a par définition

$$h'(\lambda y + \mu y') = g(\lambda x + \mu x') = \lambda g(x) + \mu g(x') = \lambda h'(y) + \mu h'(y').$$

La linéarité est prouvée.

Toute application $h \in \mathcal{L}(\mathrm{F}, \mathrm{G})$ dont la restriction à $\operatorname{Im} f$ est égale à h' (et il en existe) répond alors à la question posée. On remarque que si f est surjective, h est unique.

Conclusion. Il existe $h : \mathrm{F} \longrightarrow \mathrm{G}$ linéaire telle que $g = h \circ f$ si, et seulement si, $\operatorname{Ker} f \subset \operatorname{Ker} g$.

2. • Dans cette seconde question, il est clairement nécessaire que l'on ait $\operatorname{Im} g \subset \operatorname{Im} h$.

• Supposons réciproquement que $\operatorname{Im} g \subset \operatorname{Im} h$. Considérons un supplémentaire F' de $\operatorname{Ker} h$ dans F. Alors h induit un isomorphisme $\tilde{h}$ de F' sur $\operatorname{Im} h$. Notons

$$k = \tilde{h}^{-1} : \operatorname{Im} h \longrightarrow \mathrm{F}'.$$

$$\begin{tikzcd} \mathrm{E} \arrow[r, dashed, "f"] \arrow[dr, "g"'] & \mathrm{F} \arrow[d, "h"] \\ & \mathrm{G} \end{tikzcd}$$

L'application $f = k \circ g$ est bien définie car $\operatorname{Im} g \subset \operatorname{Im} h$. Elle est linéaire de E dans F' ; nous la considérerons comme une application linéaire de E dans F. On obtient, $h(f(x)) = h(k(g(x))) = g(x)$, pour tout $x \in \mathrm{E}$, *i.e.* $g = h \circ f$.

Conclusion. Il existe $f : \mathrm{E} \longrightarrow \mathrm{F}$ linéaire telle que $g = h \circ f$ si, et seulement si, $\operatorname{Im} g \subset \operatorname{Im} h$. $\lhd$

L'exercice précédent permet de répondre à la question suivante : E *étant un* K*-espace vectoriel,* F *un sous-espace de* E, $s : \mathrm{E} \to \mathrm{E}/\mathrm{F}$ *la surjection canonique et* $u \in \mathcal{L}(\mathrm{E})$, *à quelle condition* u *induit-t-elle une application* $\overline{u}$ *de* $\mathcal{L}(\mathrm{E}/\mathrm{F})$ *telle que* $\overline{u} \circ s = s \circ u$ *? Comme* s *est surjective, en cas d'existence,* $\overline{u}$ *est unique. D'après la première question de l'exercice,* $\overline{u}$ *existe si et seulement si* $\operatorname{Ker} s \subset \operatorname{Ker}(s \circ u)$. *Comme* $\operatorname{Ker} s = \mathrm{F}$, *cette condition signifie que pour tout* $x \in \mathrm{F}$, $u(x) \in \mathrm{F}$. *Autrement dit,* u *passe au quotient si et seulement si* F *est stable par* u.

Plus généralement, si E *et* F *sont deux espaces vectoriels,* u *un élément de* $\mathcal{L}(\mathrm{E}, \mathrm{F})$, E' *et* F' *deux sous-espaces vectoriels de* E *et* F *respectivement,* u *induit une application linéaire de* E/E' *dans* F/F' *si, et seulement si,* $u(\mathrm{E}') \subset \mathrm{F}'$.

6.5. Condition pour que $\operatorname{rg} g \leqslant \operatorname{rg} f$

Soit E, F deux K-espaces vectoriels non nuls de dimension finie, f et g dans $\mathcal{L}(\mathrm{E}, \mathrm{F})$. Montrer que $\operatorname{rg} g \leqslant \operatorname{rg} f$ si et seulement s'il existe $h \in \mathrm{GL}(\mathrm{F})$ et $k \in \mathcal{L}(\mathrm{E})$ tels que $h \circ g = f \circ k$.

(École polytechnique)

▷ **Solution.**

• Une des implications est aisée. En effet, s'il existe $h \in \mathrm{GL(F)}$ et $k \in \mathcal{L}(\mathrm{E})$ tels que $h \circ g = f \circ k$, on a $g = h^{-1} \circ f \circ k$ et donc

$$\operatorname{Im} g = \operatorname{Im}(h^{-1} \circ f \circ k) \subset \operatorname{Im}(h^{-1} \circ f) = h^{-1}(\operatorname{Im} f),$$

d'où l'on déduit, puisque $h^{-1} \in \mathrm{GL(F)}$,

$$\operatorname{rg}(g) \leqslant \dim(h^{-1}(\operatorname{Im} f)) = \dim(\operatorname{Im} f) = \operatorname{rg} f.$$

• Notons $p = \operatorname{rg} f$ et $q = \operatorname{rg} g$ et supposons réciproquement que l'on a $q \leqslant p$. On considère $(e_{p+1}, \ldots, e_n)$ une base de $\operatorname{Ker} f$ complétée en $(e_1, \ldots, e_n)$ base de E et $(\varepsilon_{q+1}, \ldots, \varepsilon_n)$ une base de $\operatorname{Ker} g$ complétée en $(\varepsilon_1, \ldots, \varepsilon_n)$ base de E. La famille $(g(\varepsilon_1), \ldots, g(\varepsilon_q))$ est alors une base de $\operatorname{Im} g$ que l'on peut compléter en $(g(\varepsilon_1), \ldots, g(\varepsilon_q), g_{q+1}, \ldots, g_m)$ base de F. De même, $(f(e_1), \ldots, f(e_p))$ est une base de $\operatorname{Im} f$ que l'on peut compléter en $(f(e_1), \ldots, f(e_p), f_{p+1}, \ldots, f_m)$ base de F. Soit k dans $\mathcal{L}(\mathrm{E})$ défini par $k(\varepsilon_1) = e_1, \ldots, k(\varepsilon_q) = e_q$, $k(\varepsilon_{q+1}) = \cdots = k(\varepsilon_n) = 0$ et h dans $\mathrm{GL(F)}$ qui transforme la base $(g(\varepsilon_1), \ldots, g(\varepsilon_q), g_{q+1}, \ldots, g_m)$ en la base $(f(e_1), \ldots, f(e_p), f_{p+1}, \ldots, f_m)$.

On obtient alors, si $1 \leqslant i \leqslant q$, $f \circ k(\varepsilon_i) = f(e_i) = h(g(\varepsilon_i)) = h \circ g(\varepsilon_i)$ (car $i \leqslant q \leqslant p$), et si $i > q$, $f \circ k(\varepsilon_i) = 0 = h \circ g(\varepsilon_i)$. On a donc bien $h \circ g = f \circ k$. ◁

On peut donner une deuxième solution pour la réciproque utilisant un des lemmes de factorisation vus à l'exercice 6.4 : en effet, d'après le second lemme, il suffit de montrer que si $\operatorname{rg} g \leqslant \operatorname{rg} f$, *on peut trouver* $h \in \mathrm{GL(F)}$ *tel que* $\operatorname{Im}(h \circ g) \subset \operatorname{Im} f$. *Pour cela, considérons un sous-espace* G *de* $\operatorname{Im} f$ *de dimension* $\operatorname{rg} g$ *et un isomorphisme* h' *de* $\operatorname{Im} g$ *sur* G. *Si on note* F′ *et* G′ *des supplémentaires de* $\operatorname{Im} g$ *et* G *dans* F *respectivement, ces sous-espaces ont même dimension ; soit* h'' *un isomorphisme de* F′ *sur* G′. *L'endomorphisme* h *de* F *dont les restrictions à* $\operatorname{Im} g$ *et* F′ *sont respectivement* h' *et* h'' *est un isomorphisme de* F, *qui vérifie*

$$\operatorname{Im} h \circ g = h(\operatorname{Im} g) = \mathrm{G} \subset \operatorname{Im} f.$$

L'exercice 7.1 fournira une troisième solution, matricielle.

Il est bien connu du lecteur qu'un endomorphisme d'un espace E *qui stabilise toutes les droites vectorielles est une homothétie. Ce résultat intervient assez souvent ; aussi nous allons en rappeler la preuve.*

Lemme. *Soit* E *un* K*-espace vectoriel non nul, et* $u \in \mathcal{L}(\mathrm{E})$. *On suppose que pour* $x \in \mathrm{E}$, $u(x)$ *et* x *sont colinéaires. Alors* u *est une homothétie.*

Démonstration. *L'hypothèse signifie que tout vecteur non nul de* E *est un vecteur propre de* u. *Il suffit donc de montrer que* u *admet une unique valeur propre. Supposons qu'il existe deux valeurs propres distinctes* λ *et* λ' *de* u *et considérons deux vecteurs propres* x *et* x' *associés. On a*

alors $u(x) = \lambda x$ *et* $u(x') = \lambda' x'$. *On sait que* (x, x') *est une famille libre. Par hypothèse* $x + x'$ *est aussi un vecteur propre de* u *; il existe un scalaire* μ *tel que* $u(x+x') = \mu(x+x')$. *Mais, par linéarité nous obtenons aussi* $u(x + x') = u(x) + u(x') = \lambda x + \lambda' x'$. *Par unicité de l'écriture, il vient* $\lambda = \lambda' = \mu$, *ce qui est absurde.* $\diamondsuit$

Ce résultat est utile dans bien des situations. Par exemple, si E *est un* K*-espace vectoriel, on peut en déduire que le centre de* $\mathcal{L}(\mathrm{E})$ *est réduit aux homothéties. Les homothéties commutent évidemment avec tout endomorphisme. Réciproquement, supposons que* u *commute avec tout endomorphisme de* E. *Soit* $x \in \mathrm{E}$, H *un supplémentaire de* $\mathrm{K}x$ *et* p *la projection sur* $\mathrm{K}x$ *parallèlement à* H. *On a alors,*

$$u(x) = (u \circ p)(x) = (p \circ u)(x) = p(u(x)) \in \mathrm{K}x$$

et u *est une homothétie d'après le lemme.*

Les deux exercices suivants sont des variations sur le thème du lemme.

6.6. Endomorphismes stabilisant les sous-espaces de dimension k

> Soit E un K-espace vectoriel de dimension finie n et $k \in [\![1, n-1]\!]$. Que peut-on dire d'un endomorphisme u de E laissant stables tous les sous-espaces de dimension k de E ?
>
> **(École normale supérieure)**

▷ **Solution.**

On sait que pour $k = 1$, u est une homothétie (c'est le lemme ci-dessus). Soit $k \in [\![2, n-1]\!]$ et H un sous-espace de dimension $k-1$. On observe que H peut être obtenu comme intersection de deux sous-espaces de dimension k : comme $\dim \mathrm{H} \leqslant n-2$, on peut trouver un couple de vecteurs libres (e_1, e_2) tel que le plan $\mathrm{Vect}(e_1, e_2)$ soit en somme directe avec H. Posons $\mathrm{H}_1 = \mathrm{Vect}(\mathrm{H} \cup \{e_1\})$ et $\mathrm{H}_2 = \mathrm{Vect}(\mathrm{H} \cup \{e_2\})$. On a alors $\mathrm{H}_1 \cap \mathrm{H}_2 = \mathrm{H}$ et $\dim \mathrm{H}_1 = \dim \mathrm{H}_2 = k$.

Il en résulte que si $u \in \mathcal{L}(\mathrm{E})$ stabilise tous les sous-espaces de dimension k alors u stabilise aussi tous les sous-espaces de dimension $k-1$. Par une récurrence descendante finie, il en résulte que u stabilise toutes les droites vectorielles de E. On conclut alors que u est une homothétie. ◁

6.7. Exemple d'utilisation des espaces quotients

> Soit E un K-espace vectoriel de dimension finie, $a \in \mathrm{E}$. Déterminer les éléments u de $\mathcal{L}(\mathrm{E})$ tel que pour tout $x \in \mathrm{E}$, la famille $(a, x, u(x))$ soit liée.
>
> **(École polytechnique)**

▷ **Solution.**

• Si $a = 0$ ou $\dim E \leqslant 2$, tout u convient. Supposons $a \neq 0$ et $n = \dim E \geqslant 3$ et considérons u vérifiant la condition de l'énoncé. On pose $e_1 = a$ et on complète en une base $(e_1, \ldots, e_n)$ de E. Si $i \geqslant 2$, (e_i, a) est une famille libre et par hypothèse, $u(e_i) \in \mathrm{Vect}(e_i, e_1)$. Considérons le vecteur $u(e_1 + e_i)$. Comme la famille $(e_1 + e_i, e_1)$ est libre, on a

$$u(e_1 + e_i) \in \mathrm{Vect}(e_1 + e_i, e_1) = \mathrm{Vect}(e_1, e_i).$$

Puisque $u(e_1 + e_i) = u(e_1) + u(e_i)$ et que $u(e_i) \in \mathrm{Vect}(e_1, e_i)$, on en déduit que $u(e_1) \in \mathrm{Vect}(e_1, e_i)$. On obtient

$$u(e_1) \in \mathrm{Vect}(e_1, e_2) \cap \mathrm{Vect}(e_1, e_3) = \mathrm{K}e_1.$$

• On a donc $u(a) \in \mathrm{K}a$: la droite $\mathrm{K}a$ est stable par u, donc u induit un endomorphisme $\overline{u}$ de $E/\mathrm{K}a$ défini par $\overline{u}(\overline{x}) = \overline{u(x)}$.

Soit $x \in E$ tel que $\overline{x} \neq 0$. Alors, la famille (a, x) est libre et par hypothèse, $u(x) \in \mathrm{Vect}(a, x)$. Il s'ensuit que $\overline{u}(\overline{x}) = \overline{u(x)} \in \mathrm{Vect}(\overline{x})$. Comme cela vaut pour tout $\overline{x} \in E/\mathrm{K}a$, $\overline{u}$ est une homothétie : il existe donc $\lambda \in \mathrm{K}$ tel que $\overline{u(x)} = \lambda\overline{x}$ pour tout $x \in E$. Il s'ensuit que pour tout $x \in E$, $u(x) - \lambda x \in \mathrm{K}a$. L'application $x \longmapsto u(x) - \lambda x$ étant linéaire, il existe φ forme linéaire de E telle que, pour tout $x \in E$

$$\boxed{u(x) = \lambda x + \varphi(x)a}.$$

Réciproquement, une telle application répond bien au problème posé. ◁

Les deux exercices suivants concernent des endomorphismes nilpotents.

6.8. Majoration de l'indice de nilpotence

> Soit E un K-espace vectoriel de dimension finie n et $u \in \mathcal{L}(E)$, nilpotent. Montrer que $u^n = 0$.
>
> **(École normale supérieure)**

▷ **Solution.**

Voici une solution complètement élémentaire de cet exercice. Supposons par l'absurde que $u^n \neq 0$. appelons p l'indice de nilpotence de u ($p > n$). L'application u^{p-1} n'étant pas nulle, considérons un vecteur x de E tel que $u^{p-1}(x) \neq 0$. On va montrer que la famille $(x, u(x), \ldots, u^{p-1}(x))$ est libre ce qui fournit notre contradiction puisque cette famille est de cardinal $p > n$. Si la famille est liée, on peut écrire

une relation de liaison du type

$$\lambda_k u^k(x) + \lambda_{k+1} u_{k+1}(x) + \cdots + \lambda_{p-1} u^{p-1}(x) = 0$$

avec $\lambda_k \neq 0$. En appliquant u^{p-1-k} à cette égalité, il vient $\lambda_k u^{p-1}(x) = 0$, ce qui est impossible. L'hypothèse $u^n \neq 0$ est donc absurde. ◁

Bien entendu, il est encore plus rapide de dire que si $u^n \neq 0$, le polynôme minimal de u est X^p ($p > n$), ce qui est impossible puisque le polynôme minimal est de degré inférieur à n (il divise le polynôme caractéristique par le théorème de Cayley-Hamilton). Enfin le résultat découle aussi directement du résultat de l'exercice 6.14.

Voici une petite application : si $n \geqslant 2$, où n désigne toujours la dimension de l'espace, un endomorphisme nilpotent u d'indice de nilpotence n n'est pas un carré. En effet, si $u = v^2$, alors v est aussi nilpotent et donc $v^n = 0$. Mais alors $u^{n-1} = v^{2n-2} = 0$ car $2n - 2 \geqslant n$ ce qui contredit le fait que u est d'indice n.

L'énoncé suivant est une généralisation du précédent.

6.9. Produit commutatif d'endomorphismes nilpotents

Soit E un K-espace vectoriel de dimension finie n et $u_1, \ldots, u_n$ des endomorphismes nilpotents de E qui commutent deux à deux. Que vaut $u_1 \circ u_2 \circ \cdots \circ u_n$?

(École polytechnique)

▷ **Solution.**

Si tous les u_k sont égaux à u_1, leur produit vaut u_1^n qui est nul, comme nous venons de le démontrer dans l'exercice 6.8. Il est donc raisonnable de penser qu'on a toujours $u_1 \circ u_2 \circ \cdots \circ u_n = 0$.

Nous savons que, lorsque deux endomorphismes commutent, le noyau et l'image de l'un sont stables par l'autre. Ainsi, pour $1 \leqslant k < n$, u_k laisse stable $F_{k+1} = \mathrm{Im}(u_{k+1} \circ \cdots \circ u_n)$. Or si F_{k+1} n'est pas réduit à $\{0\}$, la restriction de u_k à F_{k+1} ne peut être bijective : en effet, cette restriction est aussi nilpotente. Par conséquent, $u_k(F_{k+1})$ est contenu strictement dans F_{k+1} et

$$\dim F_k = \dim u_k(F_{k+1}) < \dim F_{k+1}.$$

Si l'un des F_i est nul c'est terminé et sinon, on a par une récurrence descendante finie que $\dim F_i < i$ pour tout $1 \leqslant i < n$. Ceci implique en particulier $\dim F_1 = \mathrm{rg}(u_1 \circ u_2 \circ \cdots \circ u_n) < 1$, c'est-à-dire

$$\boxed{u_1 \circ u_2 \circ \cdots \circ u_n = 0}. \ ◁$$

Voici maintenant une série d'exercices assez faciles, centrés sur le théorème du rang. Le premier présente quelques inégalités classiques d'usage courant.

6.10. Inégalité de Sylvester

Soit E un espace vectoriel de dimension finie n, a et b deux endomorphismes de E.

1. Comparer $\mathrm{rg}(a+b)$ à $\mathrm{rg}(a)+\mathrm{rg}(b)$ et $\mathrm{rg}(a)-\mathrm{rg}(b)$.

2. Prouver l'équivalence :

$$\mathrm{rg}(a+b)=\mathrm{rg}(a)+\mathrm{rg}(b) \Longleftrightarrow (\mathrm{Im}\,a\cap\mathrm{Im}\,b=\{0\} \text{ et } \mathrm{Ker}\,a+\mathrm{Ker}\,b=\mathrm{E})$$

3. Montrer que $\mathrm{rg}(a)+\mathrm{rg}(b)-n \leqslant \mathrm{rg}(ab) \leqslant \min(\mathrm{rg}(a),\mathrm{rg}(b))$. C'est *l'inégalité de Sylvester.*

(École polytechnique)

▷ **Solution.**

1. De l'inclusion $\mathrm{Im}(a+b)\subset \mathrm{Im}\,a+\mathrm{Im}\,b$, on tire les inégalités

$$\mathrm{rg}(a+b)\leqslant \dim(\mathrm{Im}\,a+\mathrm{Im}\,b)\leqslant \dim(\mathrm{Im}\,a)+\dim(\mathrm{Im}\,b)=\mathrm{rg}(a)+\mathrm{rg}(b). \quad (\star)$$

En appliquant ce résultat à $a+b$ et $-b$, on obtient, compte tenu de l'égalité $\mathrm{rg}(b)=\mathrm{rg}(-b)$,

$$\mathrm{rg}(a)\leqslant \mathrm{rg}(a+b)+\mathrm{rg}(-b)\leqslant \mathrm{rg}(a+b)+\mathrm{rg}(b)$$

c'est-à-dire

$$\mathrm{rg}(a)-\mathrm{rg}(b)\leqslant \mathrm{rg}(a+b).$$

Par symétrie on a $\mathrm{rg}(b)-\mathrm{rg}(a)\leqslant \mathrm{rg}(a+b)$. On conclut que

$$\boxed{|\mathrm{rg}(a)-\mathrm{rg}(b)|\leqslant \mathrm{rg}(a+b)\leqslant \mathrm{rg}(a)+\mathrm{rg}(b)}.$$

2. • Supposons que $\mathrm{rg}(a+b)=\mathrm{rg}(a)+\mathrm{rg}(b)$. Toutes les inégalités de $(\star)$ sont alors des égalités. On a en particulier

$$\dim(\mathrm{Im}\,a+\mathrm{Im}\,b)=\dim \mathrm{Im}\,a+\dim \mathrm{Im}\,b.$$

Sachant que $\dim(\mathrm{Im}\,a\cap \mathrm{Im}\,b)=\dim \mathrm{Im}\,a+\dim \mathrm{Im}\,b-\dim(\mathrm{Im}\,a+\mathrm{Im}\,b)$, on en déduit que $\mathrm{Im}\,a\cap \mathrm{Im}\,b=\{0\}$.

Ceci étant réalisé, notons qu'on a ensuite $\mathrm{Ker}(a+b)=\mathrm{Ker}\,a\cap \mathrm{Ker}\,b$. En effet, on a toujours $\mathrm{Ker}\,a\cap \mathrm{Ker}\,b\subset \mathrm{Ker}(a+b)$ et si $x\in \mathrm{Ker}(a+b)$, on peut écrire

$$a(x)=-b(x)\in \mathrm{Im}\,a\cap \mathrm{Im}\,b=\{0\}$$

et $x \in \operatorname{Ker} a \cap \operatorname{Ker} b$. On obtient alors

$$\begin{aligned}\dim(\operatorname{Ker} a + \operatorname{Ker} b) &= \dim(\operatorname{Ker} a) + \dim(\operatorname{Ker} b) - \dim(\operatorname{Ker} a \cap \operatorname{Ker} b)\\ &= \dim(\operatorname{Ker} a) + \dim(\operatorname{Ker} b) - \dim(\operatorname{Ker}(a+b))\\ &= n - \operatorname{rg}(a) + n - \operatorname{rg}(b) - n + \operatorname{rg}(a+b) = n,\end{aligned}$$

puisque $\operatorname{rg}(a+b) = \operatorname{rg}(a) + \operatorname{rg}(b)$.

On a donc $\operatorname{Ker} a + \operatorname{Ker} b = \mathrm{E}$.

• Supposons que $\operatorname{Im} a \cap \operatorname{Im} b = \{0\}$ et $\operatorname{Ker} a + \operatorname{Ker} b = \mathrm{E}$. On a alors, comme il a été démontré précédemment, $\operatorname{Ker}(a+b) = \operatorname{Ker} a \cap \operatorname{Ker} b$. On en déduit

$$\begin{aligned}\operatorname{rg}(a+b) &= n - \dim(\operatorname{Ker}(a+b)) = n - \dim(\operatorname{Ker} a \cap \operatorname{Ker} b)\\ &= n - (\dim \operatorname{Ker} a + \dim \operatorname{Ker} b - \dim(\operatorname{Ker} a + \operatorname{Ker} b)\\ &= n - \dim(\operatorname{Ker} a) + n - \dim(\operatorname{Ker} b), \text{ car } \operatorname{Ker} a + \operatorname{Ker} b = \mathrm{E}\\ &= \operatorname{rg}(a) + \operatorname{rg}(b).\end{aligned}$$

3. De l'inclusion $\operatorname{Im}(ab) \subset \operatorname{Im} a$ résulte $\operatorname{rg}(ab) \leqslant \operatorname{rg} a$. Mais on a aussi $\operatorname{Im}(ab) = a(\operatorname{Im} b)$, d'où l'on déduit $\operatorname{rg}(ab) \leqslant \operatorname{rg}(b)$, car une application linéaire n'augmente pas la dimension des espaces vectoriels (cela résulte du théorème du rang). Finalement, on obtient

$$\operatorname{rg}(ab) \leqslant \min(\operatorname{rg}(a), \operatorname{rg}(b)).$$

Pour obtenir l'autre inégalité, considérons la restriction a' de a à $\operatorname{Im} b$. Elle vérifie $\operatorname{Im}(a') = \operatorname{Im}(ab)$ et $\operatorname{Ker} a' = \operatorname{Ker} a \cap \operatorname{Im} b$. Le théorème du rang donne

$$\begin{aligned}\dim \operatorname{Im}(ab) &= \dim(\operatorname{Im} b) - \dim(\operatorname{Ker} a \cap \operatorname{Im} b)\\ &\geqslant \dim(\operatorname{Im} b) - \dim(\operatorname{Ker} a) \geqslant \operatorname{rg}(b) - (n - \operatorname{rg}(a)).\end{aligned}$$

On obtient l'inégalité voulue :

$$\boxed{\operatorname{rg}(ab) \geqslant \operatorname{rg}(a) + \operatorname{rg}(b) - n}.$$

On peut obtenir d'une autre manière cette inégalité en utilisant un espace vectoriel quotient (cf. page 260 pour des rappels sur la question). Considérons la restriction u de b à $\operatorname{Ker}(ab)$. Son image est incluse dans $\operatorname{Ker} a$, car on a, pour tout $x \in \operatorname{Ker}(ab)$, $ab(x) = 0$ et donc $b(x) \in \operatorname{Ker} a$. On peut donc considérer u comme un élément de $\mathcal{L}(\operatorname{Ker}(ab), \operatorname{Ker} a)$. La restriction de u à $\operatorname{Ker} b$ est évidemment nulle, donc u induit une application linéaire $\overline{u} : \operatorname{Ker}(ab)/\operatorname{Ker} b \longrightarrow \operatorname{Ker} a$ définie par $\overline{u}(\overline{x}) = \overline{u(x)}$. L'application $\overline{u}$ est injective. En effet, pour tout $x \in \operatorname{Ker}(ab)$, on a

$\overline{u}(\overline{x}) = u(x) = b(x)$ et $\overline{u}(\overline{x}) = 0$ si et seulement si $x \in \operatorname{Ker} b$, c'est-à-dire si $\overline{x} = 0$. On en déduit que

$$\dim \operatorname{Ker} a \geqslant \dim \operatorname{Im} \overline{u} = \dim (\operatorname{Ker}(ab)/\operatorname{Ker} b) = \dim \operatorname{Ker}(ab) - \dim \operatorname{Ker} b,$$

c'est-à-dire

$$\dim \operatorname{Ker} a + \dim \operatorname{Ker} b \geqslant \dim \operatorname{Ker}(ab).$$

En utilisant le théorème du rang, on retrouve l'inégalité précédente. ◁

6.11. Pseudo-inverse

Soit E un espace vectoriel de dimension finie.

1. Soit f et g deux endomorphismes de E. On considère les trois conditions :

$$(i)\ f \circ g \circ f = f\ ; \quad (ii)\ g \circ f \circ g = g\ ; \quad (iii)\ \operatorname{rg}(f) = \operatorname{rg}(g).$$

Montrer que si deux de ces conditions sont réalisées, la troisième l'est aussi.

2. Soit f un endomorphisme de E. Montrer l'existence d'un endomorphisme g tel que (i), (ii) et (iii) soient vérifiées.

3. Soit f, g, h, $\tilde{f}$, $\tilde{g}$ des endomorphismes de E tels que

$$f \circ \tilde{f} \circ f = f \quad \text{et} \quad g \circ \tilde{g} \circ g = g.$$

Montrer qu'il existe un endomorphisme u de E tel que $f \circ u \circ g = h$ si, et seulement si, $f \circ \tilde{f} \circ h \circ \tilde{g} \circ g = h$.

(École polytechnique)

▷ **Solution.**

1. • Supposons (i) et (ii) vérifiées et montrons (iii). On a grâce à (i)

$$\operatorname{rg}(f) = \operatorname{rg}(f \circ g \circ f) \leqslant \operatorname{rg}(f \circ g) \leqslant \operatorname{rg} g$$

et de même, $\operatorname{rg}(g) = \operatorname{rg}(g \circ f \circ g) \leqslant \operatorname{rg}(g \circ f) \leqslant \operatorname{rg} f$. Par conséquent, on a $\operatorname{rg} f = \operatorname{rg} g$.

• Supposons (i) et (iii) vérifiées et montrons (ii). En composant la relation (i) à droite par g, on obtient $f \circ g = f \circ (g \circ f \circ g)$. Pour pouvoir simplifier par f à gauche, il suffit que la restriction de f à l'image de g soit injective. D'après (i), on a $\operatorname{rg}(f) \leqslant \operatorname{rg}(f \circ g)$. Comme $\operatorname{rg}(f \circ g) \leqslant \operatorname{rg} f$, il y a égalité. Mais le rang de $f \circ g$ est exactement le rang de la restriction de f à $\operatorname{Im} g$. D'où le résultat.

• La symétrie des rôles de f et g permet d'affirmer que (ii) et (iii) entraînent (i).

2. D'après la question 1, il suffit de construire g vérifiant (ii) et (iii). On remarque que si g convient, on a, pour $y \in \operatorname{Im} g$, $g \circ f(y) = y$. En particulier l'image de g doit être en somme directe avec le noyau de f et pour avoir (iii) il doit même s'agir d'un supplémentaire de $\operatorname{Ker} f$.

Soit F un supplémentaire de $\operatorname{Ker} f$. Alors $f' : x \in \mathrm{F} \longmapsto f(x) \in \operatorname{Im} f$ est un isomorphisme. Soit G un supplémentaire de $\operatorname{Im} f$. Il existe un endomorphisme g de E tel que $g_{|\operatorname{Im} f} = f'^{-1}$ et $g_{|\mathrm{G}} = 0$. On a alors l'égalité $\operatorname{Im} g = \operatorname{Im} f'^{-1} = \mathrm{F}$, qui entraine $\operatorname{rg} g = \dim \mathrm{F} = \operatorname{rg} f$: ainsi g vérifie (iii).

D'autre part, si $x \in \mathrm{E}$, $g(x)$ appartient à F. Il en résulte que

$$g \circ f \circ g(x) = g(f(g(x)) = g(f'(g(x))) = (g \circ f')(g(x)) = g(x).$$

On a donc $g \circ f \circ g = g$: g vérifie aussi (ii).

3. Supposons que $f \circ \tilde{f} \circ h \circ \tilde{g} \circ g = h$. Si on pose $u = \tilde{f} \circ h \circ \tilde{g}$, on obtient $f \circ u \circ g = h$.

Réciproquement, s'il existe $u \in \mathcal{L}(\mathrm{E})$ tel que $f \circ u \circ g = h$, on a

$$(f \circ \tilde{f} \circ f) \circ u \circ (g \circ \tilde{g} \circ g) = h$$

et donc $h = f \circ \tilde{f} \circ (f \circ u \circ g) \circ \tilde{g} \circ g = f \circ \tilde{f} \circ h \circ \tilde{g} \circ g$. ◁

6.12. Endomorphismes u tels que $\operatorname{Ker} u = \operatorname{Im} u$

Soit E un espace vectoriel (de dimension quelconque).

1. Soit u un endomorphisme de E tel que $\operatorname{Ker} u = \operatorname{Im} u$ et S un supplémentaire de $\operatorname{Im} u$: $\mathrm{E} = \mathrm{S} \oplus \operatorname{Im} u$.

a. Montrer que, pour tout $x \in \mathrm{E}$, il existe un unique couple $(y, z) \in \mathrm{S}^2$ tel que $x = y + u(z)$. On pose $z = v(x)$ et $y = w(x)$.

b. Montrer que v est linéaire et calculer $u \circ v + v \circ u$.

c. Montrer que w est linéaire et calculer $u \circ w + w \circ u$.

2. Soit $u \in \mathcal{L}(\mathrm{E})$ tel que $u^2 = 0$. On suppose qu'il existe v dans $\mathcal{L}(\mathrm{E})$ tel que $u \circ v + v \circ u = \mathrm{Id}_{\mathrm{E}}$. A-t-on nécessairement $\operatorname{Ker} u = \operatorname{Im} u$?

3. Soit $u \in \mathcal{L}(\mathrm{E})$ tel que $u^2 = 0$ et $u \neq 0$. On suppose qu'il existe $w \in \mathcal{L}(\mathrm{E})$ tel que $u \circ w + w \circ u = u$. A-t-on nécessairement $\operatorname{Ker} u = \operatorname{Im} u$?

(**École polytechnique**)

▷ **Solution.**

1.a. • Soit $x \in \mathrm{E}$. Comme $\mathrm{E} = \mathrm{S} \oplus \operatorname{Im} u$, il existe $(y, t) \in \mathrm{S} \times \operatorname{Im} u$ tel que $x = y + t$. Comme S est un supplémentaire de $\operatorname{Ker} u$, u induit un isomorphisme de S sur $\operatorname{Im} u$. Il existe donc $z \in \mathrm{S}$ tel que $t = u(z)$. On obtient donc $x = u + u(z)$, avec $(y, z) \in \mathrm{S}^2$.

• Cette écriture est unique. En effet, si $x = y' + u(z')$ avec $(y', z') \in \mathrm{S}^2$,

on a $y-y' = u(z'-z) \in \operatorname{Im} u \cap S$. D'où résultent $y-y' = 0$ et $z'-z \in \operatorname{Ker} u$. Il s'ensuit que $z'-z \in \operatorname{Im} u \cap S = \{0\}$. On a bien $y = y'$ et $z = z'$.

b. et **c.** • Montrons la linéarité de v et w. Soit x et x' deux vecteurs de E. Écrivons $x = y + u(z)$ et $x' = y' + u(z')$ avec $y = w(x)$, $y' = w(x')$, $z = v(x)$, $z' = v(x')$. Si $\lambda \in K$, on obtient

$$x + \lambda x' = y + u(z) + \lambda(y' + u(z')) = \underbrace{y + \lambda y'}_{\in S} + u(\underbrace{z + \lambda z'}_{\in S}),$$

puis, par unicité de l'écriture,

$$w(x+\lambda x') = y+\lambda y' = w(x)+\lambda w(x'), \quad v(x+\lambda x') = z+\lambda z' = v(x)+\lambda v(x').$$

Les applications v et w sont donc linéaires.

• On écrit $x = y + u(z)$ avec $(y, z) \in S^2$ et on calcule $(u \circ v + v \circ u)(x)$. On obtient

$$\begin{aligned}(u \circ v + v \circ u)(x) &= u(z) + v(u(x)) = u(z) + v(u(y)), \text{ car } u(z) \in \operatorname{Ker} u,\\ &= u(z) + y = x \text{ , par définition de } v \ (y \in S).\end{aligned}$$

On conclut que $\boxed{u \circ v + v \circ u = \mathrm{Id}_E}$.

• On calcule de même $(u \circ w + w \circ u)(x)$ et on obtient

$$\begin{aligned}(u \circ w + w \circ u)(x) &= u(y) + w(u(x)) = u(y) + w(u(y))\\ &= u(y) + 0, \text{ par définition de } w,\\ &= u(x - u(z)) = u(x), \text{ car } u(z) \in \operatorname{Ker} u.\end{aligned}$$

On conclut que $\boxed{u \circ w + w \circ u = u}$.

2. La réponse est affirmative. De $u^2 = 0$, on déduit $\operatorname{Im} u \subset \operatorname{Ker} u$. Si $x \in \operatorname{Ker} u$, on peut écrire $x = u(v(x)) + v(u(x)) = u(v(x)) \in \operatorname{Im} u$. On a donc $\operatorname{Ker} u = \operatorname{Im} u$.

3. Par contre ici, la réponse est négative. Considérons $u \in \mathcal{L}(\mathbb{R}^3)$ défini par $u(e_1) = 0$, $u(e_2) = 0$ et $u(e_3) = e_2$, où (e_1, e_2, e_3) désigne la base canonique de $\mathbb{R}^3$. Alors $\operatorname{Im} u$ est strictement incluse dans $\operatorname{Ker} u$ et pourtant si $w = \frac{1}{2}\,\mathrm{Id}_{\mathbb{R}^3}$, on a bien $u \circ w + w \circ u = u$. ◁

6.13. Endomorphismes u tels que $\operatorname{Ker} u \oplus \operatorname{Im} u = E$

> Soit E un K-espace vectoriel de dimension finie et $u \in \mathcal{L}(E)$. Trouver une condition nécessaire et suffisante sur u pour qu'il existe $v \in \mathcal{L}(E)$ tel que $u \circ v = 0$ et $u + v$ inversible.
>
> (**École polytechnique**)

▷ **Solution.**

• Analyse. Supposons que $v \in \mathcal{L}(E)$ réponde au problème posé. On

obtient $\operatorname{Im} v \subset \operatorname{Ker} u$ et donc $\operatorname{rg} v \leqslant n - \operatorname{rg} u$ et $n = \operatorname{rg}(u+v) \leqslant \operatorname{rg} u + \operatorname{rg} v$. On a donc $n = \operatorname{rg} u + \operatorname{rg} v$ et par suite $\operatorname{Im} v = \operatorname{Ker} u$, et $\operatorname{Im} u + \operatorname{Im} v = \mathrm{E}$ (car $\mathrm{E} = \operatorname{Im}(u+v) \subset \operatorname{Im} u + \operatorname{Im} v$) . Cette somme est directe et on conclut que

$$\boxed{\operatorname{Ker} u \oplus \operatorname{Im} u = \mathrm{E}}$$

• Réciproquement, supposons $\operatorname{Ker} u \oplus \operatorname{Im} u = \mathrm{E}$. Soit v le projecteur sur $\operatorname{Ker} u$ parallèlement à $\operatorname{Im} u$. On a évidemment $u \circ v = 0$. Montrons que de plus, $u + v \in \mathrm{GL}(\mathrm{E})$. Soit $x \in \mathrm{E}$ tel que $(u+v)(x) = 0$. On a alors $u(x) = -v(x) \in \operatorname{Ker} u \cap \operatorname{Im} u = \{0\}$. Donc $u(x) = v(x) = 0$ et $x \in \operatorname{Ker} u \cap \operatorname{Im} u = \{0\}$. On a donc $\operatorname{Ker}(u+v) = \{0\}$ et $u + v \in \mathrm{GL}(\mathrm{E})$.

Conclusion. Une condition nécessaire et suffisante d'existence de v est $\operatorname{Im} u \oplus \operatorname{Ker} u = \mathrm{E}$. ◁

L'exercice 6.15 donnera d'autres conditions équivalentes à celle-ci.

L'énoncé suivant établit des résultats importants qui sont à la base de la réduction de Jordan des endomorphismes nilpotents.

6.14. Décomposition de Fitting

Soit E un K-espace vectoriel de dimension finie n et u un endomorphisme de E.

1. Montrer que les suites $(\operatorname{Im} u^k)_{k\in\mathbb{N}}$ et $(\operatorname{Ker} u^k)_{k\in\mathbb{N}}$ sont d'abord strictement monotones pour l'inclusion puis constantes à partir d'un même rang $p \leqslant n$.

2. Montrer que la suite $(\operatorname{Ker} u^k)$ «s'essouffle», c'est-à-dire que la suite $(\dim \operatorname{Ker} u^{k+1} - \dim \operatorname{Ker} u^k)_{k\geqslant 0}$ est décroissante.

3. Démontrer que $\mathrm{E} = \operatorname{Ker} u^p \oplus \operatorname{Im} u^p$.

4. En déduire que toute matrice de $\mathcal{M}_n(\mathrm{K})$ est semblable à une matrice de la forme $\begin{pmatrix} \boxed{\mathrm{N}} & 0 \\ 0 & \boxed{\mathrm{C}} \end{pmatrix}$, où N est une matrice carrée nilpotente et C une matrice carrée inversible.

(École normale supérieure)

▷ **Solution.**

1. On a évidemment $\operatorname{Ker} u^k \subset \operatorname{Ker} u^{k+1}$ et $\operatorname{Im} u^{k+1} \subset \operatorname{Im} u^k$ pour tout entier naturel k. La suite $(\operatorname{Ker} u^k)_{k\in\mathbb{N}}$ est donc croissante pour l'inclusion et la suite $(\operatorname{Im} u^k)_{k\in\mathbb{N}}$ décroissante.

La suite d'entiers naturels $(\dim \operatorname{Ker} u^k)_{k\in\mathbb{N}}$ est croissante et majorée par n, donc est constante à partir d'un certain rang. La suite $(\operatorname{Ker} u^k)_{k\geqslant 0}$ est donc stationnaire. Soit p le plus petit entier tel que $\operatorname{Ker} u^p = \operatorname{Ker} u^{p+1}$. On montre que $\operatorname{Ker} u^{k+1} = \operatorname{Ker} u^k$, pour tout $k \geqslant p$. Soit $k \geqslant p$ et x dans $\operatorname{Ker} u^{k+1}$. Alors $u^{k-p}(x)$ est dans le noyau de u^{p+1}

et donc dans celui de u^p. Ainsi $u^p(u^{k-p}(x)) = u^k(x) = 0$ et $x \in \operatorname{Ker} u^k$. On a donc $\operatorname{Ker} u^{k+1} \subset \operatorname{Ker} u^k$ et donc $\operatorname{Ker} u^{k+1} = \operatorname{Ker} u^k$. La suite $(\operatorname{Ker} u^k)_{k \geqslant 0}$ est d'abord strictement croissante, puis constante à partir du rang p. En particulier, on a nécessairement $p \leqslant n$.

D'après le théorème du rang $\dim \mathrm{E} = \dim \operatorname{Ker} u^k + \dim \operatorname{Im} u^k$ pour tout k. Il en résulte que $\operatorname{rg} u^k - \operatorname{rg} u^{k+1} = \dim \operatorname{Ker} u^{k+1} - \dim \operatorname{Ker} u^k$ et donc que la suite des images est d'abord strictement décroissante, puis constante à partir du rang p.

2. La preuve la plus courte consiste à utiliser les espaces quotients (cf. p. 260 et 267 pour des rappels sur la question). On a, pour tout entier naturel k, $u(\operatorname{Ker} u^{k+2}) \subset \operatorname{Ker} u^{k+1}$ et $u(\operatorname{Ker} u^{k+1}) \subset \operatorname{Ker} u^k$. On en déduit que u induit une application linéaire $\overline{u}$ de $\operatorname{Ker} u^{k+2}/\operatorname{Ker} u^{k+1}$ dans $\operatorname{Ker} u^{k+1}/\operatorname{Ker} u^k$. Ces deux espaces vectoriels étant de dimensions respectives $\dim \operatorname{Ker} u^{k+2} - \dim \operatorname{Ker} u^{k+1}$ et $\dim \operatorname{Ker} u^{k+1} - \dim \operatorname{Ker} u^k$, il suffit pour conclure de montrer que $\overline{u}$ est injective. Soit $\overline{x} \in \operatorname{Ker} u^{k+2}/\operatorname{Ker} u^{k+1}$ tel que $\overline{u}(\overline{x}) = 0$. Cela signifie que $u(x) \in \operatorname{Ker} u^k$, donc que $x \in \operatorname{Ker} u^{k+1}$ et $\overline{x} = 0$.

Le lecteur qui veut éviter l'utilisation des quotients pourra rédiger la solution en introduisant un supplémentaire H de $\operatorname{Ker} u^{k+1}$ dans $\operatorname{Ker} u^{k+2}$ et montrer que la restriction de u à H est une injection de H sur un sous-espace de $\operatorname{Ker} u^{k+1}$ qui est en somme directe avec $\operatorname{Ker} u^k$.

3. D'après le théorème du rang, il suffit de montrer la somme est directe. Soit $y \in \operatorname{Ker} u^p \cap \operatorname{Im} u^p$ et $x \in \mathrm{E}$ tel que $y = u^p(x)$. On a alors $u^p(y) = u^{2p}(x) = 0$ donc $x \in \operatorname{Ker} u^{2p} = \operatorname{Ker} u^p$. Par conséquent, $y = u^p(x) = 0$. La somme est bien directe et

$$\boxed{\mathrm{E} = \operatorname{Ker} u^p \oplus \operatorname{Im} u^p}.$$

4. Soit $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$. On applique le résultat précédent à l'endomorphisme de K^n canoniquement associé à A. L'entier p étant défini à partir de cet endomorphisme comme dans la question 1, on a l'égalité $\mathrm{K}^n = \operatorname{Im} \mathrm{A}^p \oplus \operatorname{Ker} \mathrm{A}^p$. Les sous-espaces $\mathrm{F} = \operatorname{Ker} \mathrm{A}^p$ et $\mathrm{G} = \operatorname{Im} \mathrm{A}^p$ sont stables par A, car on a $\mathrm{A}(\operatorname{Ker} \mathrm{A}^p) \subset \operatorname{Ker} \mathrm{A}^{p-1} \subset \operatorname{Ker} \mathrm{A}^p$ et $\mathrm{A}(\operatorname{Im} \mathrm{A}^p) = \operatorname{Im} \mathrm{A}^{p+1} = \operatorname{Im} \mathrm{A}^p$. La matrice de A dans une base de K^n obtenue par juxtaposition d'une base de $\operatorname{Ker} \mathrm{A}^p$ et d'une base de $\operatorname{Im} \mathrm{A}^p$ est de la forme $\begin{pmatrix} \boxed{\mathrm{N}} & 0 \\ 0 & \boxed{\mathrm{C}} \end{pmatrix}$, où N et C sont des matrices carrées. La restriction de A à $\operatorname{Ker} \mathrm{A}^p$ est nilpotente d'indice p et la restriction de A à $\operatorname{Im} \mathrm{A}^p$ est surjective (car $\mathrm{A}(\operatorname{Im} \mathrm{A}^p) = \operatorname{Im} \mathrm{A}^p$), donc bijective. Ainsi, N est nilpotente et C inversible. $\lhd$

L'exercice qui suit fournit diverses caractérisations des endomorphismes pour lesquels $p = 2$.

6.15. Endomorphismes tels que $E = \operatorname{Ker} u \oplus \operatorname{Im} u$

Soit E de dimension finie sur K et $u \in \mathcal{L}(E)$.

1. Montrer qu'il y a équivalence entre :

(i) $\operatorname{Ker} u = \operatorname{Ker} u^2$;

(ii) $\operatorname{Im} u = \operatorname{Im} u^2$;

(iii) $E = \operatorname{Ker} u \oplus \operatorname{Im} u$.

2. Donner des exemples d'endomorphismes vérifiant ces conditions.

3. Le résultat subsiste-il en dimension infinie ?

(**École polytechnique**)

▷ **Solution.**

1. Notons que l'on a $\operatorname{Im} u^2 \subset \operatorname{Im} u$ et $\operatorname{Ker} u \subset \operatorname{Ker} u^2$, pour tout $u \in \mathcal{L}(E)$. En dimension finie, les propositions (i) et (ii) sont donc équivalentes puisque d'après le théorème du rang

$$\dim(\operatorname{Ker} u) + \dim(\operatorname{Im} u) = \dim(\operatorname{Ker} u^2) + \dim(\operatorname{Im} u^2) = \dim(E).$$

• Supposons (i) et montrons (iii). Soit $y \in \operatorname{Im} u \cap \operatorname{Ker} u$. Il existe $x \in E$ tel que $y = u(x)$. Comme $u(y) = 0$, on a $u^2(x) = 0$ et $x \in \operatorname{Ker} u^2 = \operatorname{Ker} u$. Ainsi $y = u(x) = 0$. Donc $\operatorname{Im} u$ et $\operatorname{Ker} u$ sont en somme directe. Comme le théorème du rang assure que $\dim \operatorname{Im} u + \dim \operatorname{Ker} u = \dim E$, on conclut que $E = \operatorname{Ker} u \oplus \operatorname{Im} u$.

• Supposons (iii) et montrons (ii). Soit $y \in \operatorname{Im} u$ et $x \in E$ tel que $u(x) = y$. Par hypothèse, x s'écrit $x = x' + x''$ avec $x' \in \operatorname{Im} u$ et $x'' \in \operatorname{Ker} u$. Il existe donc $z \in E$ tel que $x' = u(z)$ et $x = u(z) + x''$. D'où $y = u(u(z)) + u(x'') = u^2(z) \in \operatorname{Im} u^2$. On a donc $\operatorname{Im} u \subset \operatorname{Im} u^2$ et finalement (ii), puisque l'autre inclusion est toujours vérifiée.

Cela montre donc l'équivalence entre les trois propositions.

2. Tout projecteur, tout isomorphisme de E, tout endomorphisme diagonalisable vérifie ces conditions.

3. En dimension infinie, les trois propriétés ne sont pas équivalentes.

• Considérons $E = \mathbb{R}[X]$ et prenons comme endomorphisme u de E la dérivation. Comme u est surjective, $\operatorname{Im} u = \operatorname{Im} u^2 = E$: (ii) est vérifié. En revanche, $\operatorname{Ker} u = \mathbb{R}_0[X]$ et $\operatorname{Ker} u^2 = \mathbb{R}_1[X]$: (i) n'est pas vérifié. La propriété (iii) ne l'est pas non plus car $\operatorname{Ker} u \subset \operatorname{Im} u$ et $\operatorname{Ker} u \neq \{0\}$.

• Soit v l'endomorphisme $P \longmapsto XP$ de E. On a $\operatorname{Ker} v = \operatorname{Ker} v^2 = \{0\}$, $\operatorname{Im} v^2 = X^2\mathbb{R}[X] \neq \operatorname{Im} v = X\mathbb{R}[X]$: cette fois la condition (i) est remplie mais ni (ii), ni (iii) ne sont vérifiées.

• Par contre on peut remarquer qu'en dimension quelconque, (iii) est équivalent à (i) et (ii).

⋆ Supposons (i) et (ii). Comme précédemment, on montre que la somme $\operatorname{Ker} u + \operatorname{Im} u$ est directe. Montrons avec (ii) qu'elle fait E tout

entier. Si $x \in E$, alors $u(x) \in \operatorname{Im} u = \operatorname{Im} u^2$ et il existe $y \in E$ tel que $u(x) = u^2(y)$. On en déduit que $u(x - u(y)) = 0$ et $x - u(y) \in \operatorname{Ker} u$. On obtient finalement $x \in \operatorname{Im} u + \operatorname{Ker} u$ et $E = \operatorname{Ker} u \oplus \operatorname{Im} u$.

$\star$ Si (*iii*) est vérifié, on a déjà montré que $\operatorname{Im} u = \operatorname{Im} u^2$. Soit x dans $\operatorname{Ker} u^2$. On a $u(u(x)) = 0$, c'est-à-dire $u(x) \in \operatorname{Im} u \cap \operatorname{Ker} u = \{0\}$. On en déduit que $x \in \operatorname{Ker} u$. On a montré que $\operatorname{Ker} u^2 \subset \operatorname{Ker} u$ et donc $\operatorname{Ker} u^2 = \operatorname{Ker} u$. $\triangleleft$

Dans l'énoncé suivant on détermine de manière très élémentaire les puissances d'un endomorphisme diagonalisable ayant deux valeurs propres.

6.16. Endomorphisme annulé par un polynôme de degré 2 à racines simples

Soit E un K-espace vectoriel de dimension finie et $f \in \mathcal{L}(E)$ vérifiant $(f - a\,\mathrm{Id})(f - b\,\mathrm{Id}) = 0$ où a et b sont deux éléments distincts de K.

1. Établir l'existence de λ et μ non nuls tels que $\lambda(f - a\,\mathrm{Id})$ et $\mu(f - b\,\mathrm{Id})$ soient des projecteurs.

2. Montrer que $\operatorname{Im}(f - b\,\mathrm{Id}) = \operatorname{Ker}(f - a\,\mathrm{Id})$.

3. Calculer f^n pour tout $n \in \mathbb{N}$.

4. Si $ab \neq 0$, montrer que $f \in \mathrm{GL}(E)$, et calculer f^n pour $n \in \mathbb{Z}$.

(**École polytechnique**)

$\triangleright$ **Solution.**

1. On a par hypothèse $f^2 - (a + b)f + ab\,\mathrm{Id} = 0$. Si $\lambda \in K^*$, il suffit, pour que $\lambda(f - a\,\mathrm{Id})$ soit un projecteur, que $[\lambda(f - a\,\mathrm{Id})]^2 = \lambda(f - a\,\mathrm{Id})$. C'est le cas dès que $\lambda(f^2 - 2af + a^2\,\mathrm{Id}) = f - a\,\mathrm{Id}$. En remplaçant f^2 par $(a + b)f - ab\,\mathrm{Id}$, on obtient

$$\lambda\,[(b - a)f - a(a - b)\,\mathrm{Id}] = f - a\,\mathrm{Id}\,.$$

Comme $a \neq b$, cette identité est vérifiée pour $\boxed{\lambda = \dfrac{1}{b - a}}$ et dans ce cas, $\lambda(f - a\,\mathrm{Id})$ est un projecteur. Par symétrie du problème, $\mu(f - b\,\mathrm{Id})$ est un projecteur pour $\boxed{\mu = \dfrac{1}{a - b}}$.

2. Comme $(f - a\,\mathrm{Id})(f - b\,\mathrm{Id}) = 0$, on a $\operatorname{Im}(f - b\,\mathrm{Id}) \subset \operatorname{Ker}(f - a\,\mathrm{Id})$. Réciproquement, si $x \in \operatorname{Ker}(f - a\,\mathrm{Id})$, on a $f(x) = ax$, d'où l'on déduit que $f(x) - bx = (a - b)x$ et donc $x = \dfrac{1}{b - a}(f(x) - bx) \in \operatorname{Im}(f - b\,\mathrm{Id})$. On conclut que $\operatorname{Im}(f - b\,\mathrm{Id}) = \operatorname{Ker}(f - a\,\mathrm{Id})$.

3. Écrivons le reste de la division euclidienne de X^n par $(X-a)(X-b)$ sous la forme $\alpha(X-a)+\beta(X-b)$ avec $(\alpha,\beta)\in K^2$ (c'est possible car $a\neq b$). On note Q le quotient. En substituant a, puis b à X, il vient

$$a^n=\beta(a-b)\quad\text{et}\quad b^n=\alpha(b-a).$$

En substituant f à X, on obtient

$$\begin{aligned}f^n&=Q(f)(f-a\,\mathrm{Id})(f-b\,\mathrm{Id})+\alpha(f-a\,\mathrm{Id})+\beta(f-b\,\mathrm{Id})\\&=\alpha(f-a\,\mathrm{Id})+\beta(f-b\,\mathrm{Id})\end{aligned}$$

et donc

$$\boxed{f^n=\frac{1}{b-a}\left(b^n(f-a\,\mathrm{Id})-a^n(f-b\,\mathrm{Id})\right)}.$$

4. • Si $ab\neq 0$, l'égalité $f^2-(a+b)f+ab\,\mathrm{Id}=0$ devient

$$f\left[\frac{1}{ab}\left((a+b)\,\mathrm{Id}-f\right)\right]=\mathrm{Id}$$

et f est donc un isomorphisme de E.

• On pose $g=f^{-1}$. À partir de l'égalité $(f-a\,\mathrm{Id})(f-b\,\mathrm{Id})=0$, on obtient l'égalité $(g-a'\,\mathrm{Id})(g-b'\,\mathrm{Id})=0$, où $a'=\dfrac{1}{a}$ et $b'=\dfrac{1}{b}$. C'est une condition analogue à celle vérifiée par f. De la question précédente, on déduit que, pour $n\geqslant 1$,

$$\begin{aligned}g^n&=\frac{1}{b'-a'}\left(b'^n(g-a'\,\mathrm{Id})-a'^n(g-b'\,\mathrm{Id})\right)\\&=f^{-1}\frac{1}{a-b}\left(b^{-n+1}(a\,\mathrm{Id}-f)-a^{-n+1}(b\,\mathrm{Id}-f)\right),\end{aligned}$$

puis, en multipliant par f

$$f^{1-n}=(f^{-1})^{n-1}=\frac{1}{b-a}\left(b^{1-n}(f-a\,\mathrm{Id})-a^{1-n}(f-b\,\mathrm{Id})\right).$$

On trouve la même formule pour les exposants négatifs que pour $n\geqslant 0$. Finalement, on obtient, pour $n\in\mathbb{Z}$,

$$\boxed{f^n=\frac{1}{b-a}\left(b^n(f-a\,\mathrm{Id})-a^n(f-b\,\mathrm{Id})\right)}.\quad\triangleleft$$

6.17. Équation linéaire dans $\mathcal{L}(E)$

Soit E un K-espace vectoriel.

1. Soit $(f,g) \in \mathcal{L}(E)^2$ tel que $f \circ g - g \circ f = \mathrm{Id}$. Vérifier que, pour tout $P \in K[X]$, on a $f \circ P(g) - P(g) \circ f = P'(g)$. Si K est un sous-corps de $\mathbb{C}$, montrer que $(g^n)_{n \geqslant 0}$ est une famille libre.

2. Donner, lorsque $K = \mathbb{R}$ et $E = \mathbb{R}[X]$, un exemple d'endomorphismes f et g de E vérifiant $f \circ g - g \circ f = \mathrm{Id}$.

3. On suppose que $K = \mathbb{Z}/p\mathbb{Z}$, où p est un nombre premier, et que E est de dimension p. Soit $(e_1, e_2, \ldots, e_p)$ une base de E et $g \in \mathcal{L}(E)$ tel que $g(e_i) = e_{i+1}$ si $1 \leqslant i \leqslant p-1$ et $g(e_p) = 0$.

Déterminer les endomorphismes f de E tels que $f \circ g - g \circ f = \mathrm{Id}$.

(École polytechnique)

▷ **Solution.**

1. Par linéarité, il suffit de prouver le résultat pour $P = X^n$. Procédons par récurrence sur $n \in \mathbb{N}$.

- C'est trivial si $n = 0$, c'est l'hypothèse pour $n = 1$.
- Supposons $n \geqslant 2$. D'après l'hypothèse de récurrence, on a

$$f \circ g^{n-1} - g^{n-1} \circ f = (n-1)g^{n-2}.$$

Composant à droite par g, on obtient

$$\begin{aligned}(n-1)g^{n-1} &= f \circ g^n - g^{n-1} \circ f \circ g = f \circ g^n - g^{n-1} \circ (g \circ f + \mathrm{Id}) \\ &= f \circ g^n - g^n \circ f - g^{n-1},\end{aligned}$$

c'est-à-dire $f \circ g^n - g^n \circ f = ng^{n-1}$.

Montrons en raisonnant par l'absurde que la famille $(g^n)_{n \geqslant 0}$ est libre. Supposons qu'est liée. Il existe donc $P \in K[X]$, non nul, tel que $P(g) = 0$. Choisissons P de degré minimal ; on a nécessairement $\deg P \geqslant 1$, car g n'est pas nul. Alors, il résulte de la formule que nous venons d'établir que

$$P'(g) = f \circ P(g) - P(g) \circ f = 0.$$

Or $P' \neq 0$ (ou est sur un sous-corps de $\mathbb{C}$) et $\deg P' < \deg P$, ce qui contredit la minimalité de $\deg P$. Donc $(g^n)_{n \geqslant 0}$ est libre.

En particulier, si K *est un sous-corps de* $\mathbb{C}$ *(ou plus généralement un corps de caractéristique nulle), l'équation* $f \circ g - g \circ f = \mathrm{Id}$ *n'a pas de solution si* E *est de dimension finie. On peut aussi voir cela à l'aide de la trace : si* $\dim E = n$, $\mathrm{Tr}(\mathrm{Id}) = n$ *mais* $\mathrm{Tr}(f \circ g - g \circ f) = 0$.

2. Il s'agit de trouver f et g vérifiant

$$f \circ g = g \circ f + \mathrm{Id}.$$

Or si $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$, on a $(\mathrm{XP})' = \mathrm{XP}' + \mathrm{P}$. Il suffit donc de prendre

$$f : \mathrm{P} \longmapsto \mathrm{P}' \quad \text{et} \quad g : \mathrm{X} \longmapsto \mathrm{XP}.$$

3. L'équation d'inconnue $f \in \mathcal{L}(\mathrm{E})$ est en fait une équation linéaire. Si f_0 est une solution particulière, on obtient les autres en additionnant à f_0 une solution de l'équation homogène $f \circ g - g \circ f = 0$. Or le sous-espace des solutions de l'équation homogène est $\mathcal{C}(g)$, le commutant de g. On va donc chercher une solution particulière, puis déterminer le commutant de g.

• Si f est solution, on obtient $g(f(e_p)) = f(g(e_p)) - e_p = -e_p$. C'est le cas par exemple si $f(e_p) = -e_{p-1}$. On obtient ensuite

$$g(f(e_{p-1})) = f(g(e_{p-1})) - e_{p-1} = f(e_p) - e_{p-1} = -2e_{p-1}.$$

On peut choisir $f(e_{p-1}) = -2e_{p-2}$. En continuant, on constate que

$$f(e_i) = -(p-i+1)e_{i-1} = (i-1)e_{i-1} \text{ pour } 2 \leqslant i \leqslant p \quad \text{et} \quad f(e_1) = 0$$

est un bon choix.

Procédons à la synthèse. Soit donc $f_0 \in \mathcal{L}(\mathrm{E})$ défini, pour $1 \leqslant i \leqslant p$, par $f_0(e_i) = (i-1)e_{i-1}$. Vérifions que f_0 convient. On obtient, pour tout $1 \leqslant i \leqslant p-1$,

$$(f_0 \circ g - g \circ f_0)(e_i) = f_0(e_{i+1}) - g((i-1)e_{i-1}) = ie_i - (i-1)e_i = e_i$$

et

$$(f_0 \circ g - g \circ f_0)(e_p) = -g(f_0(e_p)) = -g((p-1)e_{p-1}) = -(p-1)e_p = e_p,$$

car dans $\mathbb{Z}/p\mathbb{Z}$, $-(p-1) = 1$. On a donc $f_0 \circ g - g \circ f_0 = \mathrm{Id}$.

• Déterminons le commutant $\mathcal{C}(g)$ de g. Les initiés auront reconnu en g un endomorphisme cyclique. En effet, la famille $(e_1, g(e_1), \ldots, g^{p-1}(e_1))$, c'est-à-dire $(e_1, e_2, \ldots, e_p)$ est une base de E. Le commutant de g est alors confondu avec $\mathrm{K}[g] = \{\mathrm{P}(g), \mathrm{P} \in \mathrm{K}[\mathrm{X}]\}$. Redémontrons ce résultat. On a déjà clairement $\mathrm{K}[g] \subset \mathcal{C}(g)$. Inversement, montrons que si $f \in \mathcal{C}(g)$, il existe un unique $(\lambda_0, \ldots, \lambda_{p-1}) \in \mathrm{K}^p$ tel que

$$f = \lambda_0 \,\mathrm{Id} + \lambda_1 g + \cdots + \lambda_{p-1} g^{p-1}. \tag{1}$$

En appliquant à e_1, on obtient

$$f(e_1) = \lambda_0 e_1 + \lambda_1 e_2 + \cdots + \lambda_{p-1} e_p. \tag{2}$$

Cette dernière égalité définit $(\lambda_0, \ldots, \lambda_p)$ de manière unique. Il s'agit de démontrer que l'égalité (1) est réalisée pour cette valeur de $(\lambda_0, \ldots, \lambda_p)$.

Il suffit de le vérifier pour les vecteurs de $e_1, g(e_1), \ldots, g_{p-1}(e_1))$ de E, c'est-à-dire de montrer que, pour $0 \leqslant i \leqslant p-1$,

$$\begin{aligned} f(g^i(e_1)) &= \lambda_0 g^i(e_1) + \lambda_1 g^{i+1}(e_1) + \cdots + \lambda_{p-1} g^{i+p-1}(e_1) \\ &= \lambda_0 g^i(e_1) + \cdots + \lambda_{p-1} g^i(e_p). \end{aligned}$$

Nous savons que c'est vrai pour $i = 0$; c'est l'égalité (2). En calculant l'image par g^i des deux membres de l'égalité (2) et en tenant compte du fait que f commute avec g donc avec g^i, on obtient

$$\begin{aligned} f(g^i(e_1)) = g^i(f(e_1)) &= g^i(\lambda_0 e_1 + \lambda_1 e_2 + \cdots + \lambda_{p-1} e_p) \\ &= \lambda_0 g^i(e_1) + \cdots + \lambda_{p-1} g^i(e_p). \end{aligned}$$

On obtient donc que f est dans $\mathrm{Vect}(\mathrm{Id}, g, \ldots, g^{p-1})$.

Nous avons démontré les inclusions

$$\mathcal{C}(g) \subset \mathrm{Vect}(\mathrm{Id}, g, \ldots, g^{p-1}) \subset \mathrm{K}[g] \subset \mathcal{C}(g),$$

qui sont donc des égalités. L'unicité de $(\lambda_0, \ldots, \lambda_p)$ pour tout $f \in \mathcal{C}(g)$ montre que $(\mathrm{Id}, g, \ldots, g^{p-1})$ est une base de $\mathcal{C}(g)$ qui est donc de dimension p.

Conclusion. L'ensemble des f qui conviennent est

$$f_0 + \mathrm{Vect}(\mathrm{Id}, g, \ldots, g^{p-1}). \lhd$$

Voici quelques exercices consacrés aux projecteurs. On rappelle que les projecteurs sont les idempotents de l'algèbre $\mathcal{L}(\mathrm{E})$, c'est-à-dire les endomorphismes p vérifiant $p^2 = p$. Leur importance provient des rapports étroits qu'ils entretiennent avec les décompositions de E *en somme directe de sous-espaces.*

6.18. Projecteurs

> Soit p et q deux projecteurs d'un espace vectoriel E tels que $\mathrm{Im}\, p \subset \mathrm{Ker}\, q$ et $r = p + q - pq$. Montrer que r est un projecteur et trouver son image et son noyau.
>
> **(École polytechnique)**

$\rhd$ **Solution.**

- Comme $\mathrm{Im}\, p \subset \mathrm{Ker}\, q$, on a $qp = 0$. On en déduit que

$$\begin{aligned} r^2 &= (p + q - pq)(p + q - pq) \\ &= p^2 + pq - p^2 q + qp + q^2 - qpq - pqp - pq^2 + pqpq \\ &= p + pq - pq + q - pq = r. \end{aligned}$$

et r est bien un projecteur de E.

• On a $pr = p^2 = p$ de sorte que $\operatorname{Ker} r \subset \operatorname{Ker} p$. De même $qr = q^2 = q$ et $\operatorname{Ker} r \subset \operatorname{Ker} q$. Ainsi, $\operatorname{Ker} r \subset \operatorname{Ker} p \cap \operatorname{Ker} q$. L'autre inclusion étant évidente, on en déduit que

$$\boxed{\operatorname{Ker} r = \operatorname{Ker} p \cap \operatorname{Ker} q}.$$

• L'image de r est clairement incluse dans $\operatorname{Im} p + \operatorname{Im} q$. Réciproquement, soit $x \in \operatorname{Im} p + \operatorname{Im} q$ que l'on écrit $x = x_1 + x_2$ avec $x_1 \in \operatorname{Im} p$ et $x_2 \in \operatorname{Im} q$. On a $q(x) = q(x_1) + q(x_2) = q(x_2) = x_2$ car $\operatorname{Im} p \subset \operatorname{Ker} q$. Ainsi, on obtient

$$r(x) = p(x) + q(x) - pq(x) = x_1 + p(x_2) + x_2 - p(x_2) = x_1 + x_2 = x.$$

Il en résulte que $x \in \operatorname{Im} r$, et on a finalement, la somme étant directe car $\operatorname{Im} p \subset \operatorname{Ker} q$,

$$\boxed{\operatorname{Im} r = \operatorname{Im} p \oplus \operatorname{Im} q}. \quad \triangleleft$$

Soit p un projecteur d'un K*-espace vectoriel de dimension finie. Si* K *est de caractéristique nulle la trace de p est égale*[1] *au rang de p. En fait, on a de manière générale,* $\operatorname{Tr} p = (\operatorname{rg} p)1_{\mathrm{K}}$ *où* 1_{K} *est l'élément unité de* K. *Pour s'en convaincre, il suffit d'écrire la matrice de p dans une base obtenue par réunion d'une base de* $\operatorname{Im} p$ *et une base de* $\operatorname{Ker} p$.

6.19. Une somme de projecteurs

Soit E un K-espace vectoriel de dimension finie n, K sous-corps de $\mathbb{C}$. On se donne n endomorphismes non nuls de E, $p_1, p_2, \ldots, p_n$ tels que, pour $1 \leqslant i, j \leqslant n$, $p_i \circ p_j = \delta_{i,j} p_i$.

1. Montrer que pour $1 \leqslant i \leqslant n$, $\operatorname{rg} p_i = 1$.

2. Montrer que les sous espaces $\operatorname{Im} p_i$, pour $1 \leqslant i \leqslant n$, sont en somme directe.

(École polytechnique)

▷ **Solution.**

1. Pour tout i, on a $p_i^2 = p_i$, donc p_i est un projecteur. Considérons la somme $p = p_1 + \cdots + p_n$. D'après l'hypothèse, on a

$$p^2 = \sum_{1 \leqslant i, j \leqslant n} p_i \circ p_j = \sum_{i=1}^{n} p_i^2 = \sum_{i=1}^{n} p_i = p$$

1. La trace de p est un élément de K et le rang de p est dans $\mathbb{N}$. Mais si K est de caractéristique nulle, on peut identifier $\mathbb{Q}$ à un sous-corps de K, ce qui est implicitement fait ici.

et p est aussi un projecteur. Comme le rang d'un projecteur n'est autre que sa trace, on a $\operatorname{rg} p = \operatorname{Tr} p = \sum_{i=1}^{n} \operatorname{Tr} p_i = \sum_{i=1}^{n} \operatorname{rg} p_i \geqslant n$, puisque les p_i sont non nuls. Donc nécessairement, $\operatorname{rg} p = \sum_{i=1}^{n} \operatorname{rg} p_i = n$, ce qui signifie que $p = \mathrm{Id}_{\mathrm{E}}$ et pour chaque i, $\operatorname{rg} p_i = 1$.

2. Montrons que les sous-espaces $\operatorname{Im} p_i$ sont en somme directe. On a

$$\mathrm{E} = \mathrm{Id}_{\mathrm{E}}(\mathrm{E}) = (p_1 + \cdots + p_n)(\mathrm{E}) \subset p_1(\mathrm{E}) + \cdots + p_n(\mathrm{E})$$

et donc $\mathrm{E} = \sum_{i=1}^{n} \operatorname{Im} p_i$. Chaque $\operatorname{Im} p_i$ est une droite et comme on a de plus $\dim \mathrm{E} = \sum_{i=1}^{n} \dim \operatorname{Im} p_i$, les images sont bien en somme directe ; c'est une conséquence du lemme suivant.

Lemme. *Soit* E *un sous-espace de dimension finie,* $(\mathrm{F}_1, \ldots, \mathrm{F}_p)$ *une famille de sous-espaces de* E. *Alors on a l'équivalence*

$$\mathrm{F}_1 + \cdots + \mathrm{F}_p \text{ est directe } \Longleftrightarrow \dim(\mathrm{F}_1 + \cdots + \mathrm{F}_p) = \sum_{k=1}^{p} \dim \mathrm{F}_k \,.$$

Démonstration. On introduit l'application linéaire

$$f : \begin{array}{ccc} \mathrm{F}_1 \times \mathrm{F}_2 \times \cdots \times \mathrm{F}_p & \longrightarrow & \mathrm{F}_1 + \mathrm{F}_2 + \cdots + \mathrm{F}_p \\ (x_1, x_2, \ldots, x_p) & \longmapsto & x_1 + x_2 + \cdots + x_p \end{array}$$

Elle est surjective. Dire que la somme $\mathrm{F}_1 + \cdots + \mathrm{F}_p$ est directe, c'est dire que f est injective ou encore que $\dim \operatorname{Ker} f = 0$, ou encore, d'après le théorème du rang que

$$\dim(\mathrm{F}_1 + \cdots + \mathrm{F}_p) = \dim(\mathrm{F}_1 \times \cdots \times \mathrm{F}_p) = \dim \mathrm{F}_1 + \cdots + \dim \mathrm{F}_p \,. \diamondsuit$$

Si dans l'exercice suivant, il est question de projecteurs de $\mathbb{C}[\mathrm{X}]$, *on s'intéresse surtout à la recherche de sous-espaces stables par certains endomorphismes.*

6.20. Endomorphismes de $\mathbb{C}[\mathrm{X}]$

Pour $\mathrm{Q} \in \mathbb{C}[\mathrm{X}]$, non nul, soit $\pi_{\mathrm{Q}} : \mathbb{C}[\mathrm{X}] \longmapsto \mathbb{C}[\mathrm{X}]$ l'application qui à P fait correspondre le reste de la division euclidienne de P par Q.

1. Montrer que, pour tout polynôme Q non nul, π_{Q} est un projecteur. Déterminer son image et son noyau.

2. Montrer que si Q_1 et Q_2 sont deux polynômes non nuls, on a, pour tout $P \in \mathbb{C}[X]$, $\pi_{Q_1Q_2}(Q_1P) = Q_1\pi_{Q_2}(P)$.

On fixe $Q \in \mathbb{C}[X]$, non nul, et on considère $S_Q : \mathbb{C}[X] \longmapsto \mathbb{C}[X]$ application définie par $S_Q(P) = \pi_Q(XP)$.

On dit qu'un sous-espace M de $\mathbb{C}[X]$ est stable si $S_Q(M) \subset M$, qu'il est invariant si $S_Q(M) = M$.

3. Montrer que si $Q = Q_1Q_2$, alors $Q_1 \operatorname{Im} \pi_{Q_2}$ est stable. À quelle condition est-il invariant ?

4. Soit N un sous-espace stable et $M = N + Q\,\mathbb{C}[X]$. Montrer que M est de la forme $Q_1\,\mathbb{C}[X]$.

5. Soit N un sous-espace invariant. Montrer qu'il existe Q_1 et Q_2 tels que $Q = Q_1Q_2$ et $N = Q_1 \operatorname{Im} \pi_{Q_2}$.

(**École polytechnique**)

▷ **Solution.**

1. Montrons que π_Q est linéaire. Notons n le degré de Q. Considérons P et P′ dans $\mathbb{C}[X]$, λ et λ' dans $\mathbb{C}$. Par définition, il existe P_1 et P'_1 dans $\mathbb{C}[X]$ tels que

$$\begin{cases} P = QP_1 + \pi_Q(P) \\ P' = QP'_1 + \pi_Q(P'). \end{cases}$$

On en déduit que $\lambda P + \lambda' P' = Q(\lambda P_1 + \lambda' P'_1) + (\lambda \pi_Q(P) + \lambda' \pi_Q(P'))$. Les polynômes $\pi_Q(P)$ et $\pi_Q(P')$ appartiennent à $\mathbb{C}_{n-1}[X]$. Il en est de même de $\lambda\pi_Q(P) + \lambda'\pi_Q(P')$. De l'unicité de la division euclidienne de $\lambda P + \lambda' P'$ par Q, il résulte que

$$\pi_Q(\lambda P + \lambda' P') = \lambda \pi_Q(P) + \lambda' \pi_Q(P'),$$

ce qui montre la linéarité de π_Q.

Pour tout $P \in \mathbb{C}[X]$, on a $\pi_Q(P) \in \mathbb{C}_{n-1}[X]$. La division euclidienne de $\pi_Q(P)$ par Q s'écrit donc $\pi_Q(P) = Q \times 0 + \pi_Q(P)$. On en déduit que $\pi_Q(\pi_Q(P)) = \pi_Q(P)$. On conclut que $\pi_Q \circ \pi_Q = \pi_Q$: π_Q est un projecteur.

On a clairement $\pi_Q(P) = 0$ si et seulement si Q divise P. Autrement dit, on a $\operatorname{Ker} \pi_Q = Q\,\mathbb{C}[X]$. Il est évident que $\operatorname{Im} \pi_Q = \mathbb{C}_{n-1}[X]$.

2. On effectue la division euclidienne de P par Q_2. Il existe $P_1 \in \mathbb{C}[X]$ tel que $P = Q_2P_1 + \pi_{Q_2}(P)$. On en déduit $Q_1P = Q_1Q_2P_1 + Q_1\pi_{Q_2}(P)$. Le polynôme $\pi_{Q_2}(P)$ est de degré strictement inférieur à celui de Q_2. On en déduit que le degré de $Q_1\pi_{Q_2}(P)$ est degré strictement inférieur au degré de Q_1Q_2. On a donc affaire à la division euclidienne de Q_1P par Q_1Q_2. On en déduit l'égalité $\pi_{Q_1Q_2}(Q_1P) = Q_1\pi_{Q_2}(P)$.

3. Soit $Q_1\pi_{Q_2}(P)$ un élément quelconque de $Q_1 \operatorname{Im} \pi_{Q_2}$. On a, d'après la question 2,

$$S_Q(Q_1\pi_{Q_2}(P)) = \pi_Q(XQ_1\pi_{Q_2}(P)) = Q_1\pi_{Q_2}(X\pi_{Q2}(P)).$$

On obtient $S_Q(Q_1 \operatorname{Im} \pi_{Q_2}) = Q_1\pi_{Q_2}(X \operatorname{Im} \pi_{Q_2}) \subset Q_1 \operatorname{Im} \pi_{Q_2}$: $Q_1 \operatorname{Im} \pi_{Q_2}$ est stable. De plus, il est invariant si $\pi_{Q_2}(X \operatorname{Im} \pi_{Q_2}) = \operatorname{Im} \pi_{Q_2}$.

Si le polynôme Q_2 est premier avec X, on obtient, pour tout $P \in \mathbb{C}[X]$,

$$\begin{aligned}\pi_{Q_2}(X\pi_{Q2}(P)) = 0 &\Longrightarrow Q_2 \text{ divise } X\pi_{Q2}(P) \Longrightarrow Q_2 \text{ divise } \pi_{Q2}(P)\\ &\Longrightarrow \pi_{Q^2}(P) = 0.\end{aligned}$$

La restriction de π_{Q_2} à $X \operatorname{Im} \pi_{Q_2}$ est injective. On a donc

$$\dim \pi_{Q_2}(X \operatorname{Im} \pi_{Q_2}) = \dim(X \operatorname{Im} \pi_{Q_2}) = \dim(\operatorname{Im} \pi_{Q_2}),$$

ce qui avec l'inclusion déjà démontrée, permet de conclure que

$$\pi_{Q_2}(X \operatorname{Im} \pi_{Q_2}) = \operatorname{Im} \pi_{Q_2} : Q_1 \operatorname{Im} \pi_{Q_2} \text{ est invariant.}$$

Par contre si X divise Q_2, on écrit $Q_2 = XQ_2'$ et on obtient, d'après la question 2,

$$\pi_{Q_2}(X\pi_{Q_2}(P)) = \pi_{XQ_2'}(X\pi_{Q_2}(P)) = X\pi_{Q_2'}(\pi_{Q_2}(P)).$$

Ce polynôme est toujours divisible par X. On n'obtient pas ainsi $\operatorname{Im} \pi_{Q_2}$ en entier. Le sous-espace vectoriel $Q_1 \operatorname{Im} \pi_{Q_2}$ n'est pas invariant.

4. L'anneau $\mathbb{C}[X]$ étant principal, pour démontrer que M s'écrit $Q_1\mathbb{C}[X]$, il suffit de démontrer que c'est un idéal de $\mathbb{C}[X]$. C'est déjà clairement un sous-groupe additif, puisqu'un sous-espace vectoriel. En effet, c'est la somme de deux sous-espaces vectoriels de $\mathbb{C}[X]$.

Il reste à montrer que si $P \in M$ et $R \in \mathbb{C}[X]$, alors $PR \in M$. Le sous-espace M étant somme de N et de $Q\mathbb{C}[X]$, il suffit de le démontrer pour $P \in N$ et pour $P \in Q\mathbb{C}[X]$. Or, il est clair que si $P \in Q\mathbb{C}[X]$, alors $PR \in Q\mathbb{C}[X]$. On prend donc $P \in N$ et on démontre que $PR \in M$. Par linéarité, on peut se limiter à $R = X^k$, pour $k \geqslant 1$, et même à $R = X$.

Supposons en effet démontré que, pour tout $P \in N$, on a $XP \in M$. Un récurrence simple sur k conduit à $X^kP \in M$ pour tout $P \in N$. C'est démontré pour $k = 1$, et si on suppose que c'est vrai pour $k \geqslant 1$, alors, pour $P \in N$, il existe $P_1 \in N$ et $P_2 \in \mathbb{C}[X]$ tels que $X^kP = P_1 + QP_2$. On en déduit que $X^{k+1}P = XP_1 + QXP_2$. Le cas $k = 1$ donne $XP_1 \in M$ et d'autre part, on a $QXP_2 \in Q\mathbb{C}[X] \subset M$. On conclut que $X^{k+1}P$ est dans M.

Soit donc $P \in N$. Il existe $P' \in \mathbb{C}[X]$ tel que

$$PX = QP' + \pi_Q(PX) = QP' + S_Q(P).$$

Le polynôme QP' est dans $Q\,\mathbb{C}[X]$ donc dans M et par hypothèse, N est stable, donc $S_Q(P)$ est dans N. On en déduit que XP appartient à M.

5. Le sous-espace N est invariant, donc stable. On définit M et Q_1 comme dans la question 4. On remarque que Q est dans M. On en déduit que Q_1 divise Q : il existe $Q_2 \in \mathbb{C}[X]$ tel que $Q = Q_1 Q_2$.

Soit $P \in N$. Puisque N est invariant par S_Q, il existe $P' \in N$ tel que $P = S_Q(P')$. Le polynôme P' appartient à N donc à $Q_1\,\mathbb{C}[X]$. Il s'écrit donc $P' = Q_1 P''$. On a donc

$$P = S_Q(Q_1 P'') = \pi_Q(Q_1 X P'') = \pi_{Q_1 Q_2}(Q_1 X P'') = Q_1 \pi_{Q_2}(X P''),$$

d'après la question 2. Ceci démontre que $N \subset Q_1 \operatorname{Im} \pi_{Q_2}$. Soit N' le sous-espace vectoriel de $\operatorname{Im} \pi_{Q_2}$ tel que $N = Q_1 N'$.

De l'égalité $Q_1\,\mathbb{C}[X] = N + Q\,\mathbb{C}[X]$, on déduit que $\mathbb{C}[X] = N' + Q_2\,\mathbb{C}[X]$. Le sous-espace N' étant inclus dans $\operatorname{Im} \pi_{Q_2} = C_{d-1}[X]$, où d est le degré de Q_2, on a $N' \cap Q_2\,\mathbb{C}[X] = \{0\}$. On a donc $\mathbb{C}[X] = N' \oplus Q_2\,\mathbb{C}[X]$. Mais on a aussi $\mathbb{C}[X] = \operatorname{Im} Q_2 \oplus Q_2\,\mathbb{C}[X]$ (π_{Q_2} est la projection sur $\operatorname{Im} Q_2$, parallèlement à $Q_2\,\mathbb{C}[X]$), et puisque $N' \subset \operatorname{Im} \pi_{Q_2}$, on conclut que $N' = \operatorname{Im} \pi_{Q_2}$, c'est-à-dire que $N = Q_1 \operatorname{Im} \pi_{Q_2}$.

On a démontré que tout sous-espace N invariant s'écrit $Q_1 \operatorname{Im} \pi_{Q_2}$, avec $Q_1 Q_2 = Q$. La question 3 permet de préciser que Q_2 est premier avec X. ◁

L'égalité entre le rang et la trace d'un projecteur rappelée plus haut est utilisée dans l'exercice suivant, pour déterminer la dimension de l'espace des points invariants sous l'action d'un sous-groupe fini de GL(E).

6.21. Formule de Burnside

1. Soit E un $\mathbb{C}$-espace vectoriel de dimension finie $n \geqslant 1$, G un sous-groupe fini de GL(E). On pose

$$E^G = \{x \in E,\ \forall g \in G,\ g(x) = x\}.$$

Montrer que
$$\dim E^G = \frac{1}{|G|} \sum_{g \in G} \operatorname{Tr}(g).$$

2. Soit G un sous-groupe de $\mathcal{S}_n$. Pour $g \in G$, on note $F(g)$ le nombre de points fixes de g. Soit r le nombre d'orbites pour l'opération de G sur $[\![1, n]\!]$. Déduire de ce qui précède que

$$r = \frac{1}{|G|} \sum_{g \in G} F(g).$$

3. Donner une preuve directe de la formule de la question 2.

(École normale supérieure)

▷ **Solution.**

1. Posons $u = \dfrac{1}{|\mathrm{G}|}\sum\limits_{g\in\mathrm{G}} g$. On voit que, si $g \in \mathrm{G}$, on a $gu = ug = u$. En effet, on peut écrire par exemple,

$$gu = g\frac{1}{|\mathrm{G}|}\sum_{g'\in\mathrm{G}} g' = \frac{1}{|\mathrm{G}|}\sum_{g'\in\mathrm{G}} gg' = u$$

car, g étant fixé, l'application $g' \longmapsto gg'$ est une bijection de G sur G. On en déduit que

$$u^2 = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} gu = \frac{1}{|\mathrm{G}|}\sum_{g\in\mathrm{G}} u = u,$$

c'est-à-dire que u est un projecteur.

Si $x \in \mathrm{E}^{\mathrm{G}}$, il est clair que $u(x) = x$. Mais inversement, si $x \in \operatorname{Im} u$, on a $u(x) = x$ et la relation $gu = u$ implique que pour tout $g \in \mathrm{G}$,

$$g(x) = g(u(x)) = u(x) = x,$$

ce qui montre que $x \in \mathrm{E}^{\mathrm{G}}$. Finalement E^{G} est l'image du projecteur u. En caractéristique nulle, ce qui est le cas ici, la trace d'un projecteur est égale à son rang. D'où le résultat.

2. On réalise G comme sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ à l'aide des matrices de permutation : à tout $g \in \mathrm{G}$, on associe la matrice P_g de terme général $\delta_{i,g(j)}$, où δ désigne le symbole de Kronecker. On vérifie que, pour $(g, g') \in \mathrm{G}^2$, on a $\mathrm{P}_g \circ \mathrm{P}_{g'} = \mathrm{P}_{gg'}$. L'application $g \longmapsto \mathrm{P}_g$ est donc un morphisme de groupes, injectif, de G dans $\mathrm{GL}_n(\mathbb{C})$. On en déduit que $\mathrm{G}' = \{\mathrm{P}_g,\ g \in \mathrm{G}\}$ est un sous-groupe de $\mathrm{GL}_n(\mathbb{C})$ isomorphe à G. Le lien avec la question précédente apparaît déjà puisque $\mathrm{F}(g)$, le nombre de points fixes de la permutation g, n'est autre que la trace de la matrice P_g. Il ne reste plus qu'à voir pourquoi la dimension du sous-espace $\mathrm{E}^{\mathrm{G}'}$ est égale au nombre r d'orbites.

Notons $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$, $\Omega_1, \ldots, \Omega_r$ les différentes orbites de $[\![1, n]\!]$ sous l'opération de G et posons $\mathrm{F}_k = \mathrm{Vect}(e_i)_{i\in\Omega_k}$ pour tout $k \in [\![1, r]\!]$. On remarque que, pour tout $g \in \mathrm{G}$, on a $\mathrm{P}_g(e_j) = e_{g(j)}$. Les sous-espaces vectoriels F_k sont donc stables par les matrices de G'. De plus, on a $\mathbb{C}^n = \mathrm{F}_1 \oplus \cdots \oplus \mathrm{F}_r$. Soit $\mathrm{X} \in \mathbb{C}^n$ que l'on décompose en $\mathrm{X} = \mathrm{X}_1 + \cdots + \mathrm{X}_r$ avec $\mathrm{X}_i \in \mathrm{F}_i$, pour $1 \leqslant i \leqslant r$. On obtient, pour $g \in \mathrm{G}$, $\mathrm{P}_g\mathrm{X} = \sum\limits_{i=1}^{r} \mathrm{P}_g\mathrm{X}_i$. Comme $\mathrm{P}_g\mathrm{X}_i \in \mathrm{F}_i$, on a, par unicité de la décomposition, $\mathrm{P}_g(\mathrm{X}) = \mathrm{X}$ si et seulement si $\mathrm{P}_g\mathrm{X}_i = \mathrm{X}_i$ pour tout $i \in [\![1, r]\!]$. On en déduit que

$$\mathrm{E}^{\mathrm{G}'} = \bigoplus_{i=1}^{r} (\mathrm{E}^{\mathrm{G}'} \cap \mathrm{F}_i).$$

Or, il est aisé de voir que $E^{G'} \cap F_i$ est la droite vectorielle engendrée par le vecteur $\sum_{k\in\Omega_i} e_k$. En effet si $x \in F_i$ s'écrit $x = \sum_{k\in\Omega_i} \lambda_k e_k$, où les λ_k sont dans $\mathbb{C}$, on obtient, pour tout $g \in G$, $P_g(x) = \sum_{k\in\Omega_i} \lambda_k e_{g(k)} = \sum_{k\in\Omega_i} \lambda_{g^{-1}(k)} e_k$. On en déduit que $x \in E^{G'} \cap F_i$ si et seulement si, pour tout $k \in \Omega_i$ et tout $g \in G$, on a $\lambda_{g^{-1}(k)} = \lambda_k$. Le groupe G agissant transitivement sur Ω_i, par définition, il faut que tous les λ_k soient égaux, ce qui conduit au résultat annoncé. On a donc, pour tout $k \in \Omega_i$, $\dim(E^{G'} \cap F_i) = 1$ et par conséquent $\dim E^{G'} = r$.

3. L'idée est simplement de calculer de deux manières différentes le cardinal de l'ensemble $A = \{(g,x) \in G \times [\![1,n]\!],\ g(x) = x\}$. Si on somme d'abord selon G, on obtient $|A| = \sum_{g\in G} F(g)$. Si on somme selon les éléments de $[\![1,n]\!]$, on a $|A| = \sum_{k=1}^{n} |G_k|$ où $G_k = \{g \in G,\ g(k) = k\}$ est le stabilisateur de k. Or, si on note $\Omega_1, \ldots, \Omega_r$ les orbites de $[\![1,n]\!]$ pour l'action de G, on a

$$\sum_{1\leqslant k\leqslant n} |G_k| = \sum_{i=1}^{r} \sum_{k\in\Omega_i} |G_k| = \sum_{i=1}^{r} \sum_{k\in\Omega_i} \frac{|G|}{|\Omega_i|} = r|G|.$$

On retrouve la formule en identifiant les résultats des deux calculs. ◁

Le résultat de cette dernière question se généralise à un groupe fini quelconque G *opérant sur un ensemble fini* X*, la preuve étant la même. Cette formule de Burnside*[2] *est un résultat important en combinatoire (méthode de Pólya) qui intervient lorsqu'on cherche à dénombrer les configurations d'un ensemble modulo l'action d'un groupe : par exemple, de combien de manières différentes peut-on peindre un cube avec d couleurs, à rotation près ?*

Dans l'étude d'un endomorphisme u on essaye, autant que faire se peut, de découper l'espace en une somme directe de sous-espaces stables pour se ramener à l'étude (que l'on espère plus simple) des restrictions de u à ces sous-espaces. C'est typiquement l'objet de la réduction avec les sous-espaces propres ou les sous-espaces caractéristiques. Dans l'étude des représentations linéaires d'un groupe fini G*, on rencontre la même démarche, qui conduit à la notion de représentations irréductibles*[3]*. C'est le lemme de l'exercice suivant qui permet cela : on se donne un*

2. Bien qu'usuellement connue sous ce nom, elle n'est pas due à Burnside mais à Frobenius. Il y a comme cela un certain nombre de théorèmes injustement baptisés...

3. Pour une introduction à la théorie des représentations des groupes le lecteur pourra consulter SERRE (J.-P.), *Représentations linéaires des groupes finis*, Hermann, 1978 ou résoudre le problème posé aux ENS Lyon-Cachan en 1997 qui concerne le début de la théorie : représentations irréductibles, orthogonalité des caractères...

groupe fini de GL(E) *qui stabilise un sous-espace* F *de* E *et on cherche à montrer l'existence d'un supplémentaire stable. Ce sera l'occasion de voir, comme annoncé plus haut, le rapport entre les projecteurs et les décompositions en somme directe.*

6.22. Théorème de Maschke

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie $n \geqslant 1$, G un sous-groupe fini de GL(E) et F un sous-espace vectoriel de E stable par tous les éléments de G. Montrer que F admet un supplémentaire stable par tous les éléments de G.

(École normale supérieure)

▷ **Solution.**

• Remarquons qu'il y a une correspondance bijective entre les supplémentaires de F et les projecteurs dont l'image est F, un supplémentaire de F étant le noyau d'un tel projecteur. La question posée équivaut donc à trouver un projecteur p d'image F tel que $\operatorname{Im} p$ (par hypothèse) et $\operatorname{Ker} p$ soient stables par tous les éléments de G.

Soit p un projecteur de E et $u \in \mathcal{L}(\mathrm{E})$. Si $\operatorname{Ker} p$ et $\operatorname{Im} p$ sont stables par u, alors u commute avec p sur $\operatorname{Ker} p$ et sur $\operatorname{Im} p$, donc par linéarité sur $\mathrm{E} = \operatorname{Im} p \oplus \operatorname{Ker} p$. Réciproquement, si u et p commutent, alors $\operatorname{Ker} p$ et $\operatorname{Im} p = \operatorname{Ker}(p - \mathrm{Id})$ sont des sous-espaces stables par u (en effet, ce sont des sous-espaces propres de p).

Il nous faut donc trouver un projecteur p qui commute avec tous les éléments de G ; son noyau fournira alors un supplémentaire de F stable par tous les éléments de G.

Partons d'un projecteur quelconque q dont l'image est F. L'idée fondamentale est de moyenner les conjugués de q par les éléments de G. Posons

$$p = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} g \circ q \circ g^{-1}.$$

• Montrons que p commute avec tout élément de G. Si $g_0 \in \mathrm{G}$, on a

$$\begin{aligned} g_0 \circ p &= \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} g_0 \circ g \circ q \circ g^{-1} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g_0 \circ g) \circ q \circ g^{-1} \circ g_0^{-1} \circ g_0 \\ &= \left(\frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} (g_0 \circ g) \circ q \circ (g_0 \circ g)^{-1} \right) g_0 = p \circ g_0, \end{aligned}$$

car lorsque g décrit le groupe G, $g_0 \circ g$ également puisque la translation à gauche $g \longmapsto g_0 \circ g$ est une bijection de G.

• Pour finir, il n'y a plus qu'à vérifier que p est un projecteur d'image F.

Si $x \in \mathrm{F}$, puisque F est stable par tous les éléments de G, on obtient, pour tout $g \in \mathrm{G}$,

$$g \circ q \circ g^{-1}(x) = g(g^{-1}(x)) = x.$$

Il en résulte que $p(x) = x$. Tout vecteur de F est fixe par p.

Si maintenant x est un vecteur quelconque dans E, on a $p(x) \in \mathrm{F}$ car $g \circ q \circ g^{-1}(x) \in \mathrm{F}$ pour tout $g \in \mathrm{G}$. On en déduit que $p(p(x)) = p(x)$. On conclut que p est bien un projecteur d'image F. $\lhd$

La preuve ci-dessus reste valide en caractéristique p (premier) à condition que p ne divise pas le cardinal de G. *Sur le corps des réels (resp. des complexes) on peut également utiliser un argument de moyenne avec le produit scalaire : on munit* E *d'une structure euclidienne (resp. hermitienne) quelconque et on pose, pour* $(x, y) \in \mathrm{E}^2$.

$$\langle x, y\rangle_{\mathrm{G}} = \frac{1}{|\mathrm{G}|} \sum_{g \in \mathrm{G}} \langle g(x), g(y)\rangle.$$

On vérifie que $\langle\ ,\ \rangle_{\mathrm{G}}$ *est encore un produit scalaire sur* E *et que tous les éléments de* G *sont orthogonaux (resp. unitaires) pour ce produit scalaire. L'orthogonal de* F *au sens de* $\langle\ ,\ \rangle_{\mathrm{G}}$ *fournit alors un supplémentaire stable. Cette démarche a aussi été proposée en exercice d'oral à l'École polytechnique.*

Nous allons maintenant commencer une série d'exercices plus abstraits, consacrés à l'étude de l'algèbre $\mathcal{L}(\mathrm{E})$ *où* E *est un* K*-espace vectoriel de dimension finie. Nous rappelons au lecteur que le centre de* $\mathcal{L}(\mathrm{E})$ *est réduit aux homothéties (on trouvera une démonstration de ce fait p. 269). L'exercice suivant est consacré aux automorphismes de l'algèbre* $\mathcal{L}(\mathrm{E})$.

6.23. Automorphismes de la K-algèbre $\mathcal{L}(\mathrm{E})$

Soit E un K-espace vectoriel de dimension finie $n \geqslant 1$. Montrer que tout automorphisme de l'algèbre $\mathcal{L}(\mathrm{E})$ est de la forme

$$u \longmapsto \tau \circ u \circ \tau^{-1} \quad \text{où } \tau \in \mathrm{GL}(\mathrm{E}).$$

(École polytechnique)

▷ **Solution.**

Les conjugaisons $\varphi_\tau : u \longmapsto \tau \circ u \circ \tau^{-1}$, où $\tau \in \mathrm{GL(E)}$, sont clairement des automorphismes d'algèbre.

Réciproquement, soit φ un automorphisme d'algèbre de $\mathcal{L}(\mathrm{E})$. Choisissons une base $(e_1, \ldots, e_n)$ de E et notons pour $1 \leqslant i, j \leqslant n$, u_{ij} l'endomorphisme de $\mathcal{L}(\mathrm{E})$ défini par $u_{ij}(e_k) = \delta_{jk} e_i$, pour tout $k \in [\![1, n]\!]$. La matrice de u_{ij} dans la base canonique de K^n est la matrice E_{ij} de la base canonique de $\mathcal{M}_n(\mathrm{K})$. Les u_{ij} forment donc une base de $\mathcal{L}(\mathrm{E})$. Posons alors $v_{ij} = \varphi(u_{ij})$.

On rappelle que pour tout (i, j, k, l), $u_{ij} \circ u_{kl} = \delta_{jk} u_{il}$. Comme φ est un automorphisme d'algèbre, les v_{ij} vérifient les mêmes relations. En particulier, on a, pour tout i, $v_{ii}^2 = v_{ii}$, de sorte que v_{ii} est un projecteur.

Si φ est de la forme φ_τ, on vérifie que les v_{ij} sont définis à partir de la base $(\tau(e_1), \ldots, \tau(e_n))$, exactement comme les u_{ij} le sont à partir de $(e_1, \ldots, e_n)$. Cette remarque nous donne la méthode pour construire à partir de φ la base $(\tau(e_1), \ldots, \tau(e_n))$ et l'application τ.

Choisissons un vecteur non nul e'_1 dans l'image de v_{11} et posons pour tout $i \in [\![1, n]\!]$, $e'_i = v_{i1}(e'_1)$. On observe alors que :

- e'_i est dans l'image de v_{ii}, car $v_{ii}(e'_i) = v_{ii} \circ v_{i1}(e'_1) = v_{i1}(e'_1) = e'_i$;
- e'_i est non nul, car $v_{1i}(e'_i) = v_{1i} \circ v_{i1}(e'_1) = v_{11}(e'_1) = e'_1 \neq 0$;
- $(e'_1, \ldots, e'_n)$ est une base de E. En effet, on a $v_{jj}(e'_i) = v_{jj} \circ v_{i1}(e'_1) = \delta_{ij} v_{j1}(e'_1) = \delta_{ij} e'_i$. Ainsi, si $\sum_{i=1}^{n} \lambda_i e'_i = 0$, en appliquant v_{jj} à cette relation, il vient $\lambda_j = 0$.

Notons alors τ l'unique isomorphisme de E qui envoie e_i sur e'_i pour tout i. On va montrer que $v_{ij} = \tau \circ u_{ij} \circ \tau^{-1}$ pour tout couple (i, j). En effet, on a, pour tout $k \in [\![1, n]\!]$,

$$(\tau \circ u_{ij} \circ \tau^{-1})(e'_k) = (\tau \circ u_{ij})(e_k) = \tau(\delta_{jk} e_i) = \delta_{jk} e'_i$$

et par ailleurs,

$$v_{ij}(e'_k) = v_{ij} \circ v_{k1}(e'_1) = \delta_{jk} v_{i1}(e'_1) = \delta_{jk} e'_i.$$

Il en résulte que les automorphismes φ et φ_τ, qui coïncident sur la base (u_{ij}) de $\mathcal{L}(\mathrm{E})$ sont égaux. ◁

Les idéaux de $\mathcal{L}(\mathrm{E})$ ont fait l'objet de plusieurs exercices posés aux concours. Comme $\mathcal{L}(\mathrm{E})$ est une algèbre non commutative (dès que $\dim \mathrm{E} > 1$), on est amené à distinguer les idéaux à droite et les idéaux à gauche. Rappelons les définitions : un idéal à gauche (resp. à droite) est un sous-groupe additif tel que pour tout $a \in \mathcal{L}(\mathrm{E})$ et $u \in \mathrm{I}$, $au \in \mathrm{I}$ (resp. $ua \in \mathrm{I}$). On parle d'idéal bilatère pour un idéal à droite et à gauche. Le premier exercice fait montrer que $\mathcal{L}(\mathrm{E})$ est une algèbre simple, c'est-à-dire sans idéal bilatère non trivial.

6.24. Simplicité de $\mathcal{L}(\mathrm{E})$

1. Soit E un espace vectoriel de dimension finie. Montrer que les seuls idéaux bilatères de $\mathcal{L}(\mathrm{E})$ sont $\{0\}$ et E. Cela reste-t-il vrai en dimension infinie ?

2. Soit p une semi-norme sur $\mathrm{M}_n(\mathbb{C})$ vérifiant $p(\mathrm{AB}) \leqslant p(\mathrm{A})p(\mathrm{B})$ pour tout $(\mathrm{A}, \mathrm{B}) \in \mathrm{M}_n(\mathbb{C})^2$. Montrer que p est nulle ou que p est une norme.

(École normale supérieure)

▷ **Solution.**

1. On se ramène à la recherche des idéaux bilatères de $\mathcal{M}_n(\mathrm{K})$. Soit I un idéal bilatère non nul de $\mathcal{M}_n(\mathrm{K})$ et $\mathrm{M} = (m_{ij})_{1 \leqslant i,j \leqslant n} \in \mathrm{I}$, non nulle. Notons $(\mathrm{E}_{ij})_{1 \leqslant i,j \leqslant n}$ la base canonique de $\mathcal{M}_n(\mathrm{K})$ et $(i_0, j_0) \in [\![1, n]\!]^2$ tel que $m_{i_0 j_0} \neq 0$. Nous savons que $\mathrm{E}_{ij}\mathrm{E}_{kl} = \delta_{jk}\mathrm{E}_{il}$ pour tout (i, j, k, l) dans $[\![1, n]\!]^4$. Ainsi, l'élément

$$\mathrm{E}_{ii_0}\mathrm{M}\mathrm{E}_{j_0 j} = \sum_{1 \leqslant k,l \leqslant n} m_{kl}\mathrm{E}_{ii_0}\mathrm{E}_{kl}\mathrm{E}_{j_0 j} = \sum_{k=1}^{n} m_{kj_0}\mathrm{E}_{ii_0}\mathrm{E}_{kj} = m_{i_0 j_0}\mathrm{E}_{ij}$$

est dans I, et comme $m_{i_0 j_0} \neq 0$, E_{ij} est également dans I. Ceci est vrai pour tout (i, j) de $[\![1, n]\!]^2$. Comme les E_{ij} engendrent $\mathcal{M}_n(\mathrm{K})$, on obtient $\mathrm{I} = \mathcal{M}_n(\mathrm{K})$.

En revanche, si E est de dimension infinie, il existe des idéaux bilatères non triviaux, par exemple l'idéal des endomorphismes de rang fini.

2. Considérons l'ensemble N des matrices A telles que $p(\mathrm{A}) = 0$. La définition d'une semi-norme implique que N est un sous-espace vectoriel de $\mathrm{M}_n(\mathbb{C})$. L'inégalité vérifiée par p montre que c'est un idéal bilatère de $\mathrm{M}_n(\mathbb{C})$. Comme les seuls idéaux bilatères sont $\{0\}$ et $\mathrm{M}_n(\mathbb{C})$, on a le résultat. ◁

Les deux exercices qui suivent sont consacrés à la description des idéaux à gauche et à droite.

6.25. Idéaux à gauche de $\mathcal{L}(\mathrm{E})$

Soit E un K-espace vectoriel de dimension finie. On note, pour tout F sous-espace de E,

$$g(\mathrm{F}) = \{u \in \mathcal{L}(\mathrm{E}), \mathrm{F} \subset \operatorname{Ker} u\},$$

et si H est une partie de $\mathcal{L}(\mathrm{E})$, on pose $f(\mathrm{H}) = \bigcap_{u \in \mathrm{H}} \operatorname{Ker} u$.

1. Vérifier que, pour tout sous-espace vectoriel F de E, $g(\mathrm{F})$ est un idéal à gauche de $\mathcal{L}(\mathrm{E})$ et que l'on a $(f \circ g)(\mathrm{F}) = \mathrm{F}$.

Soit I un idéal à gauche de $\mathcal{L}(\mathrm{E})$.

2. Soit $u \in \mathrm{I}$, $v \in \mathcal{L}(\mathrm{E})$ tel que $\operatorname{Ker} u \subset \operatorname{Ker} v$. Montrer que $v \in \mathrm{I}$.

3. Si p et q sont deux projecteurs appartenant à I, montrer qu'il existe un projecteur r dans I tel que $\operatorname{Ker} r = \operatorname{Ker} p \cap \operatorname{Ker} q$.

4. Prouver qu'il existe un projecteur p appartenant à I tel que $\operatorname{Ker} p = f(\mathrm{I})$, puis que $\mathrm{I} = \mathcal{L}(\mathrm{E})p$.

5. Étudier $(g \circ f)(\mathrm{I})$ et conclure.

(École polytechnique)

▷ **Solution.**

1. Pour u et v dans $g(\mathrm{F})$ et $a \in \mathcal{L}(\mathrm{E})$, on a $\operatorname{Ker} u \subset \operatorname{Ker} au$ et $\mathrm{F} \subset \operatorname{Ker} u \cap \operatorname{Ker} v \subset \operatorname{Ker}(u+v)$. Les endomorphismes au et $u+v$ sont donc dans $g(\mathrm{F})$. Il en résulte que $g(\mathrm{F})$ est un idéal à gauche de $\mathcal{L}(\mathrm{E})$.

• On a clairement $\mathrm{F} \subset \bigcap_{u \in g(\mathrm{F})} \operatorname{Ker} u$. Si p est la projection sur un supplémentaire G de F, parallèlement à F, on a $\operatorname{Ker} p = \mathrm{F}$ et $p \in g(\mathrm{F})$. On en déduit que $\bigcap_{u \in g(\mathrm{F})} \operatorname{Ker} u \subset \mathrm{F}$ et finalement $\bigcap_{u \in g(\mathrm{F})} \operatorname{Ker} u = \mathrm{F}$, c'est-à-dire

$$\boxed{(f \circ g)(\mathrm{F}) = \mathrm{F}}.$$

2. Cela résulte directement du lemme de factorisation (cf. la première question de l'exercice 6.4) : de l'inclusion $\operatorname{Ker} u \subset \operatorname{Ker} v$, on déduit qu'il existe $a \in \mathcal{L}(\mathrm{E})$ tel que $v = au$. D'où il résulte que v est dans I.

3. Soit p et q deux projecteurs appartenant à I. On cherche un projecteur r appartenant à I tel que $\operatorname{Ker} r = \operatorname{Ker} p \cap \operatorname{Ker} q$. Soit X (resp. Y) un supplémentaire de $\operatorname{Ker} p \cap \operatorname{Ker} q$ dans $\operatorname{Ker} p$ (resp $\operatorname{Ker} q$) et Z un supplémentaire dans E de $\operatorname{Ker} p + \operatorname{Ker} q$. On obtient donc $\mathrm{E} = \mathrm{Z} \oplus \mathrm{X} \oplus \mathrm{Y} \oplus (\operatorname{Ker} p \cap \operatorname{Ker} q)$. Le projecteur r_1 sur $\mathrm{Y} \oplus \mathrm{Z}$ parallèlement à $\mathrm{X} \oplus (\operatorname{Ker} p \cap \operatorname{Ker} q) = \operatorname{Ker} p$ a pour noyau $\operatorname{Ker} p$. Il est donc dans I d'après la question précédente. De même, le projecteur r_2 sur X et de noyau $\operatorname{Ker} q \oplus \mathrm{Z}$ est dans I, toujours d'après la question précédente. On pose $r = r_1 + r_2$. Alors r est le projecteur sur $\mathrm{Z} \oplus \mathrm{X} \oplus \mathrm{Y}$ de noyau $\operatorname{Ker} p \cap \operatorname{Ker} q$ et il est dans I.

4. Soit p un projecteur de I de rang maximal ou, si l'on préfère, dont la dimension du noyau est minimale et u un élément quelconque de I. On peut trouver un projecteur q tel que $\operatorname{Ker} q = \operatorname{Ker} u$. Celui-ci est dans I, d'après la question 2. De la question précédente, on déduit qu'il existe $r \in \mathrm{I}$ tel que $\operatorname{Ker} r = \operatorname{Ker} p \cap \operatorname{Ker} q$. Comme $\dim \operatorname{Ker} r \geqslant \dim \operatorname{Ker} p$ par choix de p, on en déduit que $\operatorname{Ker} p = \operatorname{Ker} r \subset \operatorname{Ker} q = \operatorname{Ker} u$. Par conséquent, on obtient

$$\operatorname{Ker} p \subset \bigcap_{u \in I} \operatorname{Ker} u \subset \operatorname{Ker} p \quad \text{et} \quad \boxed{\operatorname{Ker} p = f(I)}.$$

On a déjà l'inclusion $\mathcal{L}(E)p \subset I$ puisque $p \in I$. Réciproquement, si $u \in I$, comme $\operatorname{Ker} p \subset \operatorname{Ker} u$, la question 2 montre que $u \in \mathcal{L}(E)p$. On conclut que $I = \mathcal{L}(E)p$.

5. On a $I \subset g(f(I))$ car tous les éléments de l'idéal I s'annulent sur le sous-espace $f(I)$. Mais inversement, si u vérifie $f(I) = \operatorname{Ker} p \subset \operatorname{Ker} u$, on a $u \in I$, toujours d'après la question 2. Ainsi, $g(f(I)) = I$ et $g \circ f$ est l'identité.

Conclusion. L'application g établit une bijection, strictement décroissante pour l'inclusion, entre les idéaux à gauche et les sous-espaces vectoriels de E. Sa bijection réciproque est f. De plus, tout idéal à gauche I est engendré par un projecteur (quelconque) de noyau le sous-espace $f(I)$. ◁

On va obtenir une description géométrique similaire des idéaux à droite, les noyaux étant remplacés par les images.

6.26. Idéaux à droite de $\mathcal{L}(E)$

Soit E un K-espace vectoriel de dimension finie. Si I est un idéal à droite de $\mathcal{L}(E)$ et F un sous-espace de E, on pose

$$f(I) = \sum_{u \in I} \operatorname{Im} u \quad \text{et} \quad g(F) = \{u \in \mathcal{L}(E), \operatorname{Im} u \subset F\}$$

1. Montrer que pour tout sous-espace F, $g(F)$ est un idéal à droite de $\mathcal{L}(E)$ et que $f \circ g(F) = F$.

Soit I un idéal à droite.

2. Soit $u \in I$, $v \in \mathcal{L}(E)$ tel que $\operatorname{Im} v \subset \operatorname{Im} u$. Montrer que $v \in I$.

3. Soit u et v deux éléments de I. Montrer qu'il existe un projecteur $p \in I$ tel que $\operatorname{Im} p = \operatorname{Im} u + \operatorname{Im} v$.

4. En déduire qu'il existe un projecteur p appartenant à I tel que $\operatorname{Im} p = f(I)$, puis que $I = p\mathcal{L}(E)$.

5. Conclure.

(École polytechnique)

▷ **Solution.**

1. On a clairement $0 \in g(F)$. Si u et v sont dans $g(F)$ et $a \in \mathcal{L}(E)$, on obtient

$$\operatorname{Im}(u+v) \subset \operatorname{Im} u + \operatorname{Im} v \subset F + F = F \quad \text{et} \quad u + v \in g(F),$$
$$\operatorname{Im}(u \circ a) \subset \operatorname{Im} u \subset F \quad \text{et} \quad u \circ a \in g(F).$$

Ainsi, $g(\mathrm{F})$ est un idéal à droite de $\mathcal{L}(\mathrm{E})$.

L'inclusion $f(g(\mathrm{F})) \subset \mathrm{F}$ est évidente. Si p est un projecteur sur F, parallèlement à un supplémentaire de F, on a $\operatorname{Im} p = \mathrm{F}$ et $p \in g(\mathrm{F})$. On en déduit que $\mathrm{F} \subset f(g(\mathrm{F}))$ et finalement

$$\boxed{f(g(\mathrm{F})) = \mathrm{F}}$$

2. Cela résulte directement du second lemme de factorisation (cf. la question 2 de l'exercice 6.4) : de l'inclusion $\operatorname{Im} v \subset \operatorname{Im} u$, on déduit l'existence de $a \in \mathcal{L}(\mathrm{E})$ tel que $v = ua$, de sorte que $v \in \mathrm{I}$.

3. Soit S un supplémentaire de $\operatorname{Im} u \cap \operatorname{Im} v$ dans $\operatorname{Im} u$. On montre facilement l'égalité $\mathrm{S} \oplus \operatorname{Im} v = \operatorname{Im} u + \operatorname{Im} v$. Soit S' un supplémentaire de cette somme dans E, de sorte que $\mathrm{E} = \mathrm{S}' \oplus \mathrm{S} \oplus \operatorname{Im} v$. Comme $v \in \mathrm{I}$, le projecteur q_1 sur $\operatorname{Im} v$ parallèlement à $\mathrm{S} \oplus \mathrm{S}'$ est dans I d'après la question précédente (car $\operatorname{Im} q_1 = \operatorname{Im} v$). Comme $u \in \mathrm{I}$, le projecteur q_2 sur S parallèlement à $\operatorname{Im} v \oplus \mathrm{S}'$ est aussi dans I, toujours par la question précédente (puisque $\operatorname{Im} q_2 \subset \operatorname{Im} u$). On en déduit que $p = q_1 + q_2$, qui est le projecteur sur $\operatorname{Im} u + \operatorname{Im} v$ parallèlement à S', est aussi dans I.

4. On choisit un élément v de I de rang maximal et on pose $\mathrm{F} = \operatorname{Im} v$, puis on considère un projecteur p sur F. D'après la question 2, p est aussi dans I. La question précédente montre que tout élément de $u \in \mathrm{I}$ a son image incluse dans F (sinon on pourrait trouver dans I un élément dont l'image $\operatorname{Im} u + \mathrm{F}$ contiendrait F strictement ; son rang serait supérieur à celui de v). On a donc $f(\mathrm{I}) = \mathrm{F} = \operatorname{Im} p$.

On a clairement $p\mathcal{L}(\mathrm{E}) \subset \mathrm{I}$. Réciproquement, si $u \in \mathrm{I}$, on sait que $\operatorname{Im} u \subset \operatorname{Im} p$ et d'après la question 2, il existe $a \in \mathcal{L}(\mathrm{E})$ tel que $u = pa$ et donc $u \in p\mathcal{L}(\mathrm{E})$. On conclut que $\mathrm{I} = p\mathcal{L}(\mathrm{E})$.

5. On a clairement $\mathrm{I} \subset g(f(\mathrm{I}))$. Inversement soit $u \in g(f(\mathrm{I}))$. On a alors $\operatorname{Im} u \subset f(\mathrm{I}) = \operatorname{Im} p$ de sorte que $u \in \mathrm{I}$, toujours d'après la question 2.

Conclusion. L'application f établit une bijection, strictement croissante pour l'inclusion, entre les idéaux à droite et les sous-espaces vectoriels de E. Sa bijection réciproque est g. De plus, tout idéal à droite I est engendré par un projecteur (quelconque) d'image le sous-espace $f(\mathrm{I})$. $\lhd$

Le thème d'étude suivant de ce chapitre est la dualité. Rappelons que le dual d'un K*-espace vectoriel* E *est le* K*-espace vectoriel* $\mathrm{E}^* = \mathcal{L}(\mathrm{E}, \mathrm{K})$ *des formes linéaires de* E *dans* K*. On a* $\dim \mathrm{E}^* = \dim \mathrm{E}$ *en dimension finie, sans qu'il existe d'isomorphisme canonique entre* E *et son dual. Soit* $(e_1, \ldots, e_n)$ *une base de* E*. La famille* $(e_1^*, \ldots, e_n^*)$ *d'éléments de* E^* *définie par* $e_i^*(e_j) = \delta_{ij}$ *est une base de* E^* *appelée* base duale *de* $(e_1, \ldots, e_n)$.

Les formes linéaires permettent de caractériser analytiquement les hyperplans de E *: tout hyperplan est le noyau d'une forme linéaire non nulle, forme qui est unique à un scalaire multiplicatif près.*

Plus généralement, si F *est une partie de* E *et* G *une partie de* E^*, *on note*

$$F^\perp = \{u \in E^*, \forall x \in F, u(x) = 0\} \quad et \quad G^\circ = \{x \in E, \forall u \in G, u(x) = 0\}.$$

On appelle $F^\perp$ *l'orthogonal de* F *et* G° *l'orthogonal de* G. *On montre que* $F^\perp$ *et* G° *sont des sous-espaces vectoriels de* E^* *et* E *respectivement et que* $F^\perp = (\mathrm{Vect}\, F)^\perp$ *et* $G^\circ = (\mathrm{Vect}\, G)^\circ$. *On a, de plus,* $F \subset (F^\perp)^\circ$ *et* $G \subset (G^\circ)^\perp$.

En dimension finie, si F *et* G *sont des sous-espaces vectoriels de* E *et* E^* *respectivement, on a les propriétés suivantes :* $\dim F^\perp = \mathrm{codim}\, F$ *et* $\dim G^\circ = \mathrm{codim}\, G$, *d'où on déduit facilement* $(F^\perp)^\circ = F$ *et* $(G^\circ)^\perp = G$.

Le premier exercice ci-après, montre que l'égalité $(G^\circ)^\perp = G$ *subsiste en dimension infinie pour les sous-espaces* G *de dimension finie.*

6.27. Orthogonalité duale en dimension quelconque

Soit $f_1, \ldots, f_p, g$ des formes linéaires sur un espace vectoriel E de dimension quelconque. On suppose que $\bigcap_{i=1}^{p} \mathrm{Ker}\, f_i \subset \mathrm{Ker}\, g$. Montrer que g appartient à $\mathrm{Vect}(f_1, \ldots, f_p)$.

(École normale supérieure)

▷ **Solution.**

On peut supposer g non nulle, sans quoi le résultat est évident.

• En dimension finie, l'exercice est une une simple application des propriétés de l'orthogonalité duale. Si on note F le sous-espace de E^* engendré par $(f_1, \ldots, f_p)$ et D la droite de E^* engendrée par g, on a par hypothèse

$$\bigcap_{i=1}^{p} \mathrm{Ker}\, f_i = F^\circ \subset D^\circ = \mathrm{Ker}\, g.$$

Il en résulte, en prenant l'orthogonal que $(D^\circ)^\perp \subset (F^\circ)^\perp$. Sachant qu'en dimension finie, on a $(G^\circ)^\perp = G$ pour tout sous-espace vectoriel G de E^*, on obtient $D \subset F$, ce qui est le résultat demandé.

• En dimension infinie, l'égalité $(G^\circ)^\perp = G$ n'est malheureusement plus vraie en général. On a *a priori* seulement l'inclusion $G \subset (G^\circ)^\perp$. L'exercice demande de prouver qu'il y a égalité lorsque G est de dimension finie. On raisonne par récurrence sur p. On pose $H = \mathrm{Ker}\, g$: c'est un hyperplan de E puisqu'on a supposé $g \neq 0$.

⋆ Traitons le cas $p = 1$. On a $H_1 = \operatorname{Ker} f_1 \subset H$. La forme linéaire f_1 n'est donc pas nulle et H_1 est un hyperplan de E. Par suite, on a $H_1 = H$ et le cours permet d'affirmer que les formes linéaires g et f_1 sont proportionnelles.

⋆ Supposons le résultat vrai au rang p et considérons des formes linéaires $f_1, \ldots, f_{p+1}$ telles que $\bigcap_{i=1}^{p+1} \operatorname{Ker} f_i \subset H$. On peut supposer que $f_{p+1} \neq 0$, sans quoi l'hypothèse de récurrence s'applique directement. Notons alors $\tilde{g}$, (resp. $\tilde{f}_i$ pour $1 \leqslant i \leqslant p$) la restriction de g (resp. de f_i) à l'hyperplan $\operatorname{Ker} f_{p+1}$. On a clairement $\bigcap_{i=1}^{p} \operatorname{Ker} \tilde{f}_i \subset \operatorname{Ker} \tilde{g}$. Par hypothèse de récurrence, il existe des scalaires $(\lambda_1, \ldots, \lambda_p)$ tels que $\tilde{g} = \sum_{i=1}^{p} \lambda_i \tilde{f}_i$. La forme linéaire $g - \sum_{i=1}^{p} \lambda_i f_i$ est alors nulle sur $\operatorname{Ker} f_{p+1}$; elle est donc proportionnelle à f_{p+1}, ce qui permet de conclure. ◁

La solution de l'exercice suivant exploite les propriétés de l'orthogonalité duale. Nous donnerons une seconde solution par récurrence, dans le chapitre sur les déterminants du tome 2 d'algèbre (exercice 1.16).

6.28. Familles libres d'applications

1. Soit K un corps commutatif et $f_1, \ldots, f_n$ des applications de K dans K. Montrer que la famille $(f_1, \ldots, f_n)$ est libre dans $\mathcal{F}(K, K)$ si et seulement s'il existe $(x_1, \ldots, x_n) \in K^n$ tel que la matrice $(f_i(x_j))_{1 \leqslant i,j \leqslant n}$ soit inversible.

2. Déterminer les applications $f : \mathbb{R} \longrightarrow \mathbb{R}$, dérivables, dont les translatées (*i.e.* les applications $f_a : x \longmapsto f(x + a)$ pour $a \in \mathbb{R}$) engendrent un sous-espace vectoriel de dimension finie de $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

(**École polytechnique**)

▷ **Solution.**

1. • Si la famille $(f_1, \ldots, f_n)$ est liée, les lignes de la matrice $(f_i(x_j))_{1 \leqslant i,j \leqslant n}$ sont liées, quel que soit le choix des scalaires $x_1, \ldots, x_n$. La contraposée fournit donc une des deux implications.

• Supposons que la famille $B = (f_1, \ldots, f_n)$ est libre et notons F le sous-espace de dimension n qu'elle engendre. Pour tout $a \in K$, l'application d'évaluation en a, $e_a : F \to K$, qui à $f \in F$ associe $f(a) \in K$, est une forme linéaire sur F. L'ensemble A des formes linéaires e_a, pour $a \in K$, constitue une partie génératrice de F^*. En effet, si $f \in A^\circ$, on a $f(a) = e_a(f) = 0$ pour tout $a \in K$, *i.e.* $f = 0$. Ainsi on a $A^\circ = \{0\}$

et $\operatorname{Vect} A = ((\operatorname{Vect} A)^\circ)^\perp = (A^\circ)^\perp = 0^\perp = F$, puisqu'on est en dimension finie. On peut donc choisir des scalaires $x_1, \ldots, x_n$ tels que les formes linéaires $e_{x_1}, \ldots, e_{x_n}$ constituent une base de F^*. Montrons que le n-uplet $(x_1, \ldots, x_n)$ répond à la question.

Considérons la matrice $M = (f_i(x_j))_{1 \leqslant i,j \leqslant n}$ et montrons que les lignes $L_1, \ldots, L_n$ de M forment une famille libre. Soit $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que $\sum\limits_{i=1}^{n} \lambda_i L_i = 0$. On a alors, pour tout $j \in [\![1, n]\!]$, $\sum\limits_{i=1}^{n} \lambda_i f_i(x_j) = 0$, c'est-à-dire $e_{x_j}\left(\sum\limits_{i=1}^{n} \lambda_i f_i\right) = 0$. La famille $e_{x_1}, \ldots, e_{x_n}$ étant une base de F^*, on a donc $\sum\limits_{i=1}^{n} \lambda_i f_i \in (F^*)^\circ = \{0\}$. La famille $(f_1, \ldots, f_n)$ étant une base de F, on en déduit que $\lambda_1 = \cdots = \lambda_n = 0$. La matrice M est donc inversible.

2. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$, dérivable, dont les translatées engendrent un $\mathbb{R}$-espace vectoriel F de dimension finie n. On considère des réels $a_1, \ldots, a_n$ tels que la famille $(f_{a_1}, \ldots, f_{a_n})$ soit une base de F. D'après la question 1, il existe des réels $x_1, \ldots, x_n$ tels que la matrice $M = (f_{a_i}(x_j))_{1 \leqslant i,j \leqslant n}$ soit inversible. La fonction f étant dérivable, les fonctions f_{a_i} le sont également. Ainsi tout élément de F est dérivable.

Soit g un élément quelconque de F. Montrons que g' est encore dans F. Il est clair que, pour tout $a \in \mathbb{R}$, la fonction g_a est dans F. En effet, on a $g_a \in \operatorname{Vect}(f_{a_1+a}, \ldots, f_{a_n+a}) \subset F$. Il existe donc des réels $\lambda_1(a), \ldots, \lambda_n(a)$ tels que $g_a = \sum\limits_{i=1}^{n} \lambda_i(a) f_{a_i}$. Montrons que les fonctions λ_i sont dérivables. On a, pour $1 \leqslant j \leqslant n$,

$$g(a + x_j) = g_a(x_j) = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}(x_j).$$

Matriciellement, cela s'écrit $\begin{pmatrix} g(a+x_1) \\ \vdots \\ g(a+x_n) \end{pmatrix} = {}^t M \begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix}$. On en déduit que $\begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix} = {}^t M^{-1} \begin{pmatrix} g(a+x_1) \\ \vdots \\ g(a+x_n) \end{pmatrix}$. Les coefficients de la matrice ${}^t M^{-1}$ étant indépendants de a, on en déduit que les fonctions $\lambda_1, \ldots, \lambda_n$ sont des combinaisons linéaires des fonctions $g_{x_1}, \ldots, g_{x_n}$. Elles sont dérivables comme ces dernières.

On a, pour tout réel x, $g(x + a) = \sum\limits_{i=1}^{n} \lambda_i(a) f_{a_i}(x)$. En dérivant par

et $\operatorname{Vect} A = ((\operatorname{Vect} A)^\circ)^\perp = (A^\circ)^\perp = 0^\perp = F$, puisqu'on est en dimension finie. On peut donc choisir des scalaires $x_1, \ldots, x_n$ tels que les formes linéaires $e_{x_1}, \ldots, e_{x_n}$ constituent une base de F^*. Montrons que le n-uplet $(x_1, \ldots, x_n)$ répond à la question.

Considérons la matrice $M = (f_i(x_j))_{1 \leqslant i,j \leqslant n}$ et montrons que les lignes $L_1, \ldots, L_n$ de M forment une famille libre. Soit $(\lambda_1, \ldots, \lambda_n) \in K^n$ tel que $\sum\limits_{i=1}^{n} \lambda_i L_i = 0$. On a alors, pour tout $j \in [\![1, n]\!]$, $\sum\limits_{i=1}^{n} \lambda_i f_i(x_j) = 0$, c'est-à-dire $e_{x_j}\left(\sum\limits_{i=1}^{n} \lambda_i f_i\right) = 0$. La famille $e_{x_1}, \ldots, e_{x_n}$ étant une base de F^*, on a donc $\sum\limits_{i=1}^{n} \lambda_i f_i \in (F^*)^\circ = \{0\}$. La famille $(f_1, \ldots, f_n)$ étant une base de F, on en déduit que $\lambda_1 = \cdots = \lambda_n = 0$. La matrice M est donc inversible.

2. Soit $f : \mathbb{R} \longrightarrow \mathbb{R}$, dérivable, dont les translatées engendrent un $\mathbb{R}$-espace vectoriel F de dimension finie n. On considère des réels $a_1, \ldots, a_n$ tels que la famille $(f_{a_1}, \ldots, f_{a_n})$ soit une base de F. D'après la question 1, il existe des réels $x_1, \ldots, x_n$ tels que la matrice $M = (f_{a_i}(x_j))_{1 \leqslant i,j \leqslant n}$ soit inversible. La fonction f étant dérivable, les fonctions f_{a_i} le sont également. Ainsi tout élément de F est dérivable.

Soit g un élément quelconque de F. Montrons que g' est encore dans F. Il est clair que, pour tout $a \in \mathbb{R}$, la fonction g_a est dans F. En effet, on a $g_a \in \operatorname{Vect}(f_{a_1+a}, \ldots, f_{a_n+a}) \subset F$. Il existe donc des réels $\lambda_1(a), \ldots, \lambda_n(a)$ tels que $g_a = \sum\limits_{i=1}^{n} \lambda_i(a) f_{a_i}$. Montrons que les fonctions λ_i sont dérivables. On a, pour $1 \leqslant j \leqslant n$,

$$g(a + x_j) = g_a(x_j) = \sum_{i=1}^{n} \lambda_i(a) f_{a_i}(x_j).$$

Matriciellement, cela s'écrit $\begin{pmatrix} g(a+x_1) \\ \vdots \\ g(a+x_n) \end{pmatrix} = {}^t M \begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix}$. On en déduit que $\begin{pmatrix} \lambda_1(a) \\ \vdots \\ \lambda_n(a) \end{pmatrix} = {}^t M^{-1} \begin{pmatrix} g(a+x_1) \\ \vdots \\ g(a+x_n) \end{pmatrix}$. Les coefficients de la matrice ${}^t M^{-1}$ étant indépendants de a, on en déduit que les fonctions $\lambda_1, \ldots, \lambda_n$ sont des combinaisons linéaires des fonctions $g_{x_1}, \ldots, g_{x_n}$. Elles sont dérivables comme ces dernières.

On a, pour tout réel x, $g(x + a) = \sum\limits_{i=1}^{n} \lambda_i(a) f_{a_i}(x)$. En dérivant par

rapport à a, on obtient $g'(x+a) = \sum_{i=1}^{n} \lambda_i'(a) f_{a_i}(x)$. On obtient en particulier, en prenant $a = 0$, $g' = \sum_{i=1}^{n} \lambda_i'(0) f_{a_i} \in \mathrm{F}$. On en déduit, de manière immédiate, que tout élément g de F est C^∞ et que, pour tout entier naturel k, on a $g^{(k)} \in \mathrm{F}$. C'est vrai en particulier pour la fonction f. L'espace vectoriel F étant de dimension finie n, il existe un entier p $(1 \leqslant p \leqslant n)$ tel que $f^{(p)} \in \mathrm{Vect}(f, f', \ldots, f^{(p-1)})$. La fonction f est solution d'une équation linéaire homogène à coefficients constants d'ordre p.

Réciproquement, si f est solution d'une équation linéaire homogène à coefficients constants d'ordre p, il est clair que, pour tout $a \in \mathbb{R}$, la fonction f_a est solution de la même équation différentielle. L'ensemble des solutions de cette équation différentielle étant un espace vectoriel de dimension p, les fonctions f_a engendrent un espace vectoriel de dimension finie inférieure ou égale à p.

Conclusion. Les translatés de f engendrent un espace vectoriel de dimension finie si, et seulement si, f est solution d'une équation linéaire homogène à coefficients constants. $\lhd$

Le lecteur trouvera d'autres exercices sur la dualité dans le chapitre 7 sur les matrices.

Les deux exercices qui suivent concernent la notion de famille positivement génératrice dans un espace vectoriel réel.

6.29. Familles positivement génératrices

Soit un espace vectoriel réel E de dimension $n \geqslant 1$ et une famille $\mathcal{F} = (e_1, e_1, \ldots, e_p)$ de vecteurs de E *positivement génératrice*, c'est-à-dire telle que pour tout $x \in \mathrm{E}$, il existe $(\lambda_1, \ldots, \lambda_p) \in (\mathbb{R}_+^*)^p$ tel que $x = \lambda_1 e_1 + \cdots + \lambda_p e_p$.

1. Montrer que $p \geqslant n+1$. Donner un exemple de famille positivement génératrice de cardinal $n+1$.

2. On suppose $p \geqslant 2n+1$. Montrer qu'il existe une sous-famille stricte de $\mathcal{F}$ qui est encore positivement génératrice. Donner un exemple de famille positivement génératrice de cardinal $2n$ dont aucune sous-famille stricte ne l'est.

(École normale supérieure)

$\rhd$ **Solution.**

1. Comme la famille $\mathcal{F}$ est génératrice, on a $p \geqslant n$. Si $p = n$, $\mathcal{F}$ est une base de E, et alors le vecteur $-e_1$ (par exemple) ne saurait être

obtenu comme combinaison à coefficients strictement positifs des e_i (par unicité de la décomposition). On a donc $p \geqslant n+1$.

Donnons-nous une base quelconque $(f_1, \ldots, f_n)$ de E et montrons que la famille $(f_1, \ldots, f_n, -f_1 - \cdots - f_n)$ est positivement génératrice. En effet, soit $x \in \mathrm{E}$, $x = x_1 f_1 + \cdots + x_n f_n$. Pour tout réel t on a

$$x = (x_1 + t)f_1 + \cdots + (x_n + t)f_n + t\Big(-\sum_{i=1}^{n} f_i\Big).$$

Il suffit de choisir t assez grand pour que tous les coefficients soient strictement positifs.

Notons que l'on montre de la même façon que toute famille génératrice $(f_1, \ldots, f_p)$ pour laquelle on a une relation de liaison $\lambda_1 f_1 + \cdots + \lambda_p f_p = 0$, avec des coefficients λ_i strictement positifs, est une famille positivement génératrice.

2. La famille $\mathcal{F}$ étant de rang n, il existe $\mathrm{I} \subset [\![1, p]\!]$ de cardinal n tel que $(e_i)_{i \in \mathrm{I}}$ soit une base de E. Posons $\mathrm{J} = [\![1, p]\!] \setminus \mathrm{I}$. Alors, la famille $(e_j)_{j \in \mathrm{J}}$ est liée car $|\mathrm{J}| \geqslant n+1$; on peut donc écrire une relation de liaison $\sum_{j \in \mathrm{J}} \lambda_j e_j = 0$, où les λ_j ne sont pas tous nuls. Par ailleurs, puisque la famille $(e_i)_{1 \leqslant i \leqslant p}$ est positivement génératrice, il existe des coefficients strictement positifs $t_1, \ldots, t_p$ tels que $t_1 e_1 + \cdots + t_p e_p = 0$. Pour tout réel x on a donc

$$\sum_{i \in \mathrm{I}} t_i e_i + \sum_{j \in \mathrm{J}} (t_j + x\lambda_j) e_j = 0.$$

On prend $x = -\dfrac{t_k}{\lambda_k}$, où $k \in \mathrm{J}$ est choisi de sorte que $\lambda_k \neq 0$ et que la valeur absolue du quotient $\dfrac{t_k}{\lambda_k}$ soit minimale. Pour cette valeur de x les coefficients $(t_j + x\lambda_j)$ restent tous positifs ou nuls. Notons K la partie formée des indices $j \in \mathrm{J}$ tels que $t_j + x\lambda_j > 0$. Il s'agit d'une partie stricte de J, car $k \notin \mathrm{K}$. La remarque faite à la fin de la question 1 montre que la famille $(e_i)_{i \in \mathrm{I} \cup \mathrm{K}}$ est encore positivement génératrice.

Si $(f_1, \ldots, f_n)$ est une base quelconque de E, alors la famille $(f_1, \ldots, f_n, -f_1, \ldots, -f_n)$ est de cardinal $2n$, positivement génératrice, mais aucune de ses sous-familles ne l'est. $\lhd$

L'exercice suivant va nous fournir une description des familles positivement génératrices du dual.

6.30. Familles positivement génératrices de E*

Soit E un $\mathbb{R}$-espace vectoriel de dimension n et p éléments $f_1, \ldots, f_p$ de son dual.

1. Montrer l'équivalence des deux propositions suivantes :

(i) $\forall x \in \mathrm{E}$, $\min\limits_{1 \leqslant i \leqslant p} f_i(x) \leqslant 0$;

(ii) $\exists (a_1, \ldots, a_p) \in (\mathbb{R}_+)^p - \{0\}$, $\sum\limits_{i=1}^{p} a_i f_i = 0$.

2. Montrer l'équivalence des deux propositions suivantes :

(i') $\forall x \in \mathrm{E} - \{0\}$, $\min\limits_{1 \leqslant i \leqslant p} f_i(x) < 0$;

(ii') $(f_1, \ldots, f_p)$ est une famille positivement génératrice de E*.

(École normale supérieure)

▷ **Solution.**

1. • Supposons (ii) vérifiée et raisonnons par l'absurde. Soit $x \in \mathrm{E}$ tel que, pour $1 \leqslant i \leqslant p$, on ait $f_i(x) > 0$. On a $\sum\limits_{i=1}^{p} a_i f_i(x) = 0$. Les termes de cette somme étant tous positifs, on en déduit que, pour $1 \leqslant i \leqslant p$, on a $a_i f_i(x) = 0$ et donc $a_i = 0$, car $f_i(x) > 0$. On a donc $(a_1, \ldots, a_p) = 0$, ce qui est contraire à l'hypothèse.

• Pour montrer que (i) implique (ii), raisonnons par récurrence sur p.

⋆ Si $p = 1$, alors, pour tout $x \in \mathrm{E}$, on a $f_1(x) \leqslant 0$ et $f_1(-x) \leqslant 0$ et donc $f_1(x) = 0$: f_1 est l'application nulle et $af_1 = 0$ pour tout $a > 0$.

⋆ Supposons que la famille $(f_1, \ldots, f_p)$ vérifie la propriété (i). Si f_p est l'application nulle, on conclut comme précédemment. Si $(f_1, \ldots, f_{p-1})$ vérifie (i), on applique directement l'hypothèse de récurrence et on prend $a_p = 0$. C'est fini. Ces cas étant écartés, soit H le noyau de f_p, et $e \in \mathrm{E}$ tel que $f_p(e) = 1$.

Considérons $x \in \mathrm{H}$ et $\alpha > 0$. Posons $y = x + \alpha e$. On obtient alors $f_p(y) = \alpha > 0$ et pour $1 \leqslant i \leqslant p-1$, $f_i(y) = f_i(x) + \alpha f_i(e)$. Supposons qu'il existe $x \in \mathrm{H}$ tel que $\min\limits_{1 \leqslant i \leqslant p-1} f_i(x) > 0$. Pour $\alpha > 0$, assez petit, on a alors $\min\limits_{1 \leqslant i \leqslant p-1} f_i(y) > 0$ et donc $\min\limits_{1 \leqslant i \leqslant p} f_i(y) > 0$, ce qui est contraire à l'hypothèse. On a donc, pour tout $x \in \mathrm{H}$, $\min\limits_{1 \leqslant i \leqslant p-1} f_i(x) \leqslant 0$. La famille $(g_1, \ldots, g_{p-1})$, où $g_i = f_{i|\mathrm{H}}$, vérifie (i). D'après l'hypothèse de récurrence, il existe $(a_1, \ldots, a_{p-1}) \in \mathbb{R}_+^{p-1} \setminus \{0\}$ tel que $\sum\limits_{i=1}^{p-1} a_i g_i = 0$. On a donc, pour tout $x \in \mathrm{H}$, $\sum\limits_{i=1}^{p-1} a_i f_i(x) = 0$. En posant $a_p = -\sum\limits_{i=1}^{p-1} a_i f_i(e)$, on obtient

finalement $\sum_{i=1}^{p} a_i f_i = 0$, puisque cette application linéaire s'annule en e et sur H et que $E = H \oplus \mathbb{R}e$.

Il reste à démontrer que $a_p \geqslant 0$. Raisonnons par l'absurde et supposons $a_p < 0$. La famille $(f_1, \ldots, f_{p-1}, -f_p)$ vérifie (ii) et donc aussi (i). Soit y un élément quelconque de E, $x \in H$ et $\alpha \in \mathbb{R}$ tel que $y = x + \alpha e$.

- Si $\alpha > 0$, on a $\min_{1 \leqslant i \leqslant p-1} f_i(y) = \min_{1 \leqslant i \leqslant p} f_i(y) \leqslant 0$, car $f_p(y) = \alpha > 0$.
- Si $\alpha < 0$, on obtient $\min_{1 \leqslant i \leqslant p-1} f_i(y) = \min(f_1(y), \ldots, f_{p-1}(y), -f_p(y))$ négatif ou nul, car $-f_p(y) = -\alpha > 0$.

Par continuité, la propriété reste vraie pour $\alpha = 0$ et on obtient pour tout $y \in E$, $\min_{1 \leqslant i \leqslant p-1} f_i(y) \leqslant 0$, cas qui a été écarté. On a donc $a_p \geqslant 0$, ce qui termine la démonstration.

2. • Supposons la propriété (i') vérifiée. Soit $f \in E^*$. Nous allons démontrer que pour $\lambda > 0$ assez petit les fonctions $(f_1 - \lambda f, \ldots, f_p - \lambda f)$ vérifient l'hypothèse (i) et appliquer le résultat de la première question.

Munissons E d'une norme quelconque (elles sont toutes équivalentes, car nous sommes en dimension finie) et notons S la sphère unité de E : S est compacte. Les fonctions f_i sont linéaires donc continues, puisque E est de dimension finie. On en déduit que la fonction $g = \min_{1 \leqslant i \leqslant p} f_i$ est elle aussi continue (cela se montre aisément par récurrence sur p, à partir de l'égalité $\min(f_1, f_2) = \dfrac{f_1 + f_2}{2} - \dfrac{|f_1 - f_2|}{2}$). Comme g est continue sur le compact S, elle y est majorée et sa borne supérieure M est atteinte. De plus, g étant strictement négative sur S, on a $M < 0$.

Pour les mêmes raisons, $|f|$ est majorée sur le compact S, par $a > 0$. Soit $\lambda > 0$ et $h = \min_{1 \leqslant i \leqslant p} f_i - \lambda f$. On a, pour tout $x \in S$ et $1 \leqslant i \leqslant p$,

$$f_i(x) - \lambda f(x) \leqslant f_i(x) + \lambda a \text{ (car } f(x) \geqslant -a).$$

On en déduit que, pour tout $x \in S$,

$$h(x) \leqslant g(x) + \lambda a \leqslant M + \lambda a.$$

Si donc on choisit $\lambda < -\dfrac{M}{a}$, alors, on a, pour tout $x \in S$, $h(x) < 0$. D'autre part, pour tout $x \in E - \{0\}$, il existe $u \in S$ et $\alpha \in \mathbb{R}_+^*$ tels que $x = \alpha u$. On a alors $h(x) = \alpha h(u) < 0$ de sorte que $h(x) \leqslant 0$ pour tout $x \in E$.

Les fonctions $g_1, \ldots, g_p$ définies par $g_i(x) = f_i(x) - \lambda f(x)$, pour $x \in E$ et $1 \leqslant i \leqslant p$ vérifient alors la condition (i) de la première question. On en déduit qu'il existe $(a_1, \ldots, a_p) \in \mathbb{R}_+^p - \{0\}$ tel que

$$\sum_{i=1}^{p} a_i g_i = \sum_{i=1}^{p} a_i (f_i - \lambda f) = 0.$$

ce qui peut s'écrire

$$f = \frac{1}{\lambda \sum\limits_{i=1}^{p} a_i} \sum_{i=1}^{p} a_i f_i,$$

puisque $\lambda \sum\limits_{i=1}^{p} a_i > 0$, ($\lambda > 0$ et les a_i sont positifs et non tous nuls).

Ainsi, tout élément $f \in \mathrm{E}^*$ s'écrit comme combinaison linéaire à coefficients positifs de $(f_1, \ldots, f_p)$. En considérant $f - \sum\limits_{i=1}^{p} f_i$, au lieu de f, on peut même supposer que les coefficients sont strictement positifs.

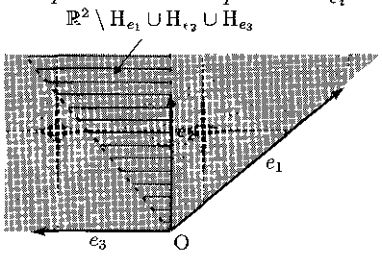
Cela prouve donc que $(f_1, \ldots, f_p)$ est une famille positivement génératrice de E^*.

• Supposons que tout élément de E^* soit combinaison linéaire à coefficients strictement positifs de $f_1, \ldots, f_p$. Soit $x \in \mathbf{E}$ et $f \in \mathbf{E}^*$ tel que $f(x) = -1$. Il existe $(a_1, \ldots, a_p) \in (\mathbb{R}_+^*)^p$ tel que $f = \sum\limits_{i=1}^{p} a_i f_i$. On ne peut avoir $\min\limits_{1 \leqslant i \leqslant p} f_i(x) \geqslant 0$, car sinon $f(x) \geqslant 0$. On a donc $\min\limits_{1 \leqslant i \leqslant p} f_i(x) < 0$ et (i') est vérifiée. $\lhd$

On peut en déduire une caractérisation géométrique des familles positivement génératrices de E *moyennant l'identification de* **E** *avec son bidual* E^{**} *qui est le dual de* E^*. *On rappelle que l'application qui à tout vecteur* $x \in \mathrm{E}$ *associe l'application* $\hat{x} \in \mathrm{E}^{**}$ *définie par* $\hat{x}(f) = f(x)$ *pour tout* $f \in \mathrm{E}^*$ *est un isomorphisme. L'équivalence de la question 2 se traduit ainsi : une famille* $(e_1, \ldots, e_p)$ *de* E *est positivement génératrice si, pour tout* $f \in \mathrm{E}^*$, *il existe* $i \in [\![1, p]\!]$ *tel que* $f(e_i) < 0$.

Si E *est muni d'une structure euclidienne, les formes linéaires sur* **E** *sont les* $f_x : y \longmapsto (x, y)$. *Il en résulte que* $(e_1, \ldots, e_p)$ *de* E *est positivement génératrice si tout vecteur non nul* x *de* **E**, *il existe* $i \in [\![1, p]\!]$ *tel que* $(x, e_i) < 0$. *Autrement dit, si* **E** *la réunion des* H_{e_i} *où* H_y *désigne le demi-espace ouvert défini par* $\mathrm{H}_y = \{x \in \mathrm{E}, \langle x, y \rangle < 0\}$ *(on pose* $\mathrm{H}_0 = \emptyset$*).*

Voici un exemple dans $\mathbb{R}^2$ *: en grisé figure le cône positif engendré par* e_1, e_2 *et* e_3, *c'est-à-dire l'ensemble des combinaisons linéaires à coefficients positifs de* e_1, e_2, e_3. *La famille n'est pas positivement génératrice car la zone grisée n'est pas recouverte par les* H_{e_i}.



Les derniers exercices de ce chapitre auront pour cadre des algèbres.

6.31. Caractérisation de $\mathbb{C}$

Soit K une algèbre sans diviseur de zéro sur $\mathbb{R}$ de dimension finie $n \geqslant 2$. On identifie $\mathbb{R}$ avec $\mathbb{R}.1$ où 1 est l'élément neutre de K pour le produit.

1. Montrer que tout élément non nul de K est inversible.

2. Soit $a \in \mathrm{K}$ n'appartenant pas à $\mathbb{R}$. Montrer que $(1, a)$ est libre et que $(1, a, a^2)$ est liée.

3. Montrer l'existence de $i \in \mathrm{K}$ tel que $i^2 = -1$.

4. Montrer que si K est commutative alors K est isomorphe à $\mathbb{C}$.

(École normale supérieure)

▷ **Solution.**

1. Soit a un élément non nul de K. Par intégrité de K, l'application $\mathbb{R}$-linéaire $x \mapsto ax$ est injective, donc bijective puisque K est de dimension finie. Il existe donc $b \in \mathrm{K}$ tel que $ab = 1$ ce qui montre que a est inversible à droite. De la même manière on prouve l'existence de c tel que $ca = 1$. En multipliant cette dernière égalité à droite par b on a $c = b$. Donc a est inversible.

2. Dire que a n'est pas réel revient à dire que la famille $(1, a)$ est $\mathbb{R}$-libre. Notons qu'un tel élément a existe car $n = \dim \mathrm{K} \geqslant 2$. Comme K est de dimension finie, la famille $(a^k)_{k \geqslant 0}$ est liée et l'idéal des polynômes $\mathrm{P} \in \mathbb{R}[\mathrm{X}]$ tels que $\mathrm{P}(a) = 0$ est non nul. Notons Q le générateur unitaire de cet idéal (c'est le polynôme minimal de a). Comme K est intègre, Q est irréductible sur $\mathbb{R}$. Comme $a \notin \mathbb{R}$, le degré de Q n'est pas égal à 1. Par suite Q est de degré 2 et on en déduit que la famille $(1, a, a^2)$ est liée.

3. Notons qu'un réel λ commute avec tout élément x de K : en effet, comme K est une $\mathbb{R}$-algèbre, on peut écrire

$$\lambda x = (\lambda 1)x = \lambda(1x) = \lambda(x1) = x(\lambda 1) = x\lambda.$$

Soit toujours a choisi comme précédemment et α, β les réels tels que $a^2 = \alpha + \beta a$. Bien entendu α est non nul car $a \notin \mathbb{R}$. On va chercher notre élément i dans le plan $\mathrm{Vect}(1, a)$. Pour $(x, y) \in \mathbb{R}^2$ on a

$$(x + ay)^2 = x^2 + 2xya + y^2a^2 = (x^2 + \alpha y^2) + (2xy + \beta y^2)a.$$

On cherche donc x, y tels que $\begin{cases} x^2 + \alpha y^2 = -1 \\ 2xy + \beta y^2 = 0 \end{cases}$. On doit prendre y non nul, ce qui impose $x = -\dfrac{\beta y}{2}$. En substituant dans la première équation

on obtient $y^2\left(\alpha + \frac{\beta^2}{4}\right) = -1$. Cette équation admet bien deux solutions car $\alpha + \frac{\beta^2}{4} < 0$ puisque le polynôme $Q(X) = X^2 - \beta X - \alpha$ est irréductible sur $\mathbb{R}$. Il existe donc deux éléments (opposés) i dans $\mathrm{Vect}(1, a)$ tels que $i^2 = -1$.

4. Le plan vectoriel $\mathrm{Vect}(1, i) = \mathrm{Vect}(1, a)$ est clairement une sous-algèbre de K qui est isomorphe à $\mathbb{C}$. On va prouver que si K est supposée commutative alors $K = \mathrm{Vect}(1, i)$. Soit b un élément quelconque de $K \setminus \mathbb{R}$. La question précédente appliquée avec b à la place de a montre l'existence d'une racine carrée de -1 dans le plan $\mathrm{Vect}(1, b)$. Or, comme K est commutative et intègre, l'équation $z^2 = -1$ n'a que deux solutions à savoir i et $-i$. On a donc forcément $\mathrm{Vect}(1, b) = \mathrm{Vect}(1, a) = \mathrm{Vect}(1, i)$. Par suite $K = \mathrm{Vect}(1, i)$ et K est isomorphe à $\mathbb{C}$. $\lhd$

L'exercice suivant offre une version plus complète qui caractérise toutes les algèbres réelles sans diviseur de zéro et de dimension finie.

6.32. Théorème de Frobenius

Soit A une $\mathbb{R}$-algèbre sans diviseurs de 0 et de dimension finie $n \geqslant 2$. On identifie $\mathbb{R}$ avec $\mathbb{R}1$ où 1 est l'élément neutre de A pour le produit.

1. Soit $x \in A$. Montrer qu'il existe $(a, b) \in \mathbb{R}^2$ tel que

$$x^2 + ax + b = 0.$$

2. Soit $x \in A$ tel que $x^2 \in \mathbb{R}^+$. Montrer que $x \in \mathbb{R}$.

3. Soit $V = \{x \in A,\ x^2 \in \mathbb{R}^-\}$. Montrer que tout $x \in A$ s'écrit de manière unique $x = r + v$ avec $r \in \mathbb{R}$ et $v \in V$.

4. Soit (u, v) une famille libre d'éléments de V et $\lambda \in \mathbb{R}$. Montrer que $u - \lambda v \notin \mathbb{R}$.

5. Montrer que V est un sous-espace vectoriel de A.

6. On suppose A de dimension 2. Montrer que A est isomorphe à $\mathbb{C}$.

7. On pose $\langle u, v\rangle = -(uv + vu)$ pour tout $(u, v) \in A^2$. Montrer que cela définit un produit scalaire sur V.

8. On suppose que $\dim A \geqslant 3$. Montrer qu'il existe i, j dans V tels que $\langle i, j\rangle = 0$, $i^2 = -1$, $j^2 = -1$ et que $(1, i, j, ij)$ est une $\mathbb{R}$-base de A.

(École normale supérieure)

$\rhd$ **Solution.**

1. Si x^2 est réel, on prend $a = 0$ et $b = -x^2$. Sinon x n'est pas réel et la famille $(1, x)$ est libre. Comme A de dimension finie, la famille $(x^k)_{k\in\mathbb{N}}$ est liée et il existe $P \in \mathbb{R}[X]$, non nul tel que $P(x) = 0$. On

décompose P en produit de polynômes irréductibles $P = P_1P_2 \dots P_n$. Il existe $k \in [\![1, n]\!]$ tel que $P_k(x) = 0$, car A n'a pas de diviseur de 0. Le polynôme P_k est de degré 2 puisque la famille $(1, x)$ est libre. En divisant par le coefficient de x^2, on obtient $(a, b) \in \mathbb{R}^2$ tel que $x^2 + ax + b = 0$.

2. Notons qu'un élément de A commute avec tout réel. En effet, si $x \in \mathbb{R}$ et $\lambda \in \mathbb{R}$, $x\lambda = x(\lambda 1) = \lambda(x1) = \lambda x$, car A est une $\mathbb{R}$-algèbre.

Soit $x \in A$ tel que $x^2 \in \mathbb{R}_+$ et λ une racine carrée réelle de x^2. On a alors $x^2 - \lambda^2 = 0$. Mais $x^2 - \lambda^2 = (x - \lambda)(x + \lambda)$ car $\lambda x = x\lambda$. On a donc $x = \pm\lambda$, car A n'a pas de diviseur de 0, et x est dans $\mathbb{R}$.

3. Soit $x \in A$.

• Pour l'existence, on considère $(a, b) \in \mathbb{R}^2$ tel que $x^2+ax+b = 0$. On peut écrire cette égalité $\left(x + \dfrac{a}{2}\right)^2 = \dfrac{a^2 - 4b}{4}$ (car x commute avec $\dfrac{a}{2}$).

Si $\dfrac{a^2 - 4b}{4} \in \mathbb{R}_+$, alors d'après la question 2, $x + \dfrac{a}{2}$ est réel donc x est réel. Il s'écrit $x = x + 0$, avec $x \in \mathbb{R}$ et $0 \in V$.

Si $\dfrac{a^2 - 4b}{4} \in \mathbb{R}_-$, alors $v = x + \dfrac{a}{2} \in V$ et $x = -\dfrac{a}{2} + v$.

• Montrons l'unicité de cette décomposition. Soit $(r, r') \in \mathbb{R}^2$, $(v, v') \in V^2$ tels que $r + v = r' + v'$. En élevant au carré, on en déduit que ${v'}^2 = (r - r' + v)^2 = (r - r')^2 + v^2 + 2(r - r')v$. Les carrés sont réels, donc si $r \neq r'$, v est réel et donc $v = 0$, puisque $v^2 \leqslant 0$. On obtient ${v'}^2 = (r-r')^2 \in \mathbb{R}_+$ et donc $v' = 0$, puis $r = r'$, ce qui est contradictoire. On conclut : $r = r'$ et $v = v'$.

4. Si $v \in V$ et $\lambda \in \mathbb{R}$, alors $(\lambda v)^2 = \lambda^2 v^2 \in \mathbb{R}_-$ et donc $\lambda v \in V$. S'il existe $r \in \mathbb{R}$ tel que $u = \lambda v + r$, par l'unicité de la décomposition étudiée dans la question 3, on obtient $r = 0$ et $u = \lambda v$, ce qui contredit la liberté de la famille (u, v).

5. L'ensemble V contient 0.

Si $v \in V$ et $\lambda \in V$, on a montré dans la question 4 que $\lambda v \in V$.

Soit u et v deux éléments de V. Si la famille (u, v) est liée, il existe par exemple $\lambda \in \mathbb{R}$ tel que $v = \lambda u$. On a alors $u + v = (1 + \lambda)u \in V$. Supposons donc la famille (u, v) libre.

En particulier, u n'est pas nul. Montrons que u est inversible. L'application $x \longmapsto ux$ est $\mathbb{R}$-linéaire. Son noyau est réduit à $\{0\}$ car A n'a pas de diviseur de 0. On en déduit qu'elle est bijective car A est de dimension finie. Ainsi il existe $u' \in A$ tel que $uu' = 1$. On montre de même qu'il existe $u'' \in A$ tel que $u''u = 1$. En considérant $u''uu'$, on montre que $u' = u''$, donc que u est inversible.

Considérons le produit uvu^{-1}. On a

$$(uvu^{-1})^2 = uv^2u^{-1} = v^2uu^{-1} = v^2,$$

car v^2 est réel, donc $uvu^{-1} = \pm v$, c'est-à-dire $uv = \pm vu$.

Si $uv = -vu$, $(u + v)^2 = u^2 + v^2 \in \mathbb{R}_-$ et $u + v \in V$. Si $uv = vu$, $(uv)^2 = u^2v^2 \in \mathbb{R}_+$ et $uv \in \mathbb{R}$. Mais alors $(u + v)^2 = u^2 + v^2 + 2uv \in \mathbb{R}$

et comme d'après la question précédente, $u+v \notin \mathbb{R}$, $(u+v)^2 \in \mathbb{R}_-$ et $u+v \in \mathrm{V}$. Dans tous les cas, $u+v \in \mathrm{V}$ et V est un sous-espace vectoriel de A.

6. Soit v un élément non nul de V (un tel élément existe sinon on a $\mathrm{A} = \mathbb{R}$). Comme $v^2 \in \mathbb{R}_-^*$, il existe $\lambda > 0$ tel que $v^2 = -\lambda^2$. Alors $\left(\frac{v}{\lambda}\right)^2 = -1$. On note $i = \frac{v}{\lambda}$. La famille $(1, i)$ est libre donc c'est une base de A et $\mathrm{A} = \mathbb{R} + \mathbb{R}i$ est isomorphe à $\mathbb{C}$.

7. Pour tout couple $(u, v) \in \mathrm{V}^2$, on a $\langle u, v\rangle = u^2 + v^2 - (u+v)^2 \in \mathbb{R}$, car $u+v \in \mathrm{V}$ donc chaque carré est réel.

L'application $(u, v) \longmapsto \langle u, v\rangle$ est clairement bilinéaire et symétrique. Cela résulte des propriétés d'une algèbre.

Enfin $\langle u, u\rangle = -2u^2 \in \mathbb{R}_+$ car $u^2 \in \mathbb{R}_-$ et $\langle u, u\rangle = 0$ implique $u = 0$, car A n'a pas de diviseur de 0. On a bien un produit scalaire.

8. On montre comme dans la question 6 qu'il existe $i \in \mathrm{V}$ tel que $i^2 = -1$. D'après la question 3, on a $\mathrm{A} = \mathbb{R} \oplus \mathrm{V}$. Comme $\dim \mathrm{A} \geqslant 3$, on a $\dim \mathrm{V} \geqslant 2$ et $\dim i^\perp \geqslant 1$. Soit $v \in i^\perp$, non nul. Il existe $\mu \in \mathbb{R}_+^*$ tel que $v^2 = -\mu^2$ et $j = \frac{v}{\mu}$ vérifie $j^2 = -1$ et $\langle i, j\rangle = 0$.

De $\langle i, j\rangle = 0$, on déduit $ji = -ij$ et $(ij)^2 = ijij = -i^2j^2 = -1$. Ainsi on a $ij \in \mathrm{V}$ et $ij \neq 0$. On a de plus $i(ij) = i^2j = -j = (ji)i = -(ij)i$ donc $\langle ij, i\rangle = 0$ et de même $\langle ij, j\rangle = 0$.

La famille (i, j, ij) est donc libre. Supposons que $\dim \mathrm{V} > 3$. On peut trouver $k \in (\mathrm{Vect}(i, j, ij))^\perp$, non nul. Il vérifie $ik = -ki$, $jk = -kj$ et $ijk = -kij$. On en déduit

$$ijk = -ikj = kij = -ijk$$

et donc $ijk = 0$, ce qui impossible car A ne possède pas de diviseur de 0. Ainsi V est de dimension 3, engendré par (i, j, ij). Comme $\mathrm{A} = \mathbb{R} \oplus \mathrm{V}$, on en déduit que $\mathrm{A} = \mathrm{Vect}(1, i, j, ij)$. $\lhd$

Dans le cas où A est de dimension supérieure ou égale à 3, on obtient une algèbre de dimension 4, de base $(1, i, j, k)$ où i, j, k vérifient $i^2 = j^2 = k^2 = ijk = -1$. Les éléments i, j, k anticommutent. Cette algèbre est un corps (puisque tout élément non nul est inversible), non commutatif, appelé corps des quaternions ; il est noté $\mathbb{H}$.

Il résulte de l'exercice que les seules $\mathbb{R}$-algèbres de dimension finie et sans diviseur de 0 sont $\mathbb{R}$, $\mathbb{C}$ et $\mathbb{H}$. Ce théorème a été démontré par le mathématicien allemand Georg Frobenius (1878) et indépendamment par le mathématicien et philosophe américain Charles Pierce (1880).

6.33. Sous-algèbres de dimension finie de $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$

Déterminer les sous-algèbres de dimension finie de $\mathcal{C}^0(\mathbb{R}, \mathbb{R})$.
(École normale supérieure)

▷ **Solution.**

Soit $f \in \mathcal{C}^0(\mathbb{R}, \mathbb{R})$, non constante. Alors la famille $(f^n)_{n \geq 0}$ est libre. En effet, une relation de liaison $\lambda_0 + \lambda_1 f + \cdots + \lambda_p f^p = 0$ implique que le polynôme $P = \lambda_0 + \lambda_1 X + \cdots + \lambda_p X^p$ s'annule sur l'image de f. Celle-ci étant un intervalle (d'après le théorème des valeurs intermédiaires), non réduit à un point par hypothèse, elle est de cardinal infini et $P = 0$. Il en résulte que la seule sous-algèbre de dimension finie est l'algèbre des fonctions constantes, qui est de dimension 1. ◁

Si A *est une* K*-algèbre, une dérivation de* A *est un endomorphisme* D *qui vérifie* $D(ab) = D(a)b + aD(b)$ *pour tout* $(a, b) \in A^2$. *Cette notion algébrique, directement inspirée de la dérivation analytique usuelle, a servi de thème à plusieurs exercices posés à l'ENS de Lyon.*

6.34. Racine carrée de la dérivation

Soit $E = \mathcal{C}^\infty(\mathbb{R}, \mathbb{C})$ et $D : E \to E$ l'opérateur de dérivation. Existe-t-il T dans $\mathcal{L}(E)$ tel que $T \circ T = D$?

(École normale supérieure)

▷ **Solution.**

Supposons que T existe. Considérons $\operatorname{Ker} D^2$, qui est un plan vectoriel isomorphe à $\mathbb{C}_1[X]$. Il est évidemment stable par D, mais aussi par T, car les endomorphismes T et D commutent, puisque $T \circ D = T^3 = D \circ T$. Notons d et t les restrictions de D et T à $\operatorname{Ker} D^2$. On a $t^2 = d$ et $d^2 = 0$. On en déduit que $t^4 = 0$. Ainsi t est nilpotent. Son indice de nilpotence est inférieur ou égal à la dimension de $\operatorname{Ker} D^2$, qui est 2 (voir l'exercice 6.8 et la remarque qui le suit), donc $d = t^2 = 0$. Mais c'est absurde, car $d \neq 0$.

Conclusion. L'opérateur D n'a pas de racine carrée. ◁

6.35. Φ-dérivation (1)

Soit A une $\mathbb{R}$-algèbre et $\Phi : A \to \mathbb{R}$ un morphisme d'algèbres. On appelle Φ-dérivation de A toute forme linéaire δ sur A qui vérifie, pour tout $(a, b) \in A^2$, $\delta(ab) = \Phi(a)\delta(b) + \delta(a)\Phi(b)$.

Déterminer tous les morphismes d'algèbre $\Phi : \mathbb{R}[X] \to \mathbb{R}$, puis toutes les Φ-dérivations de $\mathbb{R}[X]$.

(École normale supérieure)

▷ **Solution.**

- Soit Φ un morphisme de $\mathbb{R}[X]$ dans $\mathbb{R}$. Il est clair que Φ va être

déterminé par l'image de X. En effet, posons $\Phi(X) = \alpha$. On alors, pour tout $n \in \mathbb{N}$, $\Phi(X^n) = \alpha^n$, puis par linéarité de Φ, pour tout $P \in \mathbb{R}[X]$, $\Phi(P) = P(\alpha)$. Réciproquement, il est clair que, pour tout réel α, l'application $\Phi : P \longmapsto P(\alpha)$ est un morphisme d'algèbres de $\mathbb{R}[X]$ dans $\mathbb{R}$.

• Si Φ est le morphisme $P \longmapsto P(\alpha)$, on peut remarquer que l'application $P \longmapsto P'(\alpha)$ est alors une Φ-dérivation. Cherchons les autres. Soit D une forme linéaire sur $\mathbb{R}[X]$ vérifiant, pour tout $(A, B) \in \mathbb{R}[X]^2$, $D(AB) = \Phi(A)D(B) + \Phi(B)D(A)$. On a $D(1) = D(1 \times 1) = 2D(1)$ et donc $D(1) = 0$. Posons $D(X) = k \in \mathbb{R}$. On obtient alors successivement

$$D(X^2) = 2\Phi(X)D(X) = 2k\alpha,$$
$$D(X^3) = \Phi(X)D(X^2) + \Phi(X^2)D(X) = 2k\alpha^2 + k\alpha^2 = 3k\alpha^2.$$

On montre par récurrence sur n que $D(X^n) = kn\alpha^{n-1}$ pour tout $n \in \mathbb{N}^*$. C'est vrai pour $1 \leqslant n \leqslant 3$ et si $D(X^n) = kn\alpha^{n-1}$ alors

$$D(X^{n+1}) = \Phi(X)D(X^n) + \Phi(X^n)D(X) = \alpha(kn\alpha^{n-1}) + \alpha^n(k) = k(n+1)\alpha^n.$$

On note que $n\alpha^{n-1}$ est la dérivée en α de X^n. Par linéarité de D, on en déduit que, pour tout polynôme P, on a

$$D(P) = kP'(\alpha).$$

Réciproquement, si D est la forme linéaire définie par $D(P) = kP'(\alpha)$, on a, pour $(A, B) \in \mathbb{R}[X]^2$,

$$\begin{aligned} D(AB) &= k(AB)'(\alpha) = kA(\alpha)B'(\alpha) + kA'(\alpha)B(\alpha) \\ &= \Phi(A)D(B) + \Phi(B)D(A). \lhd \end{aligned}$$

6.36. Φ-dérivation (2)

Dans cet exercice, A désigne l'algèbre des suites réelles (a_n) telles que la série entière $\sum a_n x^n$ ait un rayon de convergence supérieur ou égal à $R > 0$ fixé.

1. Quels sont les morphismes d'algèbres de A dans $\mathbb{R}$?

2. Soit Φ un tel morphisme. Quelles sont les Φ-dérivations de l'algèbre A ?

(École normale supérieure)

$\rhd$ **Solution.**

1. Il résulte du cours d'analyse que A est bien une algèbre, pour l'addition usuelle des suites et le produit de convolution. Par ailleurs, l'application qui à une suite (a_n) de A associe l'application $f :]-R, R[\to \mathbb{R}$

définie par $f(x) = \sum_{n=0}^{+\infty} a_n x^n$ est un morphisme injectif d'algèbres, permettant d'identifier A à une sous-algèbre de $\mathcal{F}(]-R, R[, \mathbb{R})$, l'algèbre des fonctions développables en série entière en 0 avec un rayon de convergence supérieur ou égal à R. Nous ferons cette identification dans la suite en regardant les éléments de A comme des fonctions définies sur $]-R, R[$.

Soit Φ un morphisme d'algèbres de A dans $\mathbb{R}$. L'ensemble $\mathcal{P}$ des fonctions polynômes de $]-R, R[$ dans $\mathbb{R}$ forme une sous-algèbre de A, isomorphe à $\mathbb{R}[X]$. La restriction de Φ à $\mathcal{P}$ est un morphisme d'algèbres de $\mathcal{P}$ dans $\mathbb{R}$. En reprenant la démonstration de l'exercice précédent, on montre qu'il existe $\alpha \in \mathbb{R}$ tel que $\Phi(P) = P(\alpha)$ pour toute fonction polynôme P.

Lorsque a est un réel de $]-R, R[$, il est clair que l'application $\Phi_a : A \to \mathbb{R}$ qui à $f \in A$ associe $f(a)$ est un morphisme d'algèbres de A dans $\mathbb{R}$, que nous appellerons morphisme d'évaluation en a. Il semble assez naturel de penser que le réel α défini ci-dessus appartient nécessairement à l'intervalle $]R, R[$ et que Φ n'est rien d'autre que le morphisme d'évaluation en α.

• Commençons par montrer que $\alpha = \Phi(\mathrm{Id}) \in]-R, R[$. Raisonnons par l'absurde et supposons que $|\alpha| \geqslant R$. Dans ce cas, la fonction f définie par $f(x) = \sum_{n=0}^{+\infty} \frac{x^n}{\alpha^n}$ appartient à A, puisque la série entière $\sum \frac{x^n}{\alpha^n}$ est de rayon $|\alpha| \geqslant R$. Or, nous savons que, pour $|x| < \alpha$, $f(x) = \dfrac{1}{1 - \frac{x}{\alpha}}$, ce qui s'écrit encore $\left(1 - \frac{1}{\alpha}\,\mathrm{Id}\right) f = 1$. Si on applique le morphisme Φ à cette égalité, il vient $\left(1 - \frac{1}{\alpha}\Phi(\mathrm{Id})\right)\Phi(f) = (1-1)\Phi(f) = 1$, soit $1 = 0$, ce qui est clairement absurde. Ainsi, le réel α appartient à $]-R, R[$.

• Soit $g \in A$. On va montrer que $\Phi(g) = g(\alpha)$. Cela revient à prouver que $\Phi(g - g(\alpha)) = 0$. Soit la fonction h définie par $h(x) = \dfrac{g(x) - g(\alpha)}{x - \alpha}$, prolongée par continuité en α par $h(\alpha) = g'(\alpha)$. Il suffit de montrer que $h \in A$. En effet, dans ce cas, on pourra écrire $g - g(\alpha) = (\mathrm{Id} - \alpha)h$ et en appliquant Φ, il viendra $\Phi(g) - g(\alpha) = (\Phi(\mathrm{Id}) - \alpha)\Phi(h) = 0$, c'est-à-dire $\Phi(g) = g(\alpha)$.

Si $\alpha = 0$, il est clair que $h \in A$: en posant $g(x) = \sum_{n=0}^{+\infty} a_n x^n$, on a simplement $h(x) = \sum_{n=1}^{+\infty} a_n x^{n-1}$.

Supposons α non nul. Puisque h est continue en α, la relation qui définit h équivaut à $h(x)(x - \alpha) = g(x) - g(\alpha)$, pour tout $x \in]-R, R[$. Considérons la suite (a_n) telle que $g(x) - g(\alpha) = \sum_{n=0}^{+\infty} a_n x^n$ et cherchons

une suite (b_n) telle que $h(x) = \sum_{n=0}^{+\infty} b_n x^n$. La relation qui lie g et h équivaut à : $-\alpha b_0 = a_0$ et pour tout $n \in \mathbb{N}$, $b_{n-1} - \alpha b_n = a_n$. On en déduit facilement par récurrence que, pour tout entier naturel n,

$$b_n = -\sum_{k=0}^{n} a_k \alpha^{k-n-1} = \sum_{k=n+1}^{+\infty} a_k \alpha^{k-n-1},$$

puisque $\sum_{k=0}^{+\infty} a_k \alpha^k = g(\alpha) - g(\alpha) = 0$. Si $r \in]|\alpha|, \mathrm{R}[$, la suite $(a_n r^n)$ est bornée. Considérons $\mathrm{M} > 0$ tel que $|a_n r^n| \leqslant \mathrm{M}$ pour tout n. On a alors, pour tout $n \in \mathbb{N}$,

$$|b_n r^n| = \left| \sum_{k=n+1}^{+\infty} a_k r^n \alpha^{k-n-1} \right| \leqslant \sum_{k=n+1}^{+\infty} \mathrm{M} r^{n-k} |\alpha|^{k-n-1} = \frac{\mathrm{M}}{r} \sum_{i=0}^{+\infty} \left(\frac{|\alpha|}{r} \right)^i$$
$$= \frac{\mathrm{M}}{r - |\alpha|}.$$

Comme la suite $(b_n r^n)$ est bornée, le rayon de convergence de la série entière $\sum b_n x^n$ est supérieur à r. Puisque cela vaut pour tout $r \in]|\alpha|, \mathrm{R}[$, le rayon de convergence est bien supérieur ou égal à R. On a donc, pour tout $x \in]-\mathrm{R}, \mathrm{R}[$, $h(x) = \sum_{n=0}^{+\infty} b_n x^n$: la fonction h appartient à A.

Conclusion. Les seuls morphismes d'algèbres de A dans $\mathbb{R}$ sont les morphismes d'évaluation en un point de l'intervalle $]-\mathrm{R}, \mathrm{R}[$.

2. Soit $\alpha \in]-\mathrm{R}, \mathrm{R}[$ et soit D une Φ_α-dérivation de A. On sait d'après l'exercice précédent qu'il existe $k \in \mathbb{R}$ tel que, pour toute fonction polynôme P, $\mathrm{D}(\mathrm{P}) = k\mathrm{P}'(\alpha)$. Soit $g \in \mathrm{A}$. Comme ci-dessus, on introduit la fonction $h \in \mathrm{A}$ telle que $g - g(\alpha) = (\mathrm{Id} - \alpha)h$ et on applique D à cette égalité. Il vient

$$\mathrm{D}(g) = \mathrm{D}(\mathrm{Id} - \alpha)\Phi_\alpha(h) + \Phi_\alpha(\mathrm{Id} - \alpha)\mathrm{D}(h) = k\Phi_\alpha(h) = kh(\alpha) = kg'(\alpha),$$

car, $\mathrm{Id} - \alpha$ étant une fonction polynôme, $\mathrm{D}(\mathrm{Id} - \alpha) = k$.

Conclusion. Comme dans le cas des polynômes, les seules Φ_α-dérivations de A sont les applications qui à $f \in \mathrm{A}$ associe $kf'(\alpha)$. $\lhd$

6.37. Φ-dérivation (3)

Soit $\mathrm{E} = \mathcal{C}^0(\mathbb{R}, \mathbb{R})$. Déterminer les formes linéaires $\mathrm{D} : \mathrm{E} \to \mathbb{R}$ vérifiant, pour tout $(f, g) \in \mathrm{E}^2$,

$$\mathrm{D}(fg) = f(0)\mathrm{D}(g) + g(0)\mathrm{D}(f).$$

(**École normale supérieure**)

▷ **Solution.**

Si on note 1 la fonction constante $x \longmapsto 1$, on a $D(1) = D(1)+D(1)$ et donc $D(1) = 0$. On en déduit que D est nulle pour toutes les applications constantes. Si $f \in E$, on peut écrire $f = (f - f(0)) + f(0)$. Par linéarité, on obtient $D(f) = D(f - f(0))$ et on est donc ramené à étudier la restriction de D aux applications nulles en 0. Il est clair que si $f \in E$ est une application qui vérifie $f(0) = 0$, alors on a $D(f^2) = 0$.

Soit maintenant $f \in E$ telle que $f(0) = 0$. Si f est positive, on peut écrire $f = g^2$ où $g = \sqrt{f} \in E$ vérifie $g(0) = 0$. D'après ce qui précède, on a $D(f) = 0$. Dans le cas général, il est possible d'écrire f comme différence de deux fonctions continues, positives et nulles en 0. Il suffit de prendre

$$g(x) = \max(f(x), 0) \text{ et } h(x) = \max(-f(x), 0).$$

On a $f = g - h$, $g \geqslant 0$, $h \geqslant 0$ et $g(0) = h(0) = 0$. Par linéarité de D, on obtient $D(f) = D(g) - D(h) = 0$.

Conclusion. Le seule forme linéaire D qui convienne est donc la forme nulle. ◁

On termine cette série d'exercices sur les algèbres avec l'énoncé suivant.

6.38. Étude d'une algèbre

Soit $E = C^\infty(\mathbb{R}, \mathbb{R})$ et A l'ensemble des $\varphi \in \mathcal{L}(E)$ tels qu'il existe une suite $(A_i)_{i\in\mathbb{N}}$ à support fini d'éléments de $\mathbb{R}[X]$ vérifiant, pour tout $f \in E$,

$$\varphi(f) = \sum_i A_i f^{(i)},$$

où $f^{(i)}$ désigne la dérivée i-ième de f.

1. Montrer que $\varphi = 0$ équivaut à $A_i = 0$ pour tout $i \in \mathbb{N}$.

2. On admet que A est une algèbre. En déterminer les éléments inversibles.

3. Existe-t-il des morphismes d'algèbres de A dans $\mathbb{R}$?

(**École normale supérieure**)

▷ **Solution.**

1. Il est clair que si les A_i sont tous nuls, φ est nul. Réciproquement, si $\varphi = 0$, on montre par récurrence sur i que $A_i = 0$, pour tout $i \in \mathbb{N}$.

- En prenant $f = 1$, on obtient $\varphi(f) = A_0 = 0$.
- Si on suppose que $A_i = 0$, pour $0 \leqslant i \leqslant n - 1$, on obtient en

prenant $f : x \longmapsto x^n$, $\varphi(f) = \sum_{i \geqslant n} A_i f^{(i)} = n!\, A_n$, d'où l'on tire $A_n = 0$. La propriété est établie.

On en déduit qu'un élément de A s'écrit de manière unique sous la forme $\varphi(f) = \sum_i A_i f^{(i)}$.

2. Soit $\varphi \in A$ défini par $\varphi(f) = \sum_i A_i f^{(i)}$, pour tout $f \in E$. Supposons que φ soit inversible et que son inverse ψ s'écrive $\psi(f) = \sum_j B_j f^{(j)}$. On obtient alors $\psi \circ \varphi = \mathrm{Id}_E$ c'est-à-dire, pour tout $f \in E$,

$$\begin{aligned} f = (\psi \circ \varphi)(f) &= \sum_j B_j \left(\sum_i A_i f^{(i)} \right)^{(j)} \\ &= \sum_{i,j} B_j \left(\sum_{0 \leqslant k \leqslant j} C_j^k A_i^{(j-k)} f^{(i+k)} \right) \\ &= \sum_p \left(\sum_{\substack{0 \leqslant i \leqslant p \\ i+j \geqslant p}} C_j^{p-i} A_i^{(i+j-p)} B_j \right) f^{(p)}. \end{aligned}$$

en vertu de la formule de Leibniz.

Ni φ, ni ψ ne sont nuls. Soit i_0 (resp. j_0) le plus grand indice i (resp. j) pour lequel $A_i \neq 0$ (resp. $B_j \neq 0$). Considérons le coefficient de $f^{(i_0+j_0)}$ dans la somme précédente. Il est égal à $A_{i_0} B_{j_0}$. En effet, si $i + j \geqslant i_0 + j_0$, on a, si $i > i_0$, $A_i = 0$ et, si $i < i_0$, $j > j_0$ et donc $B_j = 0$. Si $i_0 + j_0 \neq 0$, le coefficient de $f^{(i_0+j_0)}$ n'étant pas nul, on ne peut pas avoir, pour tout $f \in E$,

$$f = \sum_p \left(\sum_{\substack{0 \leqslant i \leqslant p \\ i+j \geqslant p}} C_j^{p-i} A_i^{(i+j-p)} B_j \right) f^{(p)},$$

d'après l'unicité de l'écriture démontrée à la première question. On a donc nécessairement $i_0 = j_0 = 0$. On obtient alors $f = A_0 B_0 f$, pour tout $f \in E$, ce qui n'est vérifié que si $A_0 B_0 = 1$. Ceci nécessite que A_0 soit un polynôme constant non nul. Alors $\varphi = A_0\, \mathrm{Id}_E$, avec $A_0 \in \mathbb{R}^*$.

Réciproquement, s'il existe $\lambda \in \mathbb{R}^*$ tel que $\varphi = \lambda\, \mathrm{Id}_E$, alors φ est évidemment inversible, d'inverse $\psi = \dfrac{1}{\lambda}\, \mathrm{Id}_E$.

Conclusion. Les éléments inversibles de A sont les endomorphismes de la forme $\lambda\, \mathrm{Id}_E$, avec $\lambda \in \mathbb{R}^*$.

3. Supposons qu'il existe un morphisme d'algèbres F de A dans $\mathbb{R}$. Notons D et φ_1 les éléments de A définis, pour tout $f \in E$, par $D(f) = f'$

et $\varphi_1(f) = \mathrm{Id}_{\mathbb{R}} f : x \longmapsto xf(x)$. On a alors, pour tout $f \in \mathrm{E}$,

$$\mathrm{D} \circ \varphi_1(f) = \mathrm{D}(\mathrm{Id}_{\mathbb{R}} f) = f + \mathrm{Id}_{\mathbb{R}} f' = f + \varphi_1(f'),$$

et donc $\mathrm{D} \circ \varphi_1 = \mathrm{Id}_{\mathrm{E}} + \varphi_1 \circ \mathrm{D}$. On en déduit que

$$\mathrm{F}(\mathrm{Id}_{\mathrm{E}}) = \mathrm{F}(\mathrm{D} \circ \varphi_1) - \mathrm{F}(\varphi_1 \circ \mathrm{D}) = \mathrm{F}(\mathrm{D})\mathrm{F}(\varphi_1) - \mathrm{F}(\varphi_1)\mathrm{F}(\mathrm{D}) = 0.$$

Or par définition un morphisme d'algèbre doit envoyer l'élément unité de A sur 1.

Conclusion. Il n'y a pas de morphisme d'algèbres de A dans $\mathbb{R}$. $\lhd$

Chapitre 7

Matrices

Les systèmes de n équations linéaires à n inconnues sont étudiés dès le milieu du XVIIIe *siècle. Cramer décrit explicitement les formules donnant la solution sous forme du quotient de deux expressions qui porteront après Cauchy le nom de déterminants. Celui-ci donnera la formule générale définissant le produit de deux déterminants. La notion d'application linéaire, sous le nom de «substitution linéaire», apparaît au début du* XIXe *siècle dans les travaux de Lagrange, puis de Gauss sur les formes quadratiques à coefficients entiers. Ce dernier, pour la première fois, représente la substitution linéaire*

$$(x, y, z) \longmapsto (ax + by + cz, a'x + b'y + c'z, a''x + b''y + c''z)$$

par un tableau $\begin{matrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{matrix}$ *. Il étudie explicitement ce qui se passe quand on compose de telles transformations linéaires, autrement dit, il donne dans ce cas la règle de multiplication des matrices. Il note que ce résultat s'étendrait à un nombre quelconque de variables. Dans ses travaux de théorie des nombres, Eisenstein élargit le symbolisme de Gauss et introduit la notation* $\frac{1}{S}$ *quand* S *a un déterminant non nul. Le terme de matrice est inventé par Sylvester vers 1850. Cayley, qui définit un espace vectoriel de dimension n comme un système de n nombres réels ou complexes (vers 1845), écrit en 1858 le mémoire que l'on considère comme ayant créé la théorie des matrices : il y définit à la fois l'addition et la multiplication des matrices carrées et rectangulaires. Pour lui, une matrice est une façon abrégée de noter une substitution linéaire.*

L'étude plus approfondie des matrices va se faire à travers les formes quadratiques. Depuis le XVIIe *siècle, on recherche des transformations linéaires ramenant celles-ci à des formes simples. On est conduit à considérer des relations matricielles de la forme* $A' = {}^tUAV$. *À partir de 1850, une série de travaux va viser à obtenir des invariants dans le passage de* A *à* A'. *Ces résultats seront résumés et approfondis dans les mémoires de Frobenius, vers 1870. Il établit les formules de changement de bases* $A' = U^{-1}AV$, *montre que toute matrice de rang r est équivalente à* $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$. *Il élucide de manière définitive le problème de la résolution des systèmes d'équations linéaires.*

Rappelons maintenant l'essentiel du cours. Soit E, F *deux* K*-espaces vectoriels de dimension finie non nulle, respectivement* p *et* n*. Le choix d'une base* $\mathcal{B}$ *de* E *et d'une base* $\mathcal{C}$ *de* F *permet de ramener l'étude d'une application linéaire* u *de* E *dans* F *à celle de sa matrice* $A \in \mathcal{M}_{n,p}(K)$*, relativement aux bases* $\mathcal{B}$ *et* $\mathcal{C}$*. En effet,* u *s'identifie alors simplement à l'application linéaire de* K^p *dans* K^n *canoniquement associée à* A*. que l'on note souvent encore* A*. On dispose alors d'un outil analytique pour l'étude de* u *permettant le calcul du rang, et pour des endomorphismes, du déterminant, du polynôme caractéristique, du spectre, etc.*

Le fait que l'on puisse choisir librement les bases $\mathcal{B}$ *et* $\mathcal{C}$ *conduit à introduire la notion de matrices équivalentes : deux matrices* A *et* B *de* $\mathcal{M}_{n,p}(K)$ *sont équivalentes si elles représentent la même application linéaire dans des bases différentes. Pour cela, il faut et suffit qu'il existe* $(Q, P) \in GL_n(K) \times GL_p(K)$ *tel que* $B = Q^{-1}AP$*. C'est une relation d'équivalence, dont les classes sont paramétrées par le rang.*

Dans l'étude des endomorphismes de E*, prendre la même base à «l'arrivée» et au «départ», permet de faire correspondre le produit matriciel et la composition. Le changement de base se traduit alors par la notion de matrices semblables, relation d'équivalence bien plus fine que la relation précédente. On renvoie le lecteur au chapitre sur la réduction, dans le tome 2 d'algèbre, pour l'étude de cette notion. Il y trouvera de même un chapitre consacré spécifiquement au groupe linéaire.*

Commençons par une série d'exercices consacrés à la notion de rang. Le premier fournit un exemple de problème abstrait que l'on résout par une traduction matricielle. Nous en avons déjà donné une solution sans faire appel aux matrices dans l'exercice 6.5.

7.1. Condition pour que $\operatorname{rg} g \leqslant \operatorname{rg} f$

> Soit E et F deux K-espaces vectoriels non nuls de dimension finie, f et g dans $\mathcal{L}(E, F)$. Montrer que $\operatorname{rg} g \leqslant \operatorname{rg} f$ si et seulement s'il existe $h \in GL(F)$ et $k \in \mathcal{L}(E)$ tels que $h \circ g = f \circ k$.
>
> **(École polytechnique)**

▷ **Solution.**

L'exercice est traité matriciellement. On note n la dimension de F, p celle de E, r le rang de f. On fixe des bases quelconques de E et F et on considère la matrice $A \in \mathcal{M}_{n,p}(K)$ de f. En écrivant l'égalité $h \circ g = f \circ k$ sous la forme $g = h^{-1} \circ f \circ k$ et en appelant P et Q les matrices de h^{-1} et k, on voit que le problème posé consiste à montrer que l'ensemble

$$\Omega_A = \{PAM,\ P \in GL_n(K), M \in \mathcal{M}_p(K)\}$$

est l'ensemble des matrices de rang inférieur ou égal à $r = \operatorname{rg} A$.

On observe que, pour toutes matrices $P \in GL_n(K)$ et $M \in \mathcal{M}_p(K)$, on a $\mathrm{rg}(PAM) = \mathrm{rg}(AM) \leqslant \mathrm{rg}(A)$, car $\mathrm{Im}\, AM \subset \mathrm{Im}\, A$, ce qui établit une inclusion.

On remarque que si $B \in \Omega_A$, toute matrice équivalente à B est aussi dans Ω_A. On note, pour $0 \leqslant k \leqslant \min(n, m)$, $J_k = (a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant p}} \in \mathcal{M}_{n,p}(K)$ la matrice définie par $a_{11} = a_{22} = \cdots = a_{kk} = 1$ et $a_{ij} = 0$ sinon. Elle est de rang k. Comme deux matrices de $\mathcal{M}_{n,p}(K)$ qui ont le même rang sont équivalentes, il nous suffit de prouver que pour tout $s \leqslant r$, $J_s \in \Omega_A$.

On sait que $J_r \in \Omega_A$, puisque $A \in \Omega_A$. Il suffit alors de constater que pour $s \leqslant r$, $J_s = J_r M$, où M est la matrice $\begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix}$ de $\mathcal{M}_p(K)$, pour conclure. $\lhd$

L'exercice suivant sera à rapprocher des importants lemmes de factorisation de l'exercice 6.4.

7.2. Factorisation bilatère

Soit A, B, C dans $\mathcal{M}_n(K)$. Donner une condition nécessaire et suffisante pour qu'il existe X dans $\mathcal{M}_n(K)$ telle que $C = AXB$.
(**École normale supérieure**)

$\rhd$ **Solution.**

Une condition nécessaire se voit facilement : il faut que $\mathrm{Ker}\, B \subset \mathrm{Ker}\, C$ et que $\mathrm{Im}\, C \subset \mathrm{Im}\, A$ (ce qui impose en particulier que $\mathrm{rg}\, C \leqslant \mathrm{rg}\, A$ et $\mathrm{rg}\, C \leqslant \mathrm{rg}\, B$). On va voir en fait qu'elle est suffisante.

Dans ce qui suit on note φ_M l'application linéaire canoniquement associée à une matrice M. On suppose donc $\mathrm{Ker}\, B \subset \mathrm{Ker}\, C$ et $\mathrm{Im}\, C \subset \mathrm{Im}\, A$. Choisissons H un supplémentaire de $\mathrm{Ker}\, B$ dans K^n. Les applications φ_C et φ_{AXB} coïncident sur $\mathrm{Ker}\, B$ quel que soit le choix de X. Il suffit de faire en sorte qu'elles coïncident aussi sur H. L'application φ_B établit un isomorphisme entre H et l'espace $\varphi_B(H) = \mathrm{Im}\, B$, isomorphisme que nous noterons u_B. Il suffit donc de trouver X telle que si f désigne la restriction de φ_X à $\mathrm{Im}\, B$ alors $\varphi_A \circ f = \varphi_C \circ u_B^{-1}$. Donnons-nous un supplémentaire K de $\mathrm{Ker}\, A$ de sorte que φ_A induise un isomorphisme u_A entre K et $\mathrm{Im}\, A$. Par hypothèse, $\mathrm{Im}\, C \subset \mathrm{Im}\, A$. Donc $f = u_A^{-1} \circ \varphi_C \circ u_B^{-1}$ est bien définie et convient. Il existe évidemment des matrices X telles que $\varphi_X|_{\mathrm{Im}\, B} = f$. $\lhd$

L'exercice suivant montre qu'une application multiplicative de $\mathcal{M}_n(K)$ dans K, non constante, permet, comme le déterminant, de caractériser l'inversibilité.

7.3. Fonctions multiplicatives et inversibilité

Soit f une application non constante de $\mathcal{M}_n(\mathrm{K})$ dans K, telle que, pour toutes matrices A et B, on ait $f(\mathrm{AB}) = f(\mathrm{A})f(\mathrm{B})$.

Montrer que $f(\mathrm{A}) = 0$ si, et seulement si, A n'est pas inversible.

(École polytechnique)

▷ **Solution.**

• On observe d'abord que $f(0) = f(0)f(0)$ et donc que $f(0) \in \{0, 1\}$. Si $f(0) = 1$, on a $f(\mathrm{A}) = f(\mathrm{A})f(0) = f(0) = 1$, pour toute matrice A, et l'application f est constante, ce qui est contraire à l'hypothèse. On a donc $f(0) = 0$.

On obtient, de même, $f(\mathrm{I}_n) = f(\mathrm{I}_n)f(\mathrm{I}_n)$ et donc $f(\mathrm{I}_n) \in \{0, 1\}$. Si $f(\mathrm{I}_n) = 0$, on a $f(\mathrm{A}) = f(\mathrm{AI}_n) = f(\mathrm{A})f(\mathrm{I}_n) = 0$, pour toute matrice A, et f est constante. On a donc $f(\mathrm{I}_n) = 1$.

• Supposons A inversible. On peut alors écrire

$$f(\mathrm{A})f(\mathrm{A}^{-1}) = f(\mathrm{I}_n) = 1 \text{ et donc } f(\mathrm{A}) \neq 0.$$

• Soit A et B deux matrices équivalentes : $\mathrm{B} = \mathrm{QAP}$ avec (Q et P dans $\mathrm{GL}_n(\mathrm{K})$. Comme $f(\mathrm{B}) = f(\mathrm{Q})f(\mathrm{A})f(\mathrm{P})$, on a, d'après ce qui précède, $f(\mathrm{A}) = 0$ si et seulement si $f(\mathrm{B}) = 0$. Autrement dit, sur une classe d'équivalence, soit f est identiquement nulle, soit elle ne s'annule jamais.

Il suffit donc, pour la réciproque, de montrer que pour tout $r < n$ il existe une matrice A de rang r telle que $f(\mathrm{A}) = 0$. On peut prendre une matrice nilpotente de rang r, par exemple $\mathrm{K}_r = \left(\begin{array}{c|c} 0 & \mathrm{I}_r \\ \hline 0 & 0 \end{array}\right) \in \mathcal{M}_n(\mathrm{K})$. On a alors $(\mathrm{K}_r)^{r+1} = 0$ et donc $f(\mathrm{K}_r)^{r+1} = 0$ et $f(\mathrm{K}_r)$ est bien nul, tout comme $f(\mathrm{A})$. ◁

7.4. Degré et valuation du polynôme $\det(\mathrm{XA} + \mathrm{B})$

Soit A et B dans $\mathcal{M}_n(\mathbb{C})$. On pose $\mathrm{P}(t) = \det(t\mathrm{A} + \mathrm{B})$. Établir que

$$\deg \mathrm{P} \leqslant \operatorname{rg} \mathrm{A} \quad \text{et} \quad \operatorname{val} \mathrm{P} \geqslant n - \operatorname{rg} \mathrm{B}.$$

(École polytechnique)

▷ **Solution.**

• Si le rang de A est r, A est équivalente à la matrice $\mathrm{J}_r = \begin{pmatrix} \mathrm{I}_r & 0 \\ 0 & 0 \end{pmatrix}$. Elle s'écrit donc $\mathrm{A} = \mathrm{QJ}_r\mathrm{R}$ avec Q et R inversibles. On considère la matrice B′ telle que $\mathrm{B} = \mathrm{QB'R}$. On a

$$\mathrm{P}(t) = \det(\mathrm{Q}(t\mathrm{J}_r + \mathrm{B}')\mathrm{R}) = \det \mathrm{Q} \det \mathrm{R} \det(t\mathrm{J}_r + \mathrm{B}').$$

En notant $(e_1, \ldots, e_n)$ la base canonique de $\mathbb{C}^n$ et $\mathrm{C}_1, \ldots, \mathrm{C}_n$ les vecteurs colonnes de B', on obtient

$$\mathrm{P}(t) = \det \mathrm{Q} \det \mathrm{R} \det(te_1 + \mathrm{C}_1, \ldots, te_r + \mathrm{C}_r, \mathrm{C}_{r+1}, \ldots, \mathrm{C}_n).$$

En utilisant la multilinéarité du déterminant, on voit que P est un polynôme en t de degré inférieur ou égal à r, le coefficient de t^r étant $\det \mathrm{Q} \det \mathrm{R} \det(e_1, \ldots, e_r, \mathrm{C}_{r+1}, \ldots, \mathrm{C}_n)$.

• Notons $\mathrm{Q}(t) = \det(\mathrm{A} + t\mathrm{B})$ le polynôme obtenu en échangeant A et B. On a d'après le point précédent, $\deg(\mathrm{Q}) \leqslant \operatorname{rg} \mathrm{B}$. Or, par multilinéarité du déterminant, $\mathrm{P}(t) = t^n \det(\mathrm{A} + \frac{1}{t}\mathrm{B}) = t^n \mathrm{Q}(\frac{1}{t})$. Cette expression montre que la valuation de P est égale à $n - \deg \mathrm{Q}$. La seconde inégalité en résulte. ◁

On montre dans l'exercice suivant que, pour qu'un endomorphisme de $\mathcal{M}_n(\mathbb{C})$ conserve le rang, il suffit qu'il conserve le caractère inversible.

7.5. Endomorphismes de $\mathcal{M}_n(\mathbb{C})$ stabilisant le groupe linéaire

Soit φ un endomorphisme de $\mathcal{M}_n(\mathbb{C})$ tel que si M appartient à $\mathrm{GL}_n(\mathbb{C})$, alors $\varphi(\mathrm{M})$ appartient à $\mathrm{GL}_n(\mathbb{C})$.

1. Donner des exemples de tels endomorphismes.

2. Montrer que, pour tout $\mathrm{M} \in \mathcal{M}_n(\mathbb{C})$, M appartient à $\mathrm{GL}_n(\mathbb{C})$ si, et seulement si, $\varphi(\mathrm{M})$ appartient à $\mathrm{GL}_n(\mathbb{C})$. Pour cela, on prouvera que si $\operatorname{rg} \mathrm{M} < n$, il existe $\mathrm{P} \in \mathrm{GL}_n(\mathbb{C})$ tel que pour tout $\lambda \in \mathbb{C}$, $\mathrm{P} - \lambda\mathrm{M}$ est inversible.

3. Montrer que $\operatorname{rg} \varphi(\mathrm{M}) \geqslant \operatorname{rg} \mathrm{M}$. Pour cela, on montrera que si $\operatorname{rg} \mathrm{M} = r$, il existe $\mathrm{Q} \in \mathrm{GL}_n(\mathbb{C})$ tel que $\mathrm{Q} - \lambda\mathrm{M}$ soit non inversible pour r valeurs de λ exactement.

4. Montrer que φ conserve le rang.

(École normale supérieure)

▷ **Solution.**

1. Si P et Q sont dans $\mathrm{GL}_n(\mathbb{C})$, l'endomorphismes $\mathrm{M} \longmapsto \mathrm{QMP}$ convient. La transposition convient également. Par suite tous les endomorphismes du type $\mathrm{M} \longmapsto \mathrm{Q}\,{}^t\mathrm{MP}$ vérifient la propriété de l'énoncé.

2. Soit $\mathrm{M} \in \mathcal{M}_n(\mathbb{C})$.

• Montrons tout d'abord l'indication. Supposons $\operatorname{rg} \mathrm{M} < n$ et M non nulle (si $\mathrm{M} = 0$ toute matrice inversible P convient). Géométriquement, on souhaite prouver qu'il existe une droite affine de $\mathcal{M}_n(\mathbb{C})$ dirigée par M

et incluse dans le groupe linéaire. En multipliant par P^{-1}, le problème se ramène à montrer l'existence de $P \in GL_n(\mathbb{C})$ tel que pour tout $\lambda \in \mathbb{C}$, on ait $I_n - \lambda P^{-1}M \in GL_n(\mathbb{C})$. Cette condition équivaut à dire que la seule valeur propre de $P^{-1}M$ est 0, c'est-à-dire que $P^{-1}M$ est nilpotente.

On utilise encore les matrices équivalentes. Comme $\operatorname{rg} M = r < n$, elle peut s'écrire $M = AK_rB$ où $K_r = \begin{pmatrix} 0 & I_r \\ 0 & 0 \end{pmatrix}$ et $(A, B) \in GL_n(\mathbb{C})^2$. Comme la matrice K_r est nilpotente, la matrice $B^{-1}A^{-1}M = B^{-1}K_rB$, qui lui est semblable, est aussi nilpotente. Ainsi $P = AB$ convient.

• On suppose toujours $\operatorname{rg}(M) < n$ et on va montrer maintenant que $\varphi(M)$ est non inversible. La matrice P étant choisie de manière à remplir la condition ci-dessus, on a $\varphi(P - \lambda M) = \varphi(P) - \lambda\varphi(M) \in GL_n(\mathbb{C})$ pour tout λ dans $\mathbb{C}$. Comme P est inversible, $\varphi(P)$ l'est aussi et pour tout $\lambda \in \mathbb{C}$,

$$I_n - \lambda\varphi(M)\,(\varphi(P))^{-1} \in GL_n(\mathbb{C}).$$

Donc 0 est la seule valeur propre de $\varphi(M)\,(\varphi(P))^{-1}$: celle-ci est nilpotente, donc non inversible. Nécessairement, $\varphi(M)$ est non inversible. On a donc bien l'équivalence demandée.

3. L'inégalité $\operatorname{rg}(\varphi(M)) \geqslant \operatorname{rg} M$ est vérifiée si M est inversible. Supposons dans la suite $r = \operatorname{rg} M < n$.

• On commence par démontrer l'indication en suivant une démarche analogue à celle de la question 2. On écrit cette fois $M = AJ_rB$, avec $J_r = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$ et $(A, B) \in GL_n(\mathbb{C})^2$. Soit $D = \operatorname{Diag}(1, 2, \ldots, n) \in GL_n(\mathbb{C})$. Posons $Q = ADB$. On a $Q - \lambda M = A(D - \lambda J_r)B$. Elle est non inversible si et seulement si $\lambda \in \{1, 2, \ldots, r\}$.

• D'après la question précédente, $\varphi(Q - \lambda M) = \varphi(Q) - \lambda\varphi(M)$ est non inversible pour exactement r valeurs (non nulles) de λ. Il en va de même de $I_n - \lambda\varphi(Q)^{-1}\varphi(M)$. On en déduit que la matrice $\varphi(Q)^{-1}\varphi(M)$ a exactement r valeurs propres non nulles distinctes : elle est donc au moins de rang r. On en déduit que $\varphi(M)$ est au moins de rang r puisqu'elle est de même rang que $\varphi(Q)^{-1}\varphi(M)$.

4. Il résulte de la question précédente que φ est injectif ; c'est donc un automorphisme de l'espace vectoriel $\mathcal{M}_n(\mathbb{C})$. Si $M \in GL_n(\mathbb{C})$, $\varphi^{-1}(M)$ est inversible en vertu de la question 2 puisque $M = \varphi(\varphi^{-1}(M))$. L'endomorphisme φ^{-1} vérifie donc la même hypothèse que φ. D'après la question précédente appliquée à φ^{-1}, il vient

$$\operatorname{rg} M = \operatorname{rg} \varphi^{-1}(\varphi(M)) \geqslant \operatorname{rg} \varphi(M) \text{ et finalement } \operatorname{rg} M = \operatorname{rg} \varphi(M).$$

Conclusion. L'endomorphisme φ de $\mathcal{M}_n(\mathbb{C})$ conserve le rang. $\lhd$

L'exercice suivant aborde la détermination de tous les endomorphismes de l'espace vectoriel $\mathcal{M}_n(\mathbb{C})$ qui conservent le rang. On remarque que ce sont nécessairement des automorphismes. Notons que ce résultat a fait l'objet d'un problème d'écrit posé au concours de l'École polytechnique en 1988.

7.6. Endomorphismes de $\mathcal{M}_n(\mathbb{C})$ conservant le rang

1. Décrire les sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{C})$ formés de matrices de rang au plus 1.

2. Déterminer les automorphismes de l'espace vectoriel $\mathcal{M}_n(\mathbb{C})$ qui conservent le rang.

(**École normale supérieure**)

▷ **Solution.**

On supposera dans la suite que $n \geqslant 2$, sinon tous les sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{C})$, puis tous les automorphismes de $\mathcal{M}_n(\mathbb{C})$ conviennent.

1. • On commence par décrire les matrices de rang 1. Soit A une matrice de rang 1 de $\mathcal{M}_n(\mathbb{C})$. Les vecteurs colonnes de A sont proportionnels. Si on fait la convention d'identifier $\mathcal{M}_{n,1}(\mathbb{C})$ avec $\mathbb{C}^n$, il existe donc des vecteurs $X \in \mathbb{C}^n \setminus \{0\}$ et $Y = {}^t(y_1, \ldots, y_n) \in \mathbb{C}^n \setminus \{0\}$ tels que les vecteurs colonnes de A soient $(y_1 X, \ldots, y_n X)$. On a donc $A = X\,{}^tY$. Réciproquement, toute matrice qui s'écrit $X\,{}^tY$, où X et Y sont des vecteurs colonnes non nuls est de rang 1, car elle est non nulle et ses colonnes sont toutes colinéaires à X.

L'écriture de A sous la forme $X\,{}^tY$ n'est pas unique. On vérifie aisément que deux matrices $A = X\,{}^tY$ et $A' = X'\,{}^tY'$ de rang 1 écrites sous cette forme, sont colinéaires si et seulement si les deux familles (X, X') et (Y, Y') sont liées et en particulier, on a $A = A'$ si et seulement s'il existe $\lambda \in \mathbb{C}^*$ tel que $X' = \lambda X$ et $Y' = \dfrac{1}{\lambda} Y$.

• On dispose dès maintenant d'un moyen simple pour fabriquer des sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{C})$ formés de matrices de rang au plus 1. Soit $X \in \mathbb{C}^n \setminus \{0\}$ une colonne non nulle. L'application $f_X : \mathbb{C}^n \to \mathcal{M}_n(\mathbb{C})$ qui à Y associe $X\,{}^tY$ est linéaire. L'image d'un sous-espace vectoriel L de $\mathbb{C}^n$ par f_X est un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ formé de matrices de rang au plus 1. Posons $E_{X,L} = f_X(L)$. Comme le noyau de f_X est réduit à 0 d'après ce qui précède, f_X est injective et $E_{X,L}$ a même dimension que L.

De la même manière, on peut fixer une colonne $Y \in \mathbb{C}^n$ non nulle et prendre les images des sous-espaces vectoriels de $\mathbb{C}^n$ par l'application linéaire $g_Y : \mathbb{C}^n \to \mathcal{M}_n(\mathbb{C})$ qui à X associe $X\,{}^tY$. Si L est un sous-

espace de $\mathbb{C}^n$, on notera $E_{L,Y}$ le sous-espace $g_Y(L)$. On a également $\dim E_{L,Y} = \dim L$.

• On va montrer que les sous-espaces obtenus dans le point précédent sont les seuls possibles. Soit E un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ formé de matrices de rang au plus 1. Si $\dim E = 1$, le résultat est clair. On suppose donc $\dim E \geqslant 2$. Soit A et A′ deux matrices non colinéaires de E (donc non nulles), que nous écrivons $A = X\,{}^tY$ et $A' = X'\,{}^tY'$. On note que

$$\mathrm{rg}(A + A') \leqslant 1 \Longrightarrow (X, X') \text{ liée ou } (Y, Y') \text{ liée.}$$

En effet, supposons que les familles (X, X') et (Y, Y') sont libres. Si on note $Y = {}^t(y_1, \ldots, y_n)$ et $Y' = {}^t(y'_1, \ldots, y'_n)$, les vecteurs-colonnes de $A + A'$ ont pour coordonnées $\begin{pmatrix} y_1 \\ y'_1 \end{pmatrix}, \ldots, \begin{pmatrix} y_n \\ y'_n \end{pmatrix}$ dans la base (X, X'). Ils ne sont pas tous colinéaires car la famille (Y, Y') est libre et on a $\mathrm{rg}(A + A') \geqslant 2$.

⋆ Supposons alors que (X, X') est libre. D'après ce qui précède, comme $A + A' \in E$, la famille (Y, Y') est liée.

Soit maintenant une autre matrice $A'' = X''\,{}^tY''$, non nulle, de E. Supposons que la famille (Y, Y'') est libre. Alors (Y', Y'') est également libre et nécessairement les familles (X, X'') et (X', X'') sont liées (toujours grâce à l'implication ci-dessus). Mais comme $X'' \neq 0$, la famille (X, X') est liée, ce qui est contraire à notre hypothèse. On a donc Y'' colinéaire à Y. Comme Y'' n'est défini qu'à une constante multiplicative près, on peut supposer $Y'' = Y$. Tout élément de E peut donc s'écrire $X''\,{}^tY$, avec $Y \in \mathbb{C}^n \setminus \{0\}$ fixé. Comme Y est fixé, une telle écriture d'un élément de E est unique. La matrice $X''\,{}^tY$ décrivant un sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$, X'' décrit un sous-espace vectoriel L de $\mathbb{C}^n$. Finalement, on a $E = E_{L,Y}$.

⋆ On montre de la même manière que lorsque (Y, Y') est libre, il existe un sous-espace vectoriel L de $\mathbb{C}^n$ tel que $E = E_{X,L}$.

Conclusion. Il y a donc deux types de sous-espaces vectoriels de $\mathcal{M}_n(\mathbb{C})$ formés de matrices de rang au plus 1, qui sont les sous-espaces $E_{X,L} = \{X\,{}^tY, Y \in L\}$ et $E_{L,Y} = \{X\,{}^tY, X \in L\}$, X et Y étant des vecteurs non nuls de $\mathbb{C}^n$ et L un sous-espace vectoriel de $\mathbb{C}^n$. La dimension d'un tel sous-espace est celle de L ; elle est au plus égale à n.

2. Soit Φ un automorphisme de l'espace vectoriel $\mathcal{M}_n(\mathbb{C})$ conservant le rang. Il transforme tout sous-espace vectoriel de $\mathcal{M}_n(\mathbb{C})$ formé de matrices de rang $\leqslant 1$ en un sous-espace formé de matrices de rang $\leqslant 1$, et de même dimension. Nous nous intéresserons particulièrement aux sous-espaces de dimension n. Un tel sous-espace est de la forme $E_{X,\mathbb{C}^n}$ ou $E_{\mathbb{C}^n,Y}$. Pour alléger les notations, nous poserons désormais $E_{X,\mathbb{C}^n} = E^1_X$ et $E_{\mathbb{C}^n,Y} = E^2_Y$.

• Soit X_0 un élément non nul, fixé de $\mathbb{C}^n \setminus \{0\}$. Il existe $X_0' \in \mathbb{C}^n \setminus \{0\}$ tel que $\Phi(E^1_{X_0}) = E^1_{X_0'}$ ou $E^2_{X_0'}$. Nous nous contenterons d'examiner le premier cas, le deuxième pouvant s'en déduire. En effet, considérons l'endomorphisme T de $\mathcal{M}_n(\mathbb{C})$: $A \longmapsto {}^tA$. C'est un automorphisme de $\mathcal{M}_n(\mathbb{C})$ qui conserve le rang et $T \circ \Phi$ également. Mais si $\Phi(E^1_{X_0}) = E^2_{X_0'}$, alors $T \circ \Phi(E^1_{X_0}) = E^1_{X_0'}$ et en remplaçant Φ par $T \circ \Phi$ on est ramené au premier cas. On suppose donc dans la suite qu'il existe $X_0' \in \mathbb{C}^n \setminus \{0\}$ tel que $\Phi(E^1_{X_0}) = E^1_{X_0'}$.

⋆ Si $X \in \mathbb{C}^n \setminus \{0\}$ est colinéaire à X_0, $\Phi(E^1_X) = \Phi(E^1_{X_0}) = E^1_{X_0'}$. Si la famille (X_0, X) est libre, alors il résulte des conditions d'égalité de deux matrices de rang 1 (cf. question 1), que $E^1_{X_0} \cap E^1_X = \{0\}$. On en déduit, par injectivité de Φ que $E^1_{X_0'} \cap \Phi(E^1_X) = \{0\}$. S'il existe $X' \in \mathbb{C}^n \setminus \{0\}$ tel que $\Phi(E^1_X) = E^2_{X'}$ alors $E^1_{X_0'} \cap \Phi(E^1_X)$ est égal à $\mathrm{Vect}(X_0'\,{}^tX')$; c'est impossible. Nous avons donc démontré que, pour tout $X \in \mathbb{C}^n \setminus \{0\}$, il existe $X' \in \mathbb{C}^n \setminus \{0\}$ tel que $\Phi(E^1_X) = E^1_{X'}$.

⋆ Si on prend $Y \in \mathbb{C}^n \setminus \{0\}$, on a $E^1_{X_0} \cap E^2_Y = \mathrm{Vect}(X_0\,{}^tY)$ et $\Phi(E^1_{X_0}) \cap \Phi(E^2_Y) = E^1_{X_0'} \cap \Phi(E^2_Y)$. Si $\Phi(E^2_Y) = E^1_{Y'}$, alors $\Phi(E^1_{X_0}) \cap \Phi(E^2_Y)$ est $\{0\}$ ou $E^1_{X_0'}$, selon que X_0' et Y' sont ou non colinéaires. Ce n'est pas une droite vectorielle ; c'est impossible. Nous avons donc démontré que, pour tout $Y \in \mathbb{C}^n \setminus \{0\}$, il existe $Y' \in \mathbb{C}^n \setminus \{0\}$ tel que $\Phi(E^2_Y) = E^2_{Y'}$.

Le problème est que X' et Y' ne sont pas définis de manière unique.

• Soit X un élément non nul, fixé de $\mathbb{C}^n \setminus \{0\}$. Supposons choisi un vecteur X' tel que $\Phi(E^1_X) = E^1_{X'}$. Pour tout $Y \in \mathbb{R}^n$, $\Phi(X\,{}^tY)$ appartient à $\Phi(E^1_X) = E^1_{X'}$. Il existe donc $Z \in \mathbb{R}^n$ tel que $\Phi(X\,{}^tY) = X'\,{}^tZ$. Le vecteur X' étant fixé, ceci définit un Z unique. Considérons l'application $G_X : Y \in \mathbb{C}^n \longmapsto Z \in \mathbb{C}^n$. Puisque Φ est linéaire, l'application G_X est aussi linéaire. D'autre part, on a

$$G_X(Y) = 0 \Longleftrightarrow \Phi(X\,{}^tY) = 0 \Longrightarrow X\,{}^tY = 0 \Longrightarrow Y = 0, \text{ car } X \neq 0.$$

On en déduit que $G_X \in \mathrm{GL}_n(\mathbb{C})$. On définit en particulier G_{X_0} par le choix de X_0' effectué tout au début.

Soit alors $Y \in \mathbb{C}^n \setminus \{0\}$ et Y' tel que $\Phi(E^2_Y) = E^2_{Y'}$. On a, pour tout $X \in \mathbb{C}^n \setminus \{0\}$,

$$X'\,{}^tG_X(Y) = \Phi(X\,{}^tY) \in \Phi(E^2_Y) = E^2_{Y'}.$$

On en déduit que, pour tout $X \in \mathbb{C}^n \setminus \{0\}$, $G_X(Y)$ est colinéaire à Y' et donc que $G_X(Y)$ est colinéaire à $G_{X_0}(Y)$. Ce qui peut encore s'écrire : $G_{X_0}^{-1} \circ G_X(Y)$ est colinéaire à Y, ceci pour tout $Y \in \mathbb{C}^n$. C'est un résultat classique (rappelé avant l'exercice 6.6) qui permet alors d'affirmer que $G_{X_0}^{-1} \circ G_X$ est un homothétie : il existe $\lambda_X \in \mathbb{C}^*$ tel que $G_X = \lambda_X G_{X_0}$. Mais l'application G_X est définie à une constante multiplicative près, qui

dépend du choix de X'. En remplaçant X' par un vecteur colinéaire, on peut supposer que $G_X = G_{X_0}$, pour tout $X \in \mathbb{C}^n \setminus \{0\}$.

Pour simplifier on note $G_{X_0} = G$. On obtient donc que, pour tout $X \in \mathbb{C}^n$, il existe $X' \in \mathbb{C}^n$ tel que $\Phi(X\,{}^tY) = X'\,{}^tG(Y)$. Le vecteur X' est maintenant déterminé de manière unique. Comme précédemment pour G, on montre aisément que l'application $F : X \in \mathbb{C}^n \longmapsto X' \in \mathbb{C}^n$ est linéaire et injective.

Soit P et Q les matrices respectives de F et G dans la base canonique. Ce sont des matrices inversibles. On a, pour tout $(X, Y) \in (\mathbb{C}^n)^2$,

$$\Phi(X\,{}^tY) = F(X)\,{}^tG(Y) = PX\,{}^t(QY) = PX\,{}^tY\,{}^tQ.$$

Autrement dit, on obtient $\Phi(A) = PA\,{}^tQ$, pour toute matrice de rang 1. Toute matrice de $\mathcal{M}_n(\mathbb{C})$ étant somme de matrices de rang 1 (par exemple somme de matrices colinéaires aux matrices de base E_{ij}), cette égalité est vraie pour toute matrice $A \in \mathcal{M}_n(\mathbb{C})$.

Pour terminer, regardons ce qu'on obtient pour Φ dans le cas où $\Phi(E^1_{X_0})$ est de la forme $E^2_{X_0'}$. En composant avec T on obtient une application du type précédent : il existe donc deux matrices inversibles P et Q telles que, pour tout $A \in \mathcal{M}_n(\mathbb{C})$,

$${}^t(\Phi(A)) = T \circ \Phi(A) = PA\,{}^tQ, \text{ et donc } \Phi(A) = Q\,{}^tA\,{}^tP.$$

Conclusion. Si Φ est un automorphisme de $\mathcal{M}_n(\mathbb{C})$ conservant le rang, alors il existe deux matrices inversibles de $\mathcal{M}_n(\mathbb{C})$ telles que l'on ait soit $\Phi(A) = PAQ$, pour tout $A \in \mathcal{M}_n(\mathbb{C})$, soit $\Phi(A) = P\,{}^tAQ$, pour tout $A \in \mathcal{M}_n(\mathbb{C})$. Il est clair que, réciproquement, les applications ainsi définies sont des automorphismes de $\mathcal{M}_n(\mathbb{C})$ qui conservent le rang. $\lhd$

Notons que la preuve ci-dessus n'utilise en aucune manière le fait que le corps de base est $\mathbb{C}$. Aussi le résultat est-il valide pour un corps quelconque.

La série d'exercices qui suit concerne la trace. On commence par une petite équation matricielle qui fait intervenir la trace.

7.7. Équation matricielle $X + {}^tX = (\operatorname{Tr} X)A$

Soit $A \in \mathcal{M}_n(\mathbb{R})$. Résoudre l'équation $X + {}^tX = (\operatorname{Tr} X)A$ où l'inconnue X est dans $\mathcal{M}_n(\mathbb{R})$.

(École polytechnique)

$\rhd$ **Solution.**

Si X est solution, on obtient en prenant la trace des deux membres de l'équation $2 \operatorname{Tr} X = \operatorname{Tr} X \operatorname{Tr} A$.

• Si $\mathrm{Tr}\,\mathrm{X} = 0$, alors ${}^t\mathrm{X} = -\mathrm{X}$: X est antisymétrique. Réciproquement, toute matrice antisymétrique est solution de l'équation.

• Si $\mathrm{Tr}\,\mathrm{X} \neq 0$, nécessairement, $\mathrm{Tr}\,\mathrm{A} = 2$ et $\mathrm{A} = \dfrac{1}{\mathrm{Tr}\,\mathrm{X}}(\mathrm{X} + {}^t\mathrm{X})$ est symétrique. On a alors

$$\left(\mathrm{X} - \frac{\mathrm{Tr}\,\mathrm{X}}{2}\mathrm{A}\right) + {}^t\left(\mathrm{X} - \frac{\mathrm{Tr}\,\mathrm{X}}{2}\mathrm{A}\right) = 0$$

et donc $\mathrm{X} - \dfrac{\mathrm{Tr}\,\mathrm{X}}{2}\mathrm{A}$ est antisymétrique. Autrement dit, il existe B antisymétrique telle que

$$\mathrm{X} = \frac{\mathrm{Tr}\,\mathrm{X}}{2}\mathrm{A} + \mathrm{B}.$$

Réciproquement, si $\lambda \in \mathbb{R}$ et B est antisymétrique, $\mathrm{X} = \lambda\mathrm{A} + \mathrm{B}$ est solution. En effet, on a $\mathrm{Tr}\,\mathrm{X} = \lambda\,\mathrm{Tr}\,\mathrm{A} = 2\lambda$ et $\mathrm{X} + {}^t\mathrm{X} = 2\lambda\mathrm{A} = (\mathrm{Tr}\,\mathrm{X})\mathrm{A}$.

Conclusion. Si $\mathrm{Tr}\,\mathrm{A} \neq 2$ ou si A n'est pas symétrique, les seules solutions sont les matrices antisymétriques. Si $\mathrm{Tr}\,\mathrm{A} = 2$ et A symétrique, les solutions s'écrivent $\lambda\mathrm{A} + \mathrm{B}$ avec $\lambda \in \mathbb{R}$ et B antisymétrique quelconques. ◁

En combinant la trace et le produit, on obtient sur $\mathcal{M}_n(\mathrm{K})$ la forme bilinéaire $(\mathrm{X}, \mathrm{Y}) \longmapsto \mathrm{Tr}(\mathrm{XY})$ qui permet d'établir un isomorphisme canonique entre $\mathcal{M}_n(\mathrm{K})$ et son dual, comme le montre l'exercice suivant.

7.8. Dual de $\mathcal{M}_n(\mathrm{K})$

1. Si $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$, on note f_A la forme linéaire définie, pour tout $\mathrm{X} \in \mathcal{M}_n(\mathrm{K})$, par $f_\mathrm{A}(\mathrm{X}) = \mathrm{Tr}(\mathrm{AX})$. Montrer que l'application f qui à $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$ associe f_A établit un isomorphisme entre $\mathcal{M}_n(\mathrm{K})$ et son dual.

2. Soit $f : \mathcal{M}_n(\mathrm{K}) \longrightarrow \mathrm{K}$ une forme linéaire vérifiant, pour tout (X, Y) dans $\mathcal{M}_n(\mathrm{K})^2$, $f(\mathrm{XY}) = f(\mathrm{YX})$. Montrer l'existence de $\lambda \in \mathrm{K}$ tel que, pour tout $\mathrm{X} \in \mathcal{M}_n(\mathrm{K})$, $f(\mathrm{X}) = \lambda\,\mathrm{Tr}(\mathrm{X})$.

(**École normale supérieure**)

▷ **Solution.**

On notera $(\mathrm{E}_{ij})_{1 \leqslant i,j \leqslant n}$ la base canonique de $\mathcal{M}_n(\mathrm{K})$. On rappelle que, pour tout $1 \leqslant i, j, k, l \leqslant n$, on a $\mathrm{E}_{ij}\mathrm{E}_{kl} = \delta_{jk}\mathrm{E}_{il}$.

1. On vérifie aisément que f est linéaire. Pour des raisons de dimension, il suffit donc de prouver qu'elle est injective. Soit $\mathrm{A} = (a_{ij})_{1 \leqslant i,j \leqslant n}$ telle que $f_\mathrm{A} = 0$. On a donc, pour $1 \leqslant i_0, j_0 \leqslant n$,

$$0 = \mathrm{Tr}(\mathrm{A}\mathrm{E}_{i_0 j_0}) = \mathrm{Tr}\Big(\sum_{1\leqslant i,j\leqslant n} a_{ij}\mathrm{E}_{ij}\mathrm{E}_{i_0 j_0}\Big) = \mathrm{Tr}\Big(\sum_{i=1}^{n} a_{ii_0}\mathrm{E}_{ii_0}\mathrm{E}_{i_0 j_0}\Big)$$
$$= \sum_{i=1}^{n} a_{ii_0}\,\mathrm{Tr}\,(\mathrm{E}_{ij_0}) = a_{j_0 i_0}.$$

Donc A est nulle.

2. • On peut donner une solution directe de cette question. On obtient, si $1 \leqslant i, j \leqslant n$ et $i \neq j$,

$$f(\mathrm{E}_{ij}) = f(\mathrm{E}_{ii}\mathrm{E}_{ij}) = f(\mathrm{E}_{ij}\mathrm{E}_{ii}) = f(0) = 0.$$

On a également

$$f(\mathrm{E}_{ii}) = f(\mathrm{E}_{ij}\mathrm{E}_{ji}) = f(\mathrm{E}_{ji}\mathrm{E}_{ij}) = f(\mathrm{E}_{jj}).$$

Si on note λ la valeur commune des $f(\mathrm{E}_{ii})$, on remarque que les formes linéaires f et $\lambda\,\mathrm{Tr}$ coïncident sur la base canonique de $\mathcal{M}_n(\mathrm{K})$. Elles sont donc égales.

• On peut aussi utiliser la première question. Soit $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$ telle que $f = f_{\mathrm{A}}$. On a, pour tout $(\mathrm{X}, \mathrm{Y}) \in \mathcal{M}_n(\mathrm{K})^2$, $\mathrm{Tr}(\mathrm{AXY}) = \mathrm{Tr}(\mathrm{AYX})$. Comme $\mathrm{Tr}(\mathrm{AYX}) = \mathrm{Tr}(\mathrm{XAY})$, on en déduit que $\mathrm{Tr}((\mathrm{AX} - \mathrm{XA})\mathrm{Y}) = 0$. Cela étant valable pour toute matrice Y, on a, d'après la question 1, $\mathrm{AX} = \mathrm{XA}$. Ainsi A commute avec toute matrice X ; il s'agit donc d'une matrice scalaire. Cela résulte du fait (démontré page 269) que le centre de $\mathcal{L}(\mathrm{E})$ est l'ensemble des homothéties. Donnons-en une démonstration directe. Si $\mathrm{A} = (a_{ij})_{1\leqslant i,j\leqslant n}$, on a pour $1 \leqslant i, j \leqslant n$,

$$\mathrm{A}\mathrm{E}_{ij} = \sum_{1\leqslant k,l\leqslant n} a_{kl}\mathrm{E}_{kl}\mathrm{E}_{ij} = \sum_{k=1}^{n} a_{ki}\mathrm{E}_{kj}$$
$$= \mathrm{E}_{ij}\mathrm{A} = \sum_{1\leqslant k,l\leqslant n} a_{kl}\mathrm{E}_{ij}\mathrm{E}_{kl} = \sum_{l=1}^{n} a_{jl}\mathrm{E}_{il}.$$

Par unicité de l'écriture, on obtient $a_{ki} = 0$ pour $k \neq i$ et $a_{ii} = a_{jj}$: A est bien une matrice scalaire. On retrouve ainsi que $f = f_{\mathrm{A}}$ est colinéaire à la trace. $\lhd$

Notons que la seconde question fournit une caractérisation de la trace (à un scalaire près) parmi les formes linéaires. Les formes linéaires permettent de caractériser analytiquement l'appartenance à un hyperplan. Le résultat que l'on vient de voir est donc naturellement utilisé dans l'exercice suivant.

7.9. Tout hyperplan de $\mathcal{M}_n(\mathrm{K})$ coupe $\mathrm{GL}_n(\mathrm{K})$

Montrer que pour $n \geqslant 2$, tout hyperplan de $\mathcal{M}_n(\mathrm{K})$ rencontre $\mathrm{GL}_n(\mathrm{K})$.

(École polytechnique)

▷ **Solution.**

Soit H un hyperplan de $\mathcal{M}_n(\mathrm{K})$. C'est donc le noyau d'une forme linéaire non nulle f. D'après l'exercice précédent, il existe $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$ non nulle, telle que pour tout $\mathrm{X} \in \mathcal{M}_n(\mathrm{K})$, $f(\mathrm{X}) = \mathrm{Tr}(\mathrm{AX})$.

Le problème est donc de montrer qu'il existe X inversible telle que AX soit de trace nulle. On va une fois de plus utiliser la notion de matrice équivalente. Notons $r \geqslant 1$ le rang de A. Nous savons qu'il existe P et Q dans $\mathrm{GL}_n(\mathrm{K})$ tels que $\mathrm{PAQ} = \mathrm{J}_r = \begin{pmatrix} \mathrm{I}_r & 0 \\ 0 & 0 \end{pmatrix}$. Alors, si $\mathrm{X} \in \mathcal{M}_n(\mathrm{K})$, $\mathrm{Tr}(\mathrm{AX}) = \mathrm{Tr}(\mathrm{PJ}_r\mathrm{QX}) = \mathrm{Tr}(\mathrm{J}_r\mathrm{QXP})$. Il nous suffit donc de trouver une matrice inversible Y telle que $\mathrm{Tr}(\mathrm{J}_r\mathrm{Y}) = 0$ (on posera $\mathrm{X} = \mathrm{Q}^{-1}\mathrm{YP}^{-1}$ qui sera donc dans $\mathrm{GL}_n(\mathrm{K})$ et dans H). La matrice de permutation

$$\mathrm{Y} = \begin{pmatrix} 0 & 0 & \dots & \dots & 0 & 1 \\ 1 & 0 & \ddots & & & 0 \\ 0 & 1 & 0 & & & \vdots \\ \vdots & & \ddots & \ddots & & \vdots \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & 1 & 0 \end{pmatrix}$$

convient car $\mathrm{J}_r\mathrm{Y}$ a sa diagonale nulle. ◁

Une question se pose alors naturellement. Quelle est la dimension maximale d'un sous-espace vectoriel de $\mathcal{M}_n(\mathrm{K})$ qui ne rencontre pas le groupe linéaire ? C'est au moins $n(n-1)$ puisque le sous-espace formé des matrices dont la dernière colonne est nulle convient. L'exercice suivant détermine plus généralement la dimension maximale d'un sous-espace vectoriel de $\mathcal{M}_n(\mathrm{K})$ dont tous les éléments sont de rang inférieur à p, le cas $p = n-1$ répondant à la question posée au début.

7.10. Dimension maximale de sous-espaces de matrices de rang $\leqslant p$

Soit V un sous-espace de $\mathcal{M}_n(\mathbb{R})$ tel que, pour tout $\mathrm{M} \in \mathrm{V}$, on ait $\mathrm{rg}\,\mathrm{M} \leqslant p$. On souhaite démontrer que $\dim \mathrm{V} \leqslant pn$.

1. Montrer que que l'on peut se ramener au cas où V contient la matrice $\left(\begin{array}{c|c} \mathrm{I}_p & 0 \\ \hline 0 & 0 \end{array}\right)$. Cette condition sera supposée réalisée par la suite.

Montrer que toute matrice de V peut s'écrire $\left(\begin{array}{c|c} A & C \\ \hline B & 0 \end{array}\right)$, avec $A \in \mathcal{M}_p(\mathbb{R})$, $B \in \mathcal{M}_{n-p,p}(\mathbb{R})$, $C \in \mathcal{M}_{p,n-p}(\mathbb{R})$ et $BC = 0$.

2. Conclure, en considérant l'application qui à tout élément $\left(\begin{array}{c|c} A & C \\ \hline B & 0 \end{array}\right)$ de V associe $(A, {}^tB + C)$, élément de l'espace vectoriel $E = \mathcal{M}_p(\mathbb{R}) \times \mathcal{M}_{p,n-p}(\mathbb{R})$.

3. Montrer que le résultat reste vrai lorsqu'on remplace le corps de base $\mathbb{R}$ par un corps quelconque infini K. Pour cela, on considérera l'application q qui à $\left(\begin{array}{c|c} A & C \\ \hline B & 0 \end{array}\right)$ associe $\left(\begin{array}{c|c} 0 & C \\ \hline B & 0 \end{array}\right)$, $W = q(V)$ et l'application $\Phi : \left(\begin{array}{c|c} 0 & C \\ \hline B & 0 \end{array}\right) \in W \longmapsto C \in \mathcal{M}_{p,n-p}(K)$ et on montrera que si $\left(\begin{array}{c|c} 0 & 0 \\ \hline B & 0 \end{array}\right) \in \operatorname{Ker}\Phi$, alors pour tout $C' \in \operatorname{Im}\Phi$, on a $BC' = 0$. On en déduira que $\dim W \leqslant p(n-p)$, avant de conclure.

(École normale supérieure)

▷ **Solution.**

1. • On peut supposer que V contient une matrice de rang p (sinon on remplace p par le rang maximal d'un élément de V). Une telle matrice peut s'écrire $R\left(\begin{array}{c|c} I_p & 0 \\ \hline 0 & 0 \end{array}\right)S$, avec R et S inversibles. On considère alors $V' = \{R^{-1}MS^{-1}, M \in V\}$, qui est un sous-espace de $\mathcal{M}_n(\mathbb{R})$ de même dimension que V (puisque l'application $M \longmapsto R^{-1}MS^{-1}$ est un automorphisme de $\mathcal{M}_n(\mathbb{R})$) et dont les éléments sont encore de rang inférieur à p. Il suffit donc de démontrer le résultat pour V', qui contient la matrice $P = \left(\begin{array}{c|c} I_p & 0 \\ \hline 0 & 0 \end{array}\right)$. On suppose désormais que V contient P. Soit $M = \left(\begin{array}{c|c} A & C \\ \hline B & D \end{array}\right)$ dans V, avec $A \in \mathcal{M}_p(\mathbb{R})$, $B \in \mathcal{M}_{n-p,p}(\mathbb{R})$, $C \in \mathcal{M}_{p,n-p}(\mathbb{R})$ et $D \in \mathcal{M}_{n-p}(\mathbb{R})$.

• Considérons, pour $\lambda \in \mathbb{R}$, la matrice $M - \lambda P = \left(\begin{array}{c|c} A - \lambda I_p & C \\ \hline B & D \end{array}\right)$. Celle-ci est dans V ; son rang est donc inférieur ou égal à p. Considérons une matrice d'ordre $p+1$ extraite de $M - \lambda P$ et bordant la matrice $A - \lambda I_p$. Elle sera donc de la forme $\left(\begin{array}{c|c} A - \lambda I_p & Y_j \\ \hline X_i & d_{ij} \end{array}\right)$, avec $1 \leqslant i, j \leqslant n-p$, d_{ij} étant un coefficient quelconque de la matrice D, X_i la i-ème ligne de B et Y_j la j-ème colonne de C. Les indices i et j étant fixés, considérons l'application f qui, à tout réel λ associe le déterminant de la matrice

$\left(\begin{array}{c|c} \mathrm{A}-\lambda \mathrm{I}_p & \mathrm{Y}_j \\ \hline \mathrm{X}_i & d_{ij} \end{array}\right)$. C'est une fonction polynomiale. La matrice $\mathrm{M}-\lambda\mathrm{P}$ étant de rang inférieur ou égal à p, puisque dans V, on a $f(\lambda)=0$ pour tout réel λ : f est la fonction nulle.

$\star$ Le coefficient de λ^p dans f est $(-1)^p d_{ij}$. On a donc $d_{ij}=0$. Comme cela est vrai pour tout (i,j) tel que $1 \leqslant i,j \leqslant n-p$, on en déduit que $\mathrm{D}=0$.

$\star$ Examinons maintenant le coefficient de λ^{p-1}. Nommons e_1, e_2,..., e_n les vecteurs de la base canonique de $\mathbb{R}^n$, $\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_p$ les vecteurs colonnes de la matrice $\begin{pmatrix} \mathrm{A} \\ \mathrm{X}_i \end{pmatrix}$ et $\mathrm{Z}=\begin{pmatrix} \mathrm{Y}_j \\ 0 \end{pmatrix}$. Alors, pour tout $\lambda \in \mathbb{R}$,

$$f(\lambda)=\det(\mathrm{C}_1-\lambda e_1, \mathrm{C}_2-\lambda e_2, \ldots, \mathrm{C}_p-\lambda e_p, \mathrm{Z}).$$

On calcule ce déterminant en utilisant la multilinéarité et on trouve que le coefficient de λ^{p-1} est

$$\sum_{k=1}^{p} \det(-\lambda e_1, \ldots, -\lambda e_{k-1}, \mathrm{C}_k, -\lambda e_{k+1}, \ldots, -\lambda e_p, \mathrm{Z}).$$

En posant $\mathrm{X}_i=(x_1, x_2, \ldots, x_p)$ et $\mathrm{Y}_j={}^t(y_1, y_2, \ldots, y_p)$, on obtient, pour $1 \leqslant k \leqslant p$,

$$\det(-\lambda e_1, \ldots, -\lambda e_{k-1}, \mathrm{C}_k, -\lambda e_{k+1}, \ldots, -\lambda e_p, \mathrm{Z}) =$$

$$\begin{vmatrix} -\lambda & & a_{1k} & & & y_1 \\ & \ddots & \vdots & & & \vdots \\ & & a_{kk} & & & y_k \\ & & \vdots & \ddots & & \vdots \\ & & a_{pk} & & -\lambda & y_p \\ 0 & \ldots & x_k & \ldots & 0 & 0 \end{vmatrix} = (-\lambda)^{p-1} \begin{vmatrix} a_{kk} & y_k \\ x_k & 0 \end{vmatrix} = (-\lambda)^p x_k y_k.$$

Le coefficient de λ^{p-1} est donc $(-1)^p \sum_{k=1}^{p} x_k y_k = (-1)^{p-1}\mathrm{X}_i\mathrm{Y}_j$. On a donc, pour $1 \leqslant i,j \leqslant n-p$, $\mathrm{X}_i\mathrm{Y}_j=0$. Puisque X_i est le i-ième vecteur ligne de B et Y_j le j-ième vecteur colonne de C, $\mathrm{X}_i\mathrm{Y}_j$ est le coefficient d'indice ij de BC. On obtient finalement $\mathrm{BC}=0$.

Nous avons démontré que tout élément de V s'écrit $\mathrm{M}=\left(\begin{array}{c|c} \mathrm{A} & \mathrm{C} \\ \hline \mathrm{B} & 0 \end{array}\right)$, avec $\mathrm{A} \in \mathcal{M}_p(\mathbb{R})$, $\mathrm{B} \in \mathcal{M}_{n-p,p}(\mathbb{R})$, $\mathrm{C} \in \mathcal{M}_{p,n-p}(\mathbb{R})$ et $\mathrm{BC}=0$.

2. Considérons l'application Φ qui à toute matrice $\mathrm{M} \in \mathrm{V}$, écrite comme ci-dessus, associe le couple $(\mathrm{A}, {}^t\mathrm{B}+\mathrm{C})$, élément de l'espace vectoriel $\mathrm{E}=\mathcal{M}_p(\mathbb{R}) \times \mathcal{M}_{p,n-p}(\mathbb{R})$. L'application Φ est clairement

linéaire. Montrons qu'elle est injective. L'égalité $\Phi(\mathrm{M}) = 0$ équivaut à $\mathrm{A} = {}^t\mathrm{B} + \mathrm{C} = 0$. Sachant que $\mathrm{BC} = 0$, on a alors $\mathrm{B}\,{}^t\mathrm{B} = -\mathrm{BC} = 0$. Pour tout $k \in [\![1, p]\!]$, le coefficient d'indice (k, k) de $\mathrm{B}\,{}^t\mathrm{B}$ est $\sum\limits_{j=1}^{n-p} b_{jk}^2$. On a donc $b_{jk} = 0$ pour $1 \leqslant k \leqslant p$ et $1 \leqslant j \leqslant n - p$. Finalement $\mathrm{B} = 0$ et donc $\mathrm{C} = 0$. La matrice M est nulle.

De l'injectivité de Φ, on déduit que $\dim \mathrm{V} = \dim(\operatorname{Im}\Phi) \leqslant \dim \mathrm{E}$. Sachant que $\dim \mathrm{E} = p^2 + p(n-p) = np$, on peut donc affirmer que $\dim \mathrm{V} \leqslant np$.

3. Par des arguments analogues à ceux développés dans la première question, on se ramène au cas où toute matrice de V s'écrit $\left(\begin{array}{c|c} \mathrm{A} & \mathrm{C} \\ \hline \mathrm{B} & 0 \end{array}\right)$, avec $\mathrm{A} \in \mathcal{M}_p(\mathrm{K})$, $\mathrm{B} \in \mathcal{M}_{n-p,p}(\mathrm{K})$, $\mathrm{C} \in \mathcal{M}_{p,n-p}(\mathrm{K})$ et $\mathrm{BC} = 0$ (la nullité du polynôme f est assurée par le fait que tout élément de K, qui est supposé infini, est racine de f).

L'application q étant linéaire, W est un sous-espace vectoriel de $\mathcal{M}_n(\mathrm{K})$. D'après ce qui précède, tout élément $\left(\begin{array}{c|c} 0 & \mathrm{C} \\ \hline \mathrm{B} & 0 \end{array}\right)$ de W vérifie $\mathrm{BC} = 0$. Soit $\left(\begin{array}{c|c} 0 & 0 \\ \hline \mathrm{B} & 0 \end{array}\right) \in \operatorname{Ker}\Phi$. Si $\mathrm{C}' = \Phi\left(\left(\begin{array}{c|c} 0 & \mathrm{C}' \\ \hline \mathrm{B}' & 0 \end{array}\right)\right) \in \operatorname{Im}\Phi$, alors la matrice $\left(\begin{array}{c|c} 0 & \mathrm{C}' \\ \hline \mathrm{B}+\mathrm{B}' & 0 \end{array}\right)$ est dans W, comme somme de deux éléments de W, et on a donc

$$0 = (\mathrm{B} + \mathrm{B}')\mathrm{C}' = \mathrm{BC}' + \mathrm{B}'\mathrm{C}' = \mathrm{BC}',$$

car $\mathrm{B}'\mathrm{C}' = 0$. En identifiant les matrices aux endomorphismes canoniquement associés, on obtient donc, pour tout $\mathrm{C}' \in \operatorname{Im}\Phi$, $\operatorname{Im}\mathrm{C}' \subset \operatorname{Ker}\mathrm{B}$.

Considérons $\mathrm{W}' = \left\{\mathrm{B} \in \mathcal{M}_{n-p,p}(\mathrm{K}),\ \left(\begin{array}{c|c} 0 & 0 \\ \hline \mathrm{B} & 0 \end{array}\right) \in \mathrm{W}\right\}$. Cet espace vectoriel est isomorphe à $\operatorname{Ker}\Phi$. Posons $\mathrm{E} = \bigcap\limits_{\mathrm{B}\in\mathrm{W}'} \operatorname{Ker}\mathrm{B}$. On a, pour tout $\mathrm{C}' \in \operatorname{Im}\Phi$, $\operatorname{Im}\mathrm{C}' \subset \mathrm{E}$. Les éléments de $\operatorname{Im}\Phi$ s'identifient donc à des éléments de $\mathcal{L}(\mathrm{K}^{n-p}, \mathrm{E})$. On en déduit que $\dim \operatorname{Im}\Phi \leqslant (n-p)\dim \mathrm{E}$. Si on considère un supplémentaire E' de E dans K^p, on a, pour tout $\mathrm{B} \in \mathrm{W}'$, $\mathrm{E} \subset \operatorname{Ker}\mathrm{B}$ et les éléments de W' s'identifient à des éléments de $\mathcal{L}(\mathrm{E}', \mathrm{K}^{n-p})$. On a donc $\dim \operatorname{Ker}\Phi = \dim \mathrm{W}' \leqslant (n-p)\dim \mathrm{E}'$. Du théorème du rang, on déduit alors que

$$\dim \mathrm{W} = \dim \operatorname{Im}\Phi + \dim \operatorname{Ker}\Phi \leqslant (n-p)(\dim \mathrm{E} + \dim \mathrm{E}') = (n-p)p.$$

Considérons maintenant l'ensemble W'' des matrices de $\mathcal{M}_n(\mathrm{K})$ de la forme $\left(\begin{array}{c|c} \mathrm{A} & 0 \\ \hline 0 & 0 \end{array}\right)$, avec $\mathrm{A} \in \mathcal{M}_p(\mathrm{K})$. Il est clair que $\mathrm{V} \subset \mathrm{W} \oplus \mathrm{W}''$. On en déduit que

$$\dim \mathrm{V} \leqslant \dim \mathrm{W} + \dim \mathrm{W}'' \leqslant (n-p)p + p^2 \leqslant np. \quad \lhd$$

Cette dimension maximale est atteinte : on peut exhiber sans mal un sous-espace de dimension np formé de matrices de rang $\leqslant p$, par exemple l'ensemble des matrices ayant leurs $n-p$ dernières colonnes nulles.

L'exercice qui suit exploite les propriétés de l'orthogonalité duale et la connaissance des formes linéaires sur $\mathcal{M}_n(\mathrm{K})$. Pour des rappels sur la dualité, on se reportera à la page 298 du chapitre 6 (Espaces vectoriels).

7.11. Orthogonalité duale

Soit $(\mathrm{A},\mathrm{B}) \in \mathcal{M}_n(\mathrm{K})^2$. Montrer l'équivalence des deux assertions suivantes :

(i) $\exists \mathrm{X} \in \mathcal{M}_n(\mathrm{K})$, $\mathrm{AX}+\mathrm{XA}=\mathrm{B}$;

(ii) $\forall \mathrm{C} \in \mathcal{M}_n(\mathrm{K})$, $\mathrm{AC}+\mathrm{CA}=0 \Longrightarrow \mathrm{Tr}(\mathrm{BC})=0$.

(**École normale supérieure**)

▷ **Solution.**

• L'implication $(i) \Longrightarrow (ii)$ résulte d'un simple calcul. Soit C dans $\mathcal{M}_n(\mathrm{K})$ telle que $\mathrm{AC}+\mathrm{CA}=0$. On a alors

$$\begin{aligned}\mathrm{Tr}(\mathrm{BC}) &= \mathrm{Tr}(\mathrm{AXC}+\mathrm{XAC}) = \mathrm{Tr}(\mathrm{AXC})+\mathrm{Tr}(\mathrm{XAC})\\ &= \mathrm{Tr}(\mathrm{CAX})+\mathrm{Tr}(\mathrm{ACX}) = \mathrm{Tr}((\mathrm{AC}+\mathrm{CA})\mathrm{X}) = 0,\end{aligned}$$

car on sait que, pour tout couple $(\mathrm{M},\mathrm{N}) \in \mathcal{M}_n(\mathrm{K})^2$, $\mathrm{Tr}(\mathrm{MN})=\mathrm{Tr}(\mathrm{NM})$.

• Pour montrer que $(ii) \Longrightarrow (i)$, interprétons les deux conditions. L'application $f : \mathcal{M}_n(\mathrm{K}) \to \mathcal{M}_n(\mathrm{K})$ définie par $f(\mathrm{X})=\mathrm{AX}+\mathrm{XA}$ est un endomorphisme de $\mathcal{M}_n(\mathrm{K})$. L'assertion (i) signifie que B appartient au sous-espace $\mathrm{Im}\, f$. Essayons de dégager la signification de (ii). Pour tout $\mathrm{C} \in \mathcal{M}_n(\mathrm{K})$, l'application $\mathrm{T_C} : \mathrm{M} \longmapsto \mathrm{Tr}(\mathrm{CM})$ est une forme linéaire sur $\mathcal{M}_n(\mathrm{K})$ et on a vu dans l'exercice 7.8 que l'application T qui à C associe la forme $\mathrm{T_C}$ est un isomorphisme de $\mathcal{M}_n(\mathrm{K})$ sur son dual. Notons F le sous-espace $\mathrm{T}(\mathrm{Ker}\, f)$ de $\mathcal{M}_n(\mathrm{K})^*$. La condition (ii) s'écrit : pour tout $\mathrm{C} \in \mathrm{Ker}\, f$, $\mathrm{T_C}(\mathrm{B})=0$. Elle signifie simplement que B appartient à F°, orthogonal dual de F. La première implication a montré que $\mathrm{Im}\, f \subset \mathrm{F}^\circ$. L'égalité provient simplement du fait que les deux espaces ont la même dimension, puisque $\dim \mathrm{F}^\circ = n^2 - \dim \mathrm{F} = n^2 - \dim \mathrm{Ker}\, f = \dim \mathrm{Im}\, f$. ◁

Si A, B *sont deux matrices de* $\mathcal{M}_n(\mathrm{K})$, *on appelle crochet de Lie de* A *et* B, *la matrice* $[\mathrm{A},\mathrm{B}] = \mathrm{AB}-\mathrm{BA}$. *Il s'agit d'une nouvelle loi de composition interne sur* $\mathcal{M}_n(\mathrm{K})$, *qui en fait une algèbre de Lie*[1].

1. Le lecteur intéressé pourra consulter : MNEIMNÉ (R.) et TESTARD (F.), *Introduction à la théorie des groupes de Lie classiques*, Hermann, 1986.

L'exercice suivant se propose de déterminer, en caractéristique nulle, les matrices qui sont des crochets de Lie.

7.12. Crochets de Lie de $\mathcal{M}_n(\mathrm{K})$

Soit K un corps de caractéristique nulle.

1. Montrer qu'une matrice de $\mathcal{M}_n(\mathrm{K})$ de trace nulle est semblable à une matrice de diagonale nulle.

2. Montrer que si une matrice $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$ est de trace nulle, il existe B et C dans $\mathcal{M}_n(\mathrm{K})$ telles que $\mathrm{A} = \mathrm{BC} - \mathrm{CB} = [\mathrm{B}, \mathrm{C}]$ (crochet de Lie).

(**École normale supérieure**)

▷ **Solution.**

1. On va procéder par récurrence sur $n \geqslant 1$, le résultat étant trivial pour $n = 1$. Supposons $n \geqslant 2$ et A non nulle. Alors, A n'est pas la matrice d'une homothétie car si $\lambda \in \mathrm{K}^*$, la trace de $\lambda \mathrm{I}$ n'est pas nulle, puisque K est un corps de caractéristique nulle. Il existe donc $e \in \mathrm{K}^n$ tel que $(e, \mathrm{A}e)$ soit libre (d'après le résultat rappelé avant l'exercice 6.6). On pose $e'_1 = e$ et $e'_2 = \mathrm{A}(e)$ et on complète le système libre (e'_1, e'_2) en une base $\mathcal{B}' = (e'_1, e'_2, \ldots, e'_n)$ de K^n. On note $\mathcal{B} = (e_1, e_2, \ldots, e_n)$ la base canonique de K^n. Si P est la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$, $\mathrm{P}^{-1}\mathrm{AP}$ s'écrit

$$\mathrm{P}^{-1}\mathrm{AP} = \left(\begin{array}{c|c} 0 & \times \ \ldots\ldots \ \times \\ \hline \mathbf{1} & \\ 0 & \\ \vdots & \mathrm{A}' \\ 0 & \end{array}\right) \quad \text{avec } \mathrm{A}' \in \mathcal{M}_{n-1}(\mathrm{K}).$$

On a alors $\operatorname{Tr} \mathrm{A} = 0 + \operatorname{Tr} \mathrm{A}' = 0$. D'après l'hypothèse de récurrence, il existe $\mathrm{Q} \in \mathrm{GL}_{n-1}(\mathrm{K})$ tel que $\mathrm{Q}^{-1}\mathrm{A}'\mathrm{Q}$ soit à diagonale nulle. Posons

$$\mathrm{P}' = \left(\begin{array}{c|c} \mathbf{1} & 0\,0 \ \ldots \ 0 \\ \hline 0 & \\ \vdots & \mathrm{Q} \\ 0 & \end{array}\right) \in \mathrm{GL}_n(\mathrm{K}).$$

On obtient, d'après les règles de multiplication par blocs,

$$\mathrm{P}'^{-1}\mathrm{P}^{-1}\mathrm{APP}' = \left(\begin{array}{c|c} 0 & \times \ \ldots\ldots \ \times \\ \hline \times & \\ \vdots & \mathrm{Q}^{-1}\mathrm{A}'\mathrm{Q} \\ \times & \end{array}\right).$$

Comme $Q^{-1}A'Q$ est de diagonale nulle, $(PP')^{-1}APP'$ l'est aussi. La récurrence est achevée.

Ce résultat ne demeure pas en caractéristique non nulle. Par exemple, pour tout p premier, Id_p a une trace nulle dans $\mathcal{M}_p(\mathbb{Z}/p\mathbb{Z})$ et n'est évidemment semblable qu'à elle-même.

2. Nous savons que $\mathrm{Tr}(BC) = \mathrm{Tr}(CB)$, pour tous B et C dans $\mathcal{M}_n(K)$. On en déduit que tout crochet de Lie est de trace nulle. Il faut démontrer la réciproque. Observons, pour commencer, que si $A = [B, C]$ est un crochet de Lie, alors toute matrice semblable à A en est un aussi, puisque, pour tout $P \in GL_n(K)$, $P^{-1}AP = [P^{-1}BP, P^{-1}CP]$. La question précédente permet donc de supposer que la diagonale de A est nulle.

L'idée est de fixer une matrice B «simple», par exemple diagonale, et de regarder l'ensemble des crochets de Lie $[B, C]$, où C décrit $\mathcal{M}_n(K)$. Considérons $B = \mathrm{Diag}(b_1, \ldots, b_n)$ et considérons l'endomorphisme ad_B de $\mathcal{M}_n(K)$ définie par $ad_B(C) = [B, C]$. En notant $C = (c_{ij})$, on obtient $ad_B(C) = [B, C] = ((b_i - b_j)c_{ij})$. On voit déjà que $\mathrm{Im}\, ad_B$ est inclus dans l'ensemble des matrices de diagonale nulle. Si on prend soin de choisir les b_i deux à deux distincts (ce qui est possible puisque K est infini), on a alors $[B, C] = 0$ si et seulement si C est diagonale. Le noyau de ad_B (qui n'est autre que le commutant de B) est dans ce cas de dimension n. Par le théorème du rang, on obtient $\dim(\mathrm{Im}\, ad_B) = n^2 - n$. C'est exactement la dimension du sous-espace vectoriel de $\mathcal{M}_n(K)$ formé des matrices de diagonale nulle ; celui-ci est donc égal à $\mathrm{Im}\, ad_B$.

Conclusion. Toute matrice de trace nulle est un crochet de Lie. $\lhd$

Le lecteur intéressé pourra consulter le problème de l'ENSET de 1983 où l'on démontre que, pour $n \geqslant 3$, le résultat de la seconde question reste vrai pour tout corps K différent de $\mathbb{Z}/2\mathbb{Z}$.

7.13. Diagonales possibles dans une classe de similitude

> Soit $A \in \mathcal{M}_n(K)$. Quels sont les n-uplets $(a_1, \ldots, a_n) \in K^n$ tels qu'il existe une matrice de diagonale $(a_1, \ldots, a_n)$ semblable à A ?
> (**École normale supérieure**)

$\rhd$ **Solution.**

On identifiera matrice et endomorphisme canoniquement associé. Il est connu que si A est une matrice scalaire λI_n, elle n'est semblable qu'à elle même. Dans ce cas particulier, seul $(\lambda, \ldots, \lambda)$ convient.

Supposons désormais que A n'est pas une matrice scalaire. Nous savons que la trace est un invariant de similitude. Si $(a_1, \ldots, a_n)$ convient, nécessairement $a_1 + \cdots + a_n = \mathrm{Tr}\, A$. Nous allons démontrer par récurrence sur n que $a_1 + \cdots + a_n = \mathrm{Tr}\, A$ est une condition suffisante pour A soit semblable à une matrice de diagonale $(a_1, \ldots, a_n)$.

Prenons $n \geqslant 2$, $\mathrm{A} \in \mathcal{M}_n(\mathrm{K})$ et $(a_1, \ldots, a_n) \in \mathrm{K}^n$ de somme $\operatorname{Tr} \mathrm{A}$. La matrice $\mathrm{A}' = \mathrm{A} - a_1 \mathrm{I}_n$ n'est pas scalaire. Classiquement, il existe donc e_1 un vecteur de K^n tel que $(e_1, \mathrm{A}'e_1)$ soit libre (voir page 269). On complète ce système libre en une base $(e_1, e_2, \ldots, e_n)$ de K^n (avec $e_2 = \mathrm{A}'e_1$). Via ce changement de base, la matrice A' est donc semblable à une matrice qui admet comme première colonne $\begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ et A est semblable à

$$\mathrm{A}'' = \begin{pmatrix} a_1 & \times & \times & \times \\ 1 & & & \\ 0 & & \mathrm{B} & \\ \vdots & & & \\ 0 & & & \end{pmatrix}.$$

Si $n = 2$, B est un scalaire b qui vérifie $\operatorname{Tr} \mathrm{A} = \operatorname{Tr} \mathrm{A}'' = a_1 + b$; c'est forcément a_2. Le résultat est vérifié.

Supposons $n \geqslant 3$. Si B n'est pas une matrice scalaire, comme sa trace est

$$\operatorname{Tr} \mathrm{B} = \operatorname{Tr} \mathrm{A} - a_1 = a_2 + \cdots + a_n,$$

il existe, par hypothèse de récurrence, P inversible de taille $n-1$ telle que $\mathrm{P}^{-1}\mathrm{BP}$ soit de diagonale $(a_2, \ldots, a_n)$. Si on pose $\mathrm{Q} = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{P} \end{pmatrix}$, un produit par blocs donne

$$\mathrm{Q}^{-1}\mathrm{A}''\mathrm{Q} = \begin{pmatrix} a_1 & \times \\ \times & \mathrm{P}^{-1}\mathrm{BP} \end{pmatrix},$$

qui est une matrice de diagonale $(a_1, \ldots, a_n)$.

Reste à traiter le cas où B est scalaire de la forme $\lambda \mathrm{I}_{n-1}$. Changeons dans la base e_3 en $e_3' = e_3 + e_1$. La famille $(e_1, e_2, e_3', e_4, \ldots, e_n)$ est encore une base de K^n. Par ce changement de base, on voit que la matrice A est semblable à

$$\begin{pmatrix} a_1 & \times & \times & \times & \times & \times \\ 1 & \lambda & 1 & 0 & \vdots & 0 \\ 0 & 0 & \lambda & & & \cdots \\ \vdots & \vdots & & \ddots & & \vdots \\ \vdots & \vdots & & & \ddots & 0 \\ 0 & 0 & \ldots & \ldots & 0 & \lambda \end{pmatrix}$$

ce qui nous ramène au cas où B n'est pas scalaire. Le résultat est ainsi démontré. $\lhd$

Voici, pour terminer cette série sur les traces, un joli petit exercice de congruence qu'on peut regarder comme une généralisation du petit théorème de Fermat.

7.14. Traces modulo p

Soit p un nombre premier, A et B deux matrices de $\mathcal{M}_n(\mathbb{Z})$.

1. Montrer que $\mathrm{Tr}(\mathrm{A}+\mathrm{B})^p \equiv \mathrm{Tr}\,\mathrm{A}^p + \mathrm{Tr}\,\mathrm{B}^p\ [p]$.

2. En déduire que $\mathrm{Tr}\,\mathrm{A}^p \equiv \mathrm{Tr}\,\mathrm{A}\ [p]$.

3. Soit la suite récurrente (u_n) définie par $u_0 = 3$, $u_1 = 0$, $u_2 = 2$ et, pour tout $n \in \mathbb{N}$, $u_{n+3} = u_{n+1} + u_n$. Montrer que p divise u_p pour tout p premier.

(**École normale supérieure**)

$\rhd$ **Solution.**

1. Si les matrices A et B commutent, on peut appliquer la formule du binôme : $(\mathrm{A}+\mathrm{B})^p = \sum_{k=0}^{n} \mathrm{C}_p^k \mathrm{A}^k \mathrm{B}^{p-k}$. On prend la trace et on passe modulo p. Comme p divise C_p^k pour $1 \leqslant k \leqslant p-1$, il vient

$$\mathrm{Tr}(\mathrm{A}+\mathrm{B})^p \equiv \sum_{k=0}^{p} \mathrm{C}_p^k\, \mathrm{Tr}(\mathrm{A}^k\mathrm{B}^{p-k}) \equiv \mathrm{Tr}\,\mathrm{A}^p + \mathrm{Tr}\,\mathrm{B}^p\ [p].$$

Dans le cas général, en absence de commutativité, le développement de $(\mathrm{A}+\mathrm{B})^p$ donne une somme de 2^p termes :

$$(\mathrm{A}+\mathrm{B})^p = \sum_{(\mathrm{A}_1,\mathrm{A}_2,\ldots,\mathrm{A}_p)\in\{\mathrm{A},\mathrm{B}\}^p} \mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_p.$$

Dans la somme de droite, certains p-uplets vont conduire à la même trace grâce à la propriété $\mathrm{Tr}(\mathrm{XY}) = \mathrm{Tr}(\mathrm{YX})$.

Précisons cela en utilisant une opération de groupe. Soit G le sous-groupe de $\mathcal{S}_p$ engendré par le p-cycle $c = (1, 2, \ldots, p)$. C'est un groupe cyclique de cardinal p. On définit une opération de groupe de G sur $\{\mathrm{A},\mathrm{B}\}^p$ par $c\cdot(\mathrm{A}_1,\ldots,\mathrm{A}_p) = (\mathrm{A}_2,\ldots,\mathrm{A}_p,\mathrm{A}_1)$. La propriété de la trace rappelée ci-dessus montre que si $(\mathrm{A}_1,\ldots,\mathrm{A}_p)$ et $(\mathrm{A}'_1,\ldots,\mathrm{A}'_p)$ sont dans la même orbite, alors $\mathrm{Tr}(\mathrm{A}_1\ldots\mathrm{A}_p) = \mathrm{Tr}(\mathrm{A}'_1\ldots\mathrm{A}'_p)$. Or les orbites ont pour cardinal un diviseur de $|\mathrm{G}| = p$. Elles sont donc toutes de cardinal p, excepté celles qui sont de cardinal 1, c'est-à-dire les orbites de $(\mathrm{A},\mathrm{A},\ldots,\mathrm{A})$ et $(\mathrm{B},\mathrm{B},\ldots,\mathrm{B})$. Il en résulte que $\mathrm{Tr}(\mathrm{A}+\mathrm{B})^p \equiv \mathrm{Tr}\,\mathrm{A}^p + \mathrm{Tr}\,\mathrm{B}^p\ [p]$.

2. Soit E le sous-ensemble de $\mathcal{M}_n(\mathbb{Z})$ formé des matrices A vérifiant $\mathrm{Tr}(\mathrm{A}^p) \equiv \mathrm{Tr}(\mathrm{A})\ [p]$. La question précédente montre que E est stable pour l'addition. Si $\mathrm{A} \in \mathrm{E}$, une récurrence immédiate montre que $k\mathrm{A} \in \mathrm{E}$ pour tout $k \in \mathbb{N}$. On a ensuite, en distinguant les cas $p = 2$ et p impair,

$$\mathrm{Tr}(-\mathrm{A})^p \equiv (-1)^p \,\mathrm{Tr}\,\mathrm{A}^p \equiv (-1)^p \mathrm{A} \equiv -\mathrm{A}\ [p],$$

ce qui montre que $-\mathrm{A} \in \mathrm{E}$. Finalement $k\mathrm{A}$ est dans E, pour tout $k \in \mathbb{Z}$. Le lecteur vérifiera facilement que les matrices E_{ij} de la base canonique sont dans E ($\mathrm{E}_{ij}^p = 0$ si $i \neq j$ et $\mathrm{E}_{ij}^p = \mathrm{E}_{ij}$ si $i = j$). Il en résulte que $\mathrm{E} = \mathcal{M}_n(\mathbb{Z})$, ce qui est le résultat demandé.

3. Considérons la matrice $\mathrm{A} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ associée à la relation de récurrence linéaire : si $\mathrm{X}_n = \begin{pmatrix} u_n \\ u_{n+1} \\ u_{n+2} \end{pmatrix}$ on a $\mathrm{X}_{n+1} = \mathrm{A}\mathrm{X}_n$ pour tout n. On constate que $\mathrm{A}^0 = \mathrm{I}_3$ est de trace 3, que A est de trace nulle et enfin que $\mathrm{A}^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ est de trace 2. Autrement dit, on a $u_n = \mathrm{Tr}\,\mathrm{A}^n$ pour $n \in \{0, 1, 2\}$.

Or, comme $\mathrm{A}^3 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \mathrm{A} + \mathrm{I}_3$ on a $\mathrm{A}^{n+3} = \mathrm{A}^{n+1} + \mathrm{A}^n$ pour tout n et la suite $(\mathrm{Tr}\,\mathrm{A}^n)_{n \geqslant 0}$ vérifie la même relation de récurrence que la suite $(u_n)_{n \geqslant 0}$. On en déduit que $u_n = \mathrm{Tr}\,\mathrm{A}^n$ pour tout n. En particulier, pour tout entier p premier, on a $u_p = \mathrm{Tr}\,\mathrm{A}^p \equiv \mathrm{Tr}\,\mathrm{A} \equiv 0$ modulo p. D'où le résultat. $\lhd$

Le résultat de la seconde question s'obtient directement si on admet que $\mathbb{Z}/p\mathbb{Z}$ possède un sur-corps K, algébriquement clos. Notons $\bar{\mathrm{A}}$ la matrice obtenue à partir de A en prenant les classes modulo p de ses coefficients. La matrice $\bar{\mathrm{A}}$ est trigonalisable dans K. Si on note $\lambda_1, \ldots, \lambda_p$ les valeurs propres de $\bar{\mathrm{A}}$ comptées avec multiplicité, on a

$$\mathrm{Tr}(\bar{\mathrm{A}}^p) = \sum_{i=1}^{p} \lambda_i^p = \left(\sum_{i=1}^{p} \lambda_i\right)^p = (\mathrm{Tr}\,\bar{\mathrm{A}})^p,$$

l'avant-dernière égalité provenant du fait que K est de caractéristique p (pour x et y dans K, on $(x+y)^p = \sum_{k=0}^{p} \mathrm{C}_p^k x^k y^{p-k} = x^p + y^p$, puisque p divise C_p^k si $1 \leqslant k \leqslant p-1$). Comme la trace de $\bar{\mathrm{A}}$ est le résidu modulo p de la trace de A, on obtient $\mathrm{Tr}\,\mathrm{A}^p \equiv (\mathrm{Tr}\,\mathrm{A})^p$ et on conclut avec le petit théorème de Fermat.

Les exercices qui suivent concernent les matrices réelles positives, c'est-à-dire dont tous les coefficients sont positifs. Dans le tome 2 d'algèbre, on trouvera plusieurs exercices sur les propriétés spectrales des matrices positives, notamment le théorème de Perron-Frobenius (exercice 2.10).

7.15. Matrices monotones

On dit qu'une matrice à coefficients réels A est positive, ce qu'on note $A \geqslant 0$, si tous ses coefficients sont positifs ou nuls. On dit que $A \in \mathcal{M}_n(\mathbb{R})$ est monotone si elle est inversible et si $A^{-1} \geqslant 0$.

1. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que $A \geqslant 0$ si et seulement si pour tout vecteur colonne X on a : $X \geqslant 0 \Longrightarrow AX \geqslant 0$.

2. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Montrer que A est monotone si et seulement si pour tout vecteur colonne X on a : $AX \geqslant 0 \Longrightarrow X \geqslant 0$.

3. Soit $(c_1, \ldots, c_n) \in (\mathbb{R}_+)^n$. Montrer que la matrice suivante est monotone :

$$\begin{pmatrix} 2+c_1 & -1 & 0 & \ldots & 0 \\ -1 & 2+c_2 & -1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & -1 \\ 0 & \ldots & \ldots & -1 & 2+c_n \end{pmatrix}.$$

4. Déterminer les matrices qui sont à la fois positives et monotones.

(**École polytechnique**)

▷ **Solution.**

1. Il est clair que le produit de deux matrices positives est encore une matrice positive. Ainsi, si $A \geqslant 0$, on a pour tout $X \geqslant 0$, $AX \geqslant 0$. Réciproquement, les vecteurs $e_1, \ldots, e_n$ de la base canonique de $\mathbb{R}^n$ sont positifs. Il en résulte que les colonnes $Ae_1, \ldots, Ae_n$ de A sont toutes positives. D'où l'équivalence voulue.

2. Supposons A monotone. Comme A^{-1} est positive, si X est tel que $AX \geqslant 0$ alors $A^{-1}AX = X \geqslant 0$ d'après la question précédente.

Réciproquement, supposons que pour tout vecteur colonne X, $AX \geqslant 0$ implique $X \geqslant 0$. Montrons d'abord que A est inversible. Soit $X \in \operatorname{Ker} A$. Comme $AX = 0 \geqslant 0$, on a $X \geqslant 0$. Mais comme $-X$ est aussi dans le noyau de A, on a également $-X \geqslant 0$, de sorte que $X = 0$. A appartient donc à $GL_n(\mathbb{R})$. L'hypothèse peut s'écrire : $AX \geqslant 0$ implique $A^{-1}AX \geqslant 0$ et la question précédente permet de conclure que A^{-1} est positive.

3. On va utiliser la caractérisation obtenue dans la question 2.

Soit $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ tel que $AX \geqslant 0$. En posant $x_0 = x_{n+1} = 0$, cette condition s'écrit : pour tout $k \in [\![1, n]\!]$, $(2 + c_k)x_k \geqslant x_{k-1} + x_{k+1}$. Notons p le plus petit des indices ℓ de $[\![1, n]\!]$ tels que $x_\ell = \min\limits_{1 \leqslant k \leqslant n} x_k$.

• Si $p = 1$ ou n, on tire des inégalités précédentes $(2 + c_p)x_p \geqslant x_p$, soit $(1 + c_p)x_p \geqslant 0$ et donc $x_p \geqslant 0$.

• Si $p \in [\![2, n-1]\!]$, on obtient $(2 + c_p)x_p \geqslant 2x_p$, c'est-à-dire $c_p x_p \geqslant 0$. Si $c_p > 0$, on conclut comme précédemment $x_p \geqslant 0$. Mais il est impossible d'avoir $c_p = 0$, car l'inégalité $2x_p \geqslant x_{p-1} + x_{p+1}$ impose que l'on ait $x_p = x_{p-1} = x_{p+1}$, ce qui est contraire à la définition de p.

On a donc $x_p \geqslant 0$, ce qui implique $X \geqslant 0$, par définition de p.

4. Montrons que les matrices positives et monotones sont les matrices positives ayant exactement un terme non nul par ligne et par colonne, autrement dit les matrices $A = (a_{ij})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{R})$ pour lesquelles il existe une permutation $\sigma \in \mathcal{S}_n$ telle que, pour tout $i \in [\![1, n]\!]$, $a_{i,\sigma(i)} > 0$ et $a_{ij} = 0$ si $j \neq \sigma(i)$.

Un telle matrice est évidemment positive et inversible. D'autre part, si on considère $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$, on obtient $AX = \begin{pmatrix} a_{1,\sigma(1)}x_{\sigma(1)} \\ \vdots \\ a_{n,\sigma(n)}x_{\sigma(n)} \end{pmatrix}$. La condition $AX \geqslant 0$ impose $x_{\sigma(i)} \geqslant 0$, pour tout i et donc $X \geqslant 0$. La matrice A est donc monotone d'après la question 2.

Réciproquement, soit A une matrice positive et monotone. Les termes de sa première colonne sont positifs et l'un au moins est strictement positif, puisque A est inversible. Notons $J = \{i \in [\![1, n]\!], a_{i,1} > 0\}$. Soit $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$ et $Y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = AX$. Fixons $x_2, \ldots, x_n$ strictement positifs. Si $i \notin J$, alors $y_i \geqslant 0$, quel que soit le choix de x_1. Si $i \in J$, alors la condition $y_i \geqslant 0$ équivaut à $x_1 \geqslant -\dfrac{1}{a_{i1}} \sum\limits_{j=2}^{n} a_{ij}x_j$. Notons z_i le terme de droite de cette inégalité. Si, pour tout $i \in J$, on a $z_i < 0$, alors on pourra trouver $x_1 < 0$ vérifiant cette série d'inégalités. On aura alors $AX \geqslant 0$ sans avoir $X \geqslant 0$, ce qui est contradictoire avec A monotone. Il existe donc i tel que $z_i = 0$, c'est-à-dire tel que $a_{ij} = 0$ pour tout $j \neq 1$. Un tel i est unique, sinon A aurait deux lignes proportionnelles. On peut effectuer le même raisonnement pour toutes les colonnes. Pour

tout $j \in [\![1,n]\!]$, il existe un unique $i \in [\![1,n]\!]$ tel que tous les termes de la i-ième ligne soient nuls sauf le j-ième. L'application $j \longmapsto i$ est bijective et en la notant σ^{-1}, A a la forme voulue. $\lhd$

L'exercice suivant étudie les puissances d'une matrice strictement stochastique. Les matrices stochastiques interviennent en probabilités (d'où leur nom). Si X *et* Y *sont deux variables aléatoires à valeurs dans le même ensemble fini* $\mathrm{E} = [\![1,k]\!]$, *la matrice* $\mathrm{A} = (a_{ij}) \in \mathcal{M}_k(\mathbb{R})$ *définie par* $a_{ij} = \mathrm{P}(\mathrm{Y} = j \mid \mathrm{X} = i)$ *est stochastique, ce qui par définition signifie qu'on a* $a_{ij} \geqslant 0$ $(1 \leqslant i,j \leqslant k)$ *et* $\sum_{j=1}^{k} a_{ij} = 1$ $(1 \leqslant i \leqslant k)$.

Indiquons dans quel contexte on rencontre les matrices stochastiques. L'évolution d'un système susceptible de prendre un nombre fini d'états 1, ..., k *est représentée mathématiquement par une suite* $(\mathrm{X}_n)_{n\geq 0}$ *de variables aléatoires à valeurs dans* E. *C'est ce qu'on appelle un processus aléatoire (ou stochastique). Si* X_{n+1} *s'obtient à partir de la valeur de* X_n *et d'un tirage au sort effectué selon une loi ne dépendant que de cette valeur, on dit que le processus est une chaîne de Markov. Les exemples abondent : marches aléatoires, fortune d'un joueur, modélisation de l'alternance des voyelles et des consonnes dans un poème de Pouchkine (par Markov lui-même), ou prévision (en probabilité) des états successifs d'un signal pour améliorer la compression en traitement du signal (Shannon).*

Techniquement, on dit qu'une suite de variables aléatoires (X_n) *est une chaîne de Markov si «la loi de l'état* $n+1$ *conditionnelle au passé ne dépend que de l'état antérieur* n*», ce qui se traduit par*

$$\mathrm{P}(\mathrm{X}_{n+1} = j \mid \mathrm{X}_0 = i_0, \mathrm{X}_1 = i_1, \ldots, \mathrm{X}_n = i_n) = \mathrm{P}(\mathrm{X}_{n+1} = j \mid \mathrm{X}_n = i_n).$$

Si la matrice $\mathrm{A} = (a_{ij}) \in \mathcal{M}_k(\mathbb{R})$ *définie par* $a_{ij} = \mathrm{P}(\mathrm{X}_{n+1} = j \mid \mathrm{X}_n = i)$ *est indépendante de* n, *on dit que la chaîne de Markov est stationnaire.*

Si, dans ce dernier cas, on introduit pour $n \geqslant 0$ *le vecteur-colonne* $\mathrm{Y}_n = \begin{pmatrix} \mathrm{P}(\mathrm{X}_n = 1) \\ \vdots \\ \mathrm{P}(\mathrm{X}_n = k) \end{pmatrix}$, *on obtient* $\mathrm{Y}_{n+1} = \mathrm{A}\mathrm{Y}_n$ *et donc* $\mathrm{Y}_n = \mathrm{A}^n \mathrm{Y}_0$.

Le comportement (probabiliste) d'une chaîne de Markov stationnaire, et notamment son comportement asymptotique, est donc entièrement décrit par la donnée de la loi initiale Y_0 *et des puissances de* A.

7.16. Puissances d'une matrice strictement stochastique

Soit $\mathrm{A} = (a_{ij}) \in \mathcal{M}_n(\mathbb{R})$ une matrice strictement stochastique, c'est-à-dire vérifiant

$$\forall (i,j) \in [\![1,n]\!]^2, \quad a_{ij} > 0 \quad \text{et} \quad \forall i \in [\![1,n]\!], \ \sum_{j=1}^{n} a_{ij} = 1.$$

Soit $\varepsilon = \min_{i,j} a_{ij} > 0$. Pour $k \in \mathbb{N}$, on pose $A^k = (a_{ij}^{(k)})$ et, pour tout $j \in [\![1, n]\!]$, $\alpha_j^{(k)} = \min_i a_{ij}^{(k)}$, $\beta_j^{(k)} = \max_i a_{ij}^{(k)}$ et $\delta_j^{(k)} = \beta_j^{(k)} - \alpha_j^{(k)}$.

1. Montrer que pour tout $k \in \mathbb{N}^*$, A^k est strictement stochastique.

2. Montrer que

$$\alpha_j^{(k)} \leqslant \alpha_j^{(k+1)} \leqslant \beta_j^{(k+1)} \leqslant \beta_j^{(k)} \quad \text{et} \quad \delta_j^{(k+1)} \leqslant (1 - 2\varepsilon)\delta_j^{(k)}.$$

3. En déduire que la suite (A^k) converge vers une matrice que l'on précisera.

(École polytechnique)

▷ **Solution.**

1. Une matrice est strictement stochastique si et seulement si ses coefficients sont tous strictement positifs et si le vecteur $U = {}^t(1, 1, \ldots, 1)$ est vecteur propre pour la valeur propre 1. Il en résulte que le produit de deux matrices strictement stochastiques l'est encore. Donc, pour tout $k \in \mathbb{N}^*$, A^k est strictement stochastique.

2. $\alpha_j^{(k)}$ et $\beta_j^{(k)}$ sont respectivement les plus petit et plus grand coefficients de la j-ième colonne de la matrice A^k. Comme $A^{k+1} = A \cdot A^k$, on a

$$a_{ij}^{(k+1)} = \sum_{\ell=1}^{n} a_{i\ell} a_{\ell j}^{(k)}.$$

En majorant les $a_{\ell j}^{(k)}$ par $\beta_j^{(k)}$, on obtient

$$a_{ij}^{(k+1)} \leqslant \sum_{\ell=1}^{n} a_{i\ell}\beta_j^{(k)} = \beta_j^{(k)} \underbrace{\sum_{\ell=1}^{n} a_{i\ell}}_{=1} = \beta_j^{(k)}.$$

Ceci vaut pour tout $i \in [\![1, n]\!]$, donc $\beta_j^{(k+1)} = \max_i a_{ij}^{(k+1)} \leqslant \beta_j^{(k)}$. On procède de même pour la minoration $\alpha_j^{(k)} \leqslant \alpha_j^{(k+1)}$.

Soit j fixé, i_1 un indice tel que $\beta_j^{(k+1)} = a_{i_1 j}^{(k+1)}$. On a alors

$$\begin{aligned}\beta_j^{(k)} - \beta_j^{(k+1)} &= \beta_j^{(k)} - a_{i_1 j}^{(k+1)} = \beta_j^{(k)} - \sum_{\ell=1}^{n} a_{i_1 \ell} a_{\ell j}^{(k)} \\ &= \sum_{\ell=1}^{n} a_{i_1 \ell}(\beta_j^{(k)} - a_{\ell j}^{(k)}) \geqslant \varepsilon\delta_j^{(k)},\end{aligned}$$

car tous les termes sont positifs et il existe au moins un indice ℓ tel que $a_{\ell j}^{(k)} = \alpha_j^{(k)}$ (et $a_{i_1 l} \geqslant \varepsilon$).

De même, si i_2 un indice tel que $\alpha_j^{(k+1)} = a_{i_2 j}^{(k+1)}$, on obtient

$$\alpha_j^{(k+1)} - \alpha_j^k = \sum_{\ell=1}^{n} a_{i_2\ell}(a_{\ell j}^{(k)} - \alpha_j^{(k)}) \geqslant \varepsilon\delta_j^{(k)}.$$

En additionnant les deux inégalités, il vient $\delta_j^{(k)} - \delta_j^{(k+1)} \geqslant 2\varepsilon\delta_j^{(k)}$, c'est-à-dire $\delta_j^{(k+1)} \leqslant (1-2\varepsilon)\delta_j^{(k)}$.

3. On suppose bien entendu $n \geqslant 2$, sinon le problème est trivial. Dans ce cas, on a $\varepsilon \leqslant \dfrac{1}{2}$ et $0 \leqslant 1-2\varepsilon < 1$. Pour tout j, la suite $\delta_j^{(k)}$ tend donc vers 0 lorsque k tend vers l'infini. Les suites $(\alpha_j^{(k)})_{k\geqslant 1}$ et $(\beta_j^{(k)})_{k\geqslant 1}$ sont donc adjacentes et convergent vers une même limite $\ell_j > 0$. Il résulte de la définition de $\alpha_j^{(k)}$ et $\beta_j^{(k)}$ que pour tout $(i,j) \in [\![1,n]\!]^2$, la suite $(a_{ij}^{(k)})_{k\geqslant 1}$ converge vers ℓ_j. De l'égalité $\sum\limits_{j=1}^{n} a_{ij}^{(k)} = 1$, valable pour tous $k \geqslant 1$ et $i \in [\![1,n]\!]$, on déduit que $\sum\limits_{j=1}^{n} \ell_j = 1$.

Ceci montre que la suite $(\mathrm{A}^k)_{k\geqslant 0}$ converge vers une matrice M strictement stochastique de rang 1, dont les colonnes sont toutes proportionnelles au vecteur U. En passant à la limite dans l'égalité $\mathrm{A}^{2k} = \mathrm{A}^k\mathrm{A}^k$, on obtient $\mathrm{M}^2 = \mathrm{M}$. La matrice M est la matrice d'une projection sur Vect(U). $\lhd$

L'exercice suivant donne une condition nécessaire et suffisante pour que tous les termes qui apparaissent dans le développement du déterminant soient nuls.

7.17. Théorème de Frobenius-König (1912-1916)

Soit $\mathrm{A} \in \mathcal{M}_n(\mathbb{R})$. Pour $\sigma \in \mathcal{S}_n$ on appelle serpent de A associé à σ l'ensemble $\mathrm{S}_\sigma = \{a_{1,\sigma(1)}, \ldots, a_{n,\sigma(n)}\}$.

1. Montrer qu'il y a équivalence entre :

(i) tous les serpents de A contiennent 0 ;

(ii) il existe une sous-matrice nulle de A de taille (r,s), avec $r+s = n+1$.

2. On suppose que A est à coefficients positifs et que la somme des coefficients de chaque ligne et de chaque colonne vaut 1 (on dit que A est une matrice bistochastique). Montrer que A possède un serpent ne contenant pas 0.

(École normale supérieure)

▷ **Solution.**

1. • On commence par l'implication facile $(ii) \Longrightarrow (i)$. Pour I, J parties non vides de $[\![1, n]\!]$ on note $\mathrm{A}_{\mathrm{I},\mathrm{J}}$ la matrice extraite de A obtenue en gardant les coefficients $a_{i,j}$ d'indice $(i, j) \in \mathrm{I} \times \mathrm{J}$. Par hypothèse on peut trouver I (resp. J) de cardinal r (resp. s) telles que $\mathrm{A}_{\mathrm{I},\mathrm{J}} = 0$ et $r + s = n + 1$. Soit $\sigma \in \mathcal{S}_n$. Il suffit de montrer que $\sigma(\mathrm{I}) \cap \mathrm{J} \neq \emptyset$ pour affirmer que le serpent S_σ contient 0. C'est évident, car sinon on aurait $r = |\sigma(\mathrm{I})| \leqslant |[\![1, n]\!] \backslash \mathrm{J}| = n - s$, ce qui contredit l'hypothèse $r + s = n + 1 > n$.

• Pour l'implication contraire, on raisonne par récurrence sur n. On note que si A vérifie (i), toute matrice obtenue à partir de A en permutant les lignes ou les colonnes vérifie encore (i).

Pour $n = 1$, le résultat est trivial, car A est nulle et $r = s = 1$ conviennent. Supposons le résultat vrai jusqu'au rang $n-1$ et considérons $\mathrm{A} \in \mathcal{M}_n(\mathbb{R})$ vérifiant (i). Si A est nulle, c'est terminé. On suppose donc A non nulle et quitte à effectuer une permutation des lignes et des colonnes, on peut supposer $a_{nn} \neq 0$. Notons A′ la matrice extraite $\mathrm{A}_{[\![1,n-1]\!],[\![1,n-1]\!]}$. Comme $a_{nn} \neq 0$, tous les serpents de A′ contiennent 0. Par hypothèse de récurrence, on peut trouver une sous-matrice nulle de A′ de taille (r, s) avec $r+s = n$. Ainsi, quitte à permuter de nouveau lignes et colonnes, on peut supposer que $\mathrm{A} = \left(\begin{array}{c|c} \mathrm{B} & \mathrm{C} \\ \hline 0 & \mathrm{D} \end{array}\right)$, où B est carrée de taille s et D carrée de taille r. Supposons que B admette un serpent qui ne contienne pas 0. Alors tous les serpents de D contiennent 0. Par hypothèse de récurrence, D admet une sous-matrice nulle D′ de taille (r', s') avec $r' + s' = r + 1$. La matrice extraite de A, obtenue en gardant les r' lignes correspondant aux lignes de D′ ainsi que les s premières colonnes et les s' colonnes correspondant aux colonnes de D′ est nulle et elle est de taille $(r', s+s')$, avec $r'+s+s' = r+s+1 = n+1$. Si tous les serpents de B contiennent 0, on applique l'hypothèse de récurrence à B et on conclut de même.

2. Supposons par l'absurde que tous les serpents de A contiennent 0. Il existe alors deux matrices de permutation P et Q telles que

$$\mathrm{PAQ} = \left(\begin{array}{c|c} \mathrm{B} & \mathrm{C} \\ \hline 0 & \mathrm{D} \end{array}\right) = \mathrm{A}',$$

où la matrice nulle est de taille (r, s) avec $r + s = n + 1$. Mais la matrice A′, obtenue en permutant les lignes et les colonnes de A est encore bistochastique. La somme des éléments de chaque colonne de B vaut donc 1, de même que la somme des éléments de chaque ligne de D. Mais alors la somme de tous les éléments de B et D est égale à $r + s = n + 1$ ce qui est impossible, puisque la somme des éléments de A (et donc de A′) est égale à n. ◁

Le premier résultat a été obtenu par Frobenius en 1912. En 1915, König en donne une preuve plus élémentaire à l'aide de la théorie des

graphes. Les deux mathématiciens se sont alors disputé la paternité du résultat. Le corollaire de la seconde question est dû à König. Il signifie que le permanent d'une matrice bistochastique A, *qui est défini par* $\mathrm{per}(\mathrm{A}) = \sum_{\sigma \in \mathcal{S}_n} \prod_{i=1}^{n} a_{i\sigma(i)}$ *est strictement positif. En 1916, Van der Waerden a conjecturé que le minimum du permanent sur le compact formé des matrices bistochastiques est* $\frac{n!}{n^n}$, *ce minimum n'étant atteint que pour la matrice dont tous les termes valent* $1/n$. *Ce problème est resté ouvert jusqu'en 1981 où il a été résolu indépendamment par Egorichev et Falikman. Le beau problème posé aux ENS Lyon-Cachan en 1996, en donne une preuve.*

L'énoncé suivant constitue une autre présentation de l'exercice 6.3 sur les drapeaux, qui met en évidence ce qui était sous-jacent dans celui-ci : la décomposition de Bruhat. Celle-ci s'établit à partir des opérations élémentaires sur les lignes et les colonnes utilisées dans la méthode du pivot de Gauss.

7.18. Décomposition de Bruhat et drapeaux

On pose $\mathrm{G} = \mathrm{GL}_n(\mathrm{K})$ et on note T_s le sous-groupe de G formé des matrices triangulaires supérieures inversibles. On désigne enfin par $\mathcal{D}$ l'ensemble des drapeaux de K^n.

1. Montrer, en adaptant l'algorithme du pivot de Gauss, que toute matrice $\mathrm{A} \in \mathrm{G}$ s'écrit sous la forme $\mathrm{T}_1\mathrm{P}_\sigma\mathrm{T}_2$, où T_1 et T_2 sont dans T_s et où P_σ est une matrice de permutation, c'est-à-dire $\mathrm{P}_\sigma = (\delta_{i,\sigma(j)})_{1\leqslant i,j\leqslant n}$ avec $\sigma \in \mathcal{S}_n$. Montrer que la permutation σ est définie de manière unique. La partition $\mathrm{G} = \bigcup_{\sigma\in\mathcal{S}_n} \mathrm{T}_s\mathrm{P}_\sigma\mathrm{T}_s$ de $\mathrm{GL}_n(\mathrm{K})$ ainsi obtenue, est appelé *décomposition de Bruhat.*

2. Montrer que G opère naturellement sur $\mathcal{D}$, de manière transitive (*i.e.* il n'y a qu'une orbite), et en déduire que $\mathcal{D}$ s'identifie à l'ensemble G/T_s des classes à gauche modulo T_s.

3. On considère l'action de groupe de G sur $\mathrm{G}/\mathrm{T}_s \times \mathrm{G}/\mathrm{T}_s$ définie par $\mathrm{A}\cdot(\overline{\mathrm{X}},\overline{\mathrm{Y}}) = (\overline{\mathrm{AX}},\overline{\mathrm{AY}})$. Comment cette action de groupe se traduit-elle sur les drapeaux ? Déduire de la question 1 que l'ensemble des orbites, pour l'une de ces actions, s'identifie à $\mathcal{S}_n$.

▷ **Solution.**

1. On va utiliser les matrices correspondant aux opérations élémentaires sur les lignes et les colonnes, mais en se limitant à celles qui sont dans T_s. Rappelons ce dont il s'agit. On notera $(\mathrm{E}_{ij})_{1\leqslant i,j\leqslant n}$ la base canonique de $\mathcal{M}_n(\mathrm{K})$. On appelle matrice de transvection, toute matrice

de la forme $T_{ij}(\lambda) = Id + \lambda E_{ij}$ avec $i \neq j$ et $\lambda \in K$. Multiplier une matrice A à gauche par $T_{ij}(\lambda)$ revient à rajouter à la i-ième ligne de A, la j-ième ligne multipliée par λ et multiplier A à droite par $T_{ij}(\lambda)$ revient à rajouter à la j-ième colonne, la i-ième multipliée par λ. On appelle matrice de dilatation, toute matrice de la forme $D_i(\alpha) = Id + (\alpha - 1)E_{ii}$ où α est un scalaire non nul. Multiplier A à gauche (resp. à droite) par $D_i(\alpha)$ revient à multiplier la i-ième ligne (resp. colonne) par α. Tout matrice de dilatation est triangulaire supérieure. Une matrice $T_{ij}(\lambda)$ l'est, pour $i < j$.

Soit $A \in G$. On construit un algorithme permettant de transformer A en une matrice de permutation, en la multipliant par des matrices de transvections ou de dilatations triangulaires supérieures. D'après ce qui précède, on peut ajouter à toute ligne une combinaison linéaire de lignes d'indices supérieurs et ajouter à toute colonne une combinaison linéaire de colonnes d'indices inférieurs. La première colonne de A n'est pas nulle car $A \in G$. Notons i_1 le plus grand indice k tel que $a_{k1} \neq 0$. En multipliant A par des matrices $T_{ki_1}(\lambda)$, on peut annuler tous les coefficients a_{k1} pour $k < i_1$. À l'aide d'une matrice de dilatation, on peut remplacer le coefficient en position $(i_1, 1)$ par 1 et à l'aide d'opérations sur les colonnes, on peut annuler tous les autres coefficients de la i_1-ième ligne. Notons A_1 la matrice obtenue. Comme $A_1 \in G$, sa seconde colonne n'est pas nulle. Notons i_2 le plus grand indice k tel que le coefficient en position $(k, 2)$ de A_1 soit non nul. Comme précédemment, on peut égaler ce coefficient à 1 et mettre des 0 sur la i_2-ième ligne et la deuxième colonne partout ailleurs. On vérifie que ces opérations ne modifient pas les termes de la i_1-ième ligne et de la i_1-ième colonne. On continue l'algorithme de même avec la matrice A_2 obtenue. On construit ainsi une suite injective $i_1, i_2, \ldots, i_n$ d'entiers entre 1 et n, et en notant σ la bijection qui envoie k sur i_k, la matrice A_n obtenue à la fin de l'algorithme est la matrice de permutation P_σ. La matrice A a été multiplié à gauche et à droite par un produit d'éléments de T_s, qui est encore dans T_s. En considérant l'inverse de ces matrices, qui sont dans T_s, on écrit $T_1^{-1} A T_2^{-1} = A_n = P_\sigma$, soit encore $A = T_1 P_\sigma T_2$.

Montrons que la permutation σ est définie de manière unique. Il suffit de vérifier que, si σ et σ' sont deux permutations et T et T' deux matrices de T_s, l'égalité $TP_\sigma = P_{\sigma'}T'$ impose $\sigma = \sigma'$. On remarque, pour commencer, que la matrice TP_σ s'obtient en permutant les colonnes de T (la j-ième colonne de TP_σ est la $\sigma(j)$-ième colonne de T) et que $P_{\sigma'}T'$ s'obtient en permutant les lignes de T' (la i-ième ligne de $P_{\sigma'}T'$ est la $\sigma'^{-1}(i)$-ième ligne de T'). Pour tout indice j, les coefficients d'indice (i, j) de TP_σ sont donc nuls pour $i > \sigma(j)$. Le coefficient d'indice $(\sigma'(j), j)$ de $P_{\sigma'}T'$, c'est-à-dire le coefficient d'indice (j, j) de T' n'est pas nul,

car la matrice T' est triangulaire supérieure et inversible. On en déduit que $\sigma'(j) \leqslant \sigma(j)$. Par symétrie, on a, de même, $\sigma'(j) \leqslant \sigma(j)$. On obtient finalement $\sigma = \sigma'$.

Conclusion. On a obtenu $GL_n(K) = \bigcup_{\sigma \in \mathcal{S}_n} T_s P_\sigma T_s$ où la réunion est disjointe, ce qui constitue la décomposition de Bruhat.

2. Si $A \in G$ et si $d = (F_0, F_1, \ldots, F_n)$ est un drapeau, alors $A \cdot d = (A(F_0), A(F_1), \ldots, A(F_n))$ est également un drapeau, puisque l'image par A d'un sous-espace vectoriel est un sous-espace de même dimension. Il est clair que cela définit une opération du groupe G sur l'ensemble $\mathcal{D}$ des drapeaux. Montrons que cette opération est transitive. Soit $(e_1, \ldots, e_n)$ la base canonique de K^n et δ le drapeau formé des sous-espaces $\mathrm{Vect}(e_1, \ldots, e_k)$, $0 \leqslant k \leqslant n$. Soit $d = (F_0, F_1, \ldots, F_n)$ un drapeau quelconque. On peut clairement trouver une base $(f_1, \ldots, f_n)$ de K^n telle que pour tout $k \in [\![1, n]\!]$, $(f_1, f_2, \ldots, f_k)$ soit une base de F_k. L'unique matrice A vérifiant $A(e_i) = f_i$ pour tout i, est inversible et vérifie $A \cdot \delta = d$. L'opération de G sur $\mathcal{D}$ est donc transitive, et $\mathcal{D}$ est alors en bijection avec G/G_δ, où G_δ est le stabilisateur du drapeau δ. Or il est clair que pour $A \in G$, $A \cdot \delta = \delta$ si et seulement si A est triangulaire supérieure. On a donc $G_\delta = T_s$ et $\mathcal{D}$ est en bijection avec G/T_s.

3. Si d est un drapeau, on considère, avec les notations de la question 2, B dans G tel que $d = B \cdot \delta$. On identifie d avec l'élément $\overline{B}$ de G/T_s. Si A est un élément de G, on a $A \cdot \overline{B} = \overline{AB}$ qui s'identifie à $AB \cdot \delta = A \cdot d$. L'action de G sur $G/T_s \times G/T_s$ se traduit donc, sur les couples de drapeaux, par l'action naturelle $A \cdot (d, d') = (A \cdot d, A \cdot d')$, où l'action de G sur les drapeaux est celle qui est décrite dans la question précédente.

Si X et Y sont dans G, on peut écrire $(\overline{X}, \overline{Y}) = X(\overline{I_n}, \overline{X^{-1}Y})$. En décomposant $X^{-1}Y$ en $T_1 P_\sigma T_2$, comme dans la question 1, on obtient

$$(\overline{I_n}, \overline{X^{-1}Y}) = T_1(\overline{T_1^{-1}}, \overline{P_\sigma T_2}) = T_1(\overline{I_n}, \overline{P_\sigma}),$$

car T_1 et T_2 sont éléments de T_s, et finalement $(\overline{X}, \overline{Y}) = XT_1(\overline{I_n}, \overline{P_\sigma})$. Toute orbite contient donc un élément de la forme $(\overline{I_n}, \overline{P_\sigma})$. La permutation σ est définie de manière unique, car s'il existe $A \in G$ tel que $(\overline{I_n}, \overline{P_\sigma}) = A(\overline{I_n}, \overline{P_{\sigma'}}) = (\overline{A}, \overline{AP_{\sigma'}})$, alors A est dans T_s et il existe $T \in T_s$ tel que $AP_{\sigma'} = P_\sigma T$. D'après la question 1, ceci implique $\sigma = \sigma'$. On obtient ainsi une bijection de l'ensemble des orbites sur $\mathcal{S}_n$. $\lhd$

On retrouve ainsi le résultat de l'exercice 6.3 : le nombre de classe de $D \times D$ *sous l'action de* $GL_n(K)$ *est* $n!$.

Lorsque que le corps K *est* $\mathbb{R}$, *le cas le plus probable est celui où le plus grand coefficient non nul de la* k*-ième colonne de* A_{k-1} *est toujours sur la* $(n+1-k)$*-ième ligne. On obtient alors la permutation* $\tau : k \longmapsto n+1-k$. *On peut effectivement démontrer que l'orbite de* P_τ *est la plus grande :*

elle est ouverte et dense dans G *de sorte que les autres orbites sont d'intérieur vide*[2].

On termine le chapitre avec une série d'exercices sur les matrices à coefficients dans $\mathbb{Z}$. *Pour les lois usuelles,* $\mathcal{M}_n(\mathbb{Z})$ *est muni d'une structure d'anneau. On note* $\mathrm{GL}_n(\mathbb{Z})$ *le groupe des inversibles de cet anneau.*

• *Si* $\mathrm{M} \in \mathrm{GL}_n(\mathbb{Z})$, *il existe* $\mathrm{N} \in \mathcal{M}_n(\mathbb{Z})$ *telle que* $\mathrm{MN} = \mathrm{NM} = \mathrm{I}_n$. *En passant au déterminant, on a* $\det \mathrm{M} \det \mathrm{N} = 1$. *Donc* $\det \mathrm{M}$ *est inversible dans* $\mathbb{Z}$ *et, par conséquent,* $\det \mathrm{M} = \pm 1$.

• *Réciproquement, supposons que* $\det \mathrm{M} = \varepsilon = \pm 1$. *Notons* N *la transposée de la comatrice de* M. *C'est une matrice à coefficients entiers. L'égalité* $\mathrm{MN} = \mathrm{NM} = \det \mathrm{M}\, \mathrm{I}_n = \varepsilon \mathrm{I}_n$ *montre que la matrice* $\varepsilon \mathrm{N}$, *qui appartient à* $\mathcal{M}_n(\mathbb{Z})$, *est l'inverse de* M. *On conclut que*

$$\boxed{\mathrm{M} \in \mathrm{GL}_n(\mathbb{Z}) \iff \det \mathrm{M} = \pm 1}.$$

7.19. Bases d'un groupe abélien

Étant donné un groupe abélien G, on dit que $(e_1, \ldots, e_n) \in \mathrm{G}^n$ est une base de G si tout élément x de G s'écrit de manière unique

$$x = k_1 e_1 + k_2 e_2 + \cdots + k_n e_n, \text{ où } (k_1, k_2, \ldots, k_n) \in \mathbb{Z}^n.$$

Soit G un groupe abélien, possédant une base $(e_1, \ldots, e_n)$.

1. Si $(\varepsilon_1, \ldots, \varepsilon_m)$ est une famille de m éléments de G, on écrit pour $1 \leqslant j \leqslant p$, $\varepsilon_j = \sum_{i=1}^{n} k_{ij} e_i$, avec les k_{ij} dans $\mathbb{Z}$.

Montrer que $(\varepsilon_1, \ldots, \varepsilon_m)$ est une base de G si, et seulement si, $m = n$ et la matrice $\mathrm{P} = (k_{ij})_{1 \leqslant i,j \leqslant n}$ est dans $\mathrm{GL}_n(\mathbb{Z})$.

2. On considère un sous-groupe G′ de G. Montrer que G′ admet une base de cardinal $r \leqslant n$.

(École polytechnique)

▷ **Solution.**

1. • Supposons que $(\varepsilon_1, \ldots, \varepsilon_m)$ est une base de G. Pour $1 \leqslant p \leqslant m$, on peut écrire $e_p = \sum_{i=1}^{m} \ell_{ip} \varepsilon_i$, où les ℓ_{ip} sont dans $\mathbb{Z}$. On a alors

2. Le lecteur intéressé pourra se reporter à MNEIMNÉ (R.), TESTARD (F.), *Groupes de Lie classiques*, Hermann, 1986, p. 48-49.

$$(*) \qquad e_p = \sum_{i=1}^{m} \ell_{ip}\Big(\sum_{j=1}^{n} k_{ji}e_j\Big) = \sum_{j=1}^{n}\Big(\sum_{i=1}^{m} k_{ji}\ell_{ip}\Big)e_j$$

et, par unicité de l'écriture, $\sum\limits_{i=1}^{n} k_{ji}\ell_{ip} = \delta_{jp}$. En considérant les matrices $\mathrm{P} = (k_{ij})_{\substack{1\leqslant i\leqslant n\\ 1\leqslant j\leqslant m}} \in \mathcal{M}_{n,m}(\mathbb{Z})$ et $\mathrm{Q} = (\ell_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathcal{M}_{m,n}(\mathbb{Z})$, on obtient $\mathrm{PQ} = \mathrm{I}_n$. On en déduit, en considérant les rangs des matrices en tant que matrices à coefficients dans $\mathbb{Q}$, que $n = \operatorname{rg}\mathrm{I}_n \leqslant \operatorname{rg}\mathrm{P} \leqslant m$. Les deux bases jouant des rôles symétriques, on a, de même, $n \geqslant m$ et donc $m = n$. Les matrices P et Q sont donc carrées de taille n et l'égalité $\mathrm{PQ} = \mathrm{I}_n$ implique que P appartient à $\mathrm{GL}_n(\mathbb{Z})$.

• Réciproquement, supposons que $m = n$ et que P est dans $\mathrm{GL}_n(\mathbb{Z})$; notons son inverse $\mathrm{Q} = (\ell_{ij})_{1\leqslant i,j\leqslant n}$. Le calcul $(*)$ du sens direct montre que $e_p = \sum\limits_{i=1}^{n} \ell_{ip}\varepsilon_i$ pour tout $1 \leqslant p \leqslant n$. Il s'ensuit que les e_p sont dans le sous-groupe engendré par les ε_i. Puisque les e_p engendrent G, $(\varepsilon_1, \ldots, \varepsilon_n)$ est un système générateur de G. Il reste à montrer l'unicité de l'écriture de tout $x \in \mathrm{G}$ comme combinaison linéaire à coefficients entiers des ε_i. Clairement, il suffit de le vérifier pour 0. Soit $(k_1, \ldots, k_n) \in \mathbb{Z}^n$ tel que $k_1\varepsilon_1 + \cdots + k_n\varepsilon_n = 0$. On a alors

$$0 = \sum_{i=1}^{n} k_i\Big(\sum_{j=1}^{n} k_{ji}e_j\Big) = \sum_{j=1}^{n}\Big(\sum_{i=1}^{n} k_i k_{ji}\Big)e_j,$$

d'où pour tout $1 \leqslant i \leqslant n$, $\sum\limits_{i=1}^{n} k_{ji}k_i = 0$ et comme ce système dont les inconnues sont les k_i, est de Cramer (la matrice des k_{ij} est inversible dans $\mathcal{M}_n(\mathbb{Q})$), les k_i sont tous nuls.

2. On suppose que $\mathrm{G}' \neq \{0\}$, sinon la famille vide convient, et on raisonne par récurrence sur n.

• Traitons le cas $n = 1$. L'application $\varphi : x \in \mathbb{Z} \longmapsto xe_1 \in \mathrm{G}$ est un isomorphisme de groupes, donc $\varphi^{-1}(\mathrm{G}')$ est un sous-groupe de $\mathbb{Z}$, qui s'écrit $a\mathbb{Z}$ avec $a > 0$. Tout élément de G' s'écrit de manière unique kae_1, avec $k \in \mathbb{Z}$ et (ae_1) est une base de G'.

• Supposons que $n \geqslant 2$ et que la propriété est vérifiée au rang $n-1$. Soit G' un sous-groupe de G, groupe qui possède une base de n vecteurs $(e_1, \ldots, e_n)$. Considérons $\mathrm{G}_1 = \sum\limits_{i=1}^{n-1} \mathbb{Z}e_i$ et $\mathrm{G}'_1 = \mathrm{G}_1 \cap \mathrm{G}'$. Alors G'_1 est un sous-groupe de G_1, groupe qui possède une base de $n-1$ vecteurs. Par hypothèse de récurrence, G'_1 possède une base $(e'_1, \ldots, e'_{r-1})$ $(1 \leqslant r \leqslant n)$.

Si $\mathrm{G}'_1 = \mathrm{G}'$, c'est-à-dire si $\mathrm{G}' \subset \mathrm{G}_1$, la démonstration est achevée, sinon on considère le morphisme de groupes $\nu : \mathrm{G} \longmapsto \mathbb{Z}$ défini par $\nu\Big(\sum\limits_{i=1}^{n} k_ie_i\Big) = k_n$ et on étudie $\nu(\mathrm{G}')$. C'est un sous-groupe de $\mathbb{Z}$,

non réduit à $\{0\}$, qui s'écrit donc $a\mathbb{Z}$, avec $a > 0$. Il existe $e'_r \in G'$ tel que $\nu(e'_r) = a$.

Montrons que $(e'_1, \ldots, e'_r)$ est une base de G'.

$\star$ Supposons que $k_1 e'_1 + \cdots + k_r e'_r = 0$, avec les k_i dans $\mathbb{Z}$. On a alors

$$0 = \nu(0) = k_1 \nu(e'_1) + k_2 \nu(e'_2) + \cdots + k_r \nu(e'_r) = k_r a,$$

d'où l'on tire $k_r = 0$ et l'égalité $k_1 e'_1 + \cdots + k_{r-1} e'_{r-1} = 0$. Comme $(e'_1, \ldots, e'_{r-1})$ est une base de G'_1, on a $k_1 = \cdots = k_{r-1} = 0$.

$\star$ Si $x \in G'$, alors $\nu(x)$ appartient à $a\mathbb{Z}$ et il existe $k_r \in \mathbb{Z}$ tel que $\nu(x) = k_r a = \nu(k_r e'_r)$. On en déduit que $x - k_r e'_r \in G'_1$: il existe $k_1, \ldots, k_{r-1}$ dans $\mathbb{Z}$ tels que $x - k_r e'_r = k_1 e'_1 + \cdots k_{r-1} e'_{r-1}$. On obtient donc $x = k_1 e'_1 + \cdots + k_r e'_r$.

On conclut que $(e'_1, \ldots, e'_r)$ est une base du sous-groupe G' de G, avec $r \leqslant n$. $\lhd$

Un groupe abélien possédant une base de cardinal fini est dit libre de type fini. *Le cardinal n d'une base quelconque est appelé* rang *du groupe. Un tel groupe est isomorphe à $\mathbb{Z}^n$. La question 1 de l'exercice montre, en particulier, que si $\mathbb{Z}^m$ est isomorphe à $\mathbb{Z}^n$, alors $m = n$. La question 2 démontre qu'un sous-groupe d'un groupe libre de type fini est libre de type fini. En particulier, tout sous-groupe de $\mathbb{Z}^n$ possède une base comportant moins de n vecteurs.*

On cherche dans l'exercice suivant à décrire les vecteurs-colonnes qui peuvent figurer dans une matrice de $\mathrm{GL}_n(\mathbb{Z})$. Quitte à échanger deux colonnes, on peut se limiter à la première. Au vu de l'exercice précédent, le problème s'interprète comme suit : à quelle condition un vecteur de $\mathbb{Z}^n$ peut-il être complété en une base de $\mathbb{Z}^n$ (au sens défini dans l'exercice précédent) ? Une autre solution de ce problème sera donnée dans le chapitre sur le déterminant du tome 2 d'algèbre.

7.20. Première colonne d'une matrice inversible de $\mathcal{M}_n(\mathbb{Z})$

1. Soit $u = (u_1, \ldots, u_n) \in \mathbb{Z}^n$ et

$$\begin{array}{rcl} \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \\ \tilde{u} : (x_1, \ldots, x_n) & \longmapsto & \displaystyle\sum_{i=1}^{n} u_i x_i. \end{array}$$

On suppose qu'il existe $x \in \mathbb{Z}^n$ tel que $\tilde{u}(x) = 1$. Démontrer que $\mathbb{Z}^n = \mathbb{Z}x \oplus \operatorname{Ker} \tilde{u}$.

2. Prouver que $x \in \mathbb{Z}^n$ est la première colonne d'une matrice inversible de $\mathcal{M}_n(\mathbb{Z})$ si, et seulement si, ses composantes sont des nombres premiers entre eux.

(**École polytechnique**)

▷ **Solution.**

1. Il faut préciser la notation $\oplus$ puisqu'il ne s'agit plus de la somme directe de sous-espaces vectoriels. Si G est un groupe abélien et si $\mathrm{H}_1, \ldots, \mathrm{H}_k$ des sous-groupes de G, on écrira $\mathrm{G} = \mathrm{H}_1 \oplus \cdots \oplus \mathrm{H}_k$ si tout élément g de G s'écrit de manière unique sous la forme $g = h_1 + \cdots + h_k$ avec $(h_1, \ldots, h_k) \in \mathrm{H}_1 \times \cdots \times \mathrm{H}_k$. On remarque qu'il suffit de vérifier l'unicité pour 0.

Soit donc $x \in \mathbb{Z}^n$ tel que $\tilde{u}(x) = 1$. Pour $y \in \mathbb{Z}^n$, considérons $k = \tilde{u}(y)$ et $z = y - kx$. Comme $\tilde{u}$ est visiblement un morphisme du groupe $\mathbb{Z}^n$ dans $\mathbb{Z}$, on obtient

$$\tilde{u}(z) = \tilde{u}(y) - k\tilde{u}(x) = k - k = 0 \quad \text{et} \quad z \in \operatorname{Ker} \tilde{u}.$$

Par conséquent, $y = kx + z \in \mathbb{Z}x + \operatorname{Ker} \tilde{u}$.

Si $kx + z = 0$ avec $z \in \operatorname{Ker} \tilde{u}$ et $k \in \mathbb{Z}$, on obtient, en prenant l'image par $\tilde{u}$,

$$0 = k\tilde{u}(x) + \tilde{u}(z) = k + 0 = k \quad \text{et} \quad z = 0.$$

On conclut que

$$\boxed{\mathbb{Z}^n = \mathbb{Z}x \oplus \operatorname{Ker} \tilde{u}}.$$

2. • La condition proposée est nécessaire. En effet, soit $\mathrm{M} \in \mathrm{GL}(\mathbb{Z})$ et $(\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n)$ ses colonnes. Soit d le pgcd des coefficients de la première colonne. On a

$$\det \mathrm{M} = \pm 1 = \det(\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n) = d \det \underbrace{\left(\frac{1}{d}\mathrm{C}_1, \mathrm{C}_2, \ldots, \mathrm{C}_n\right)}_{\subset \mathcal{M}_n(\mathbb{Z})} \in d\mathbb{Z},$$

donc d est nécessairement égal à 1. Les composantes de C_1 sont donc des nombres premiers entre eux.

• Inversement, soit $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ dont les composantes sont des nombres premiers eux. D'après l'identité de Bezout, il existe $(u_1, \ldots, u_n) \in \mathbb{Z}^n$ tel que

$$1 = u_1 x_1 + \cdots + u_n x_n.$$

Notons $\tilde{u}$ l'application

$$(y_1, \ldots, y_n) \in \mathbb{Z}^n \longmapsto \sum_{i=1}^{n} u_i y_i \in \mathbb{Z}.$$

Par construction, on a $\tilde{u}(x) = 1$. De la question précédente, on déduit donc $\mathbb{Z}^n = \mathbb{Z}x \oplus \operatorname{Ker} \tilde{u}$. Puisque $\operatorname{Ker} \tilde{u}$ est un sous-groupe de $\mathbb{Z}^n$, il existe, d'après l'exercice précédent, $\varepsilon_2, \ldots, \varepsilon_r$ dans $\mathbb{Z}^n$, tels que

$$\operatorname{Ker} \tilde{u} = \mathbb{Z}\varepsilon_2 \oplus \cdots \oplus \mathbb{Z}\varepsilon_r \quad \text{et donc} \quad \mathbb{Z}^n = \mathbb{Z}x \oplus \mathbb{Z}\varepsilon_2 \oplus \cdots \oplus \mathbb{Z}\varepsilon_r$$

On vérifie alors facilement que $(x, \varepsilon_2, \ldots, \varepsilon_r)$ est une base de $\mathbb{Z}^n$. On a donc forcément $r = n$ et la matrice de cette famille dans la base canonique de $\mathbb{Z}^n$ est dans $\mathrm{GL}_n(\mathbb{Z})$. Sa première colonne contenant le vecteur x, on a le résultat souhaité. $\lhd$

Intéressons-nous à la notion de matrices équivalentes dans $\mathcal{M}_n(\mathbb{Z})$. Comme dans $\mathcal{M}_n(\mathrm{K})$, deux matrices A et B de $\mathcal{M}_n(\mathbb{Z})$ sont dites équivalentes s'il existe deux matrices P et Q de $\mathrm{GL}_n(\mathbb{Z})$ telles que $\mathrm{B} = \mathrm{PAQ}$. *C'est une relation d'équivalence. Les classes d'équivalence dans $\mathcal{M}_n(\mathbb{Z})$ ne sont plus paramétrées par un seul entier (le rang), comme dans $\mathcal{M}_n(\mathrm{K})$, mais par une suite finie d'entiers. L'outil essentiel de l'exercice suivant est l'algorithme du pivot de Gauss.*

7.21. Matrices équivalentes dans $\mathcal{M}_n(\mathbb{Z})$

On note G le sous-groupe de $\mathrm{GL}_n(\mathbb{Z})$ engendré par les matrices de la forme $\mathrm{I} - 2\mathrm{E}_{ii}$ et $\mathrm{I} + a\mathrm{E}_{ij}$ pour tout $1 \leqslant i, j \leqslant n$, $i \neq j$ et $a \in \mathbb{Z}$.

On envisage la relation $\mathcal{R}$ dans $\mathcal{M}_n(\mathbb{Z})$, définie pour A et B dans $\mathcal{M}_n(\mathbb{Z})$ par

$$\mathrm{A}\mathcal{R}\mathrm{B} \iff \exists (\mathrm{P}, \mathrm{Q}) \in \mathrm{G}^2,\ \mathrm{A} = \mathrm{PBQ}.$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.

Pour $\mathrm{A} = (a_{ij})_{1 \leqslant i,j \leqslant n} \in \mathcal{M}_n(\mathbb{Z})$ non nulle, on note

$$d(\mathrm{A}) = \min\{|a_{ij}|, 1 \leqslant i, j \leqslant n,\ a_{ij} \neq 0\}.$$

2. Montrer qu'il existe dans la classe d'équivalence de A une matrice $\mathrm{N} = (n_{ij})_{1 \leqslant i,j \leqslant n}$ telle que $d(\mathrm{N})$ soit minimal dans cette classe et $d(\mathrm{N}) = n_{11}$.

Montrer que n_{11} divise les n_{1j}, puis qu'il divise les n_{ij}.

3. Montrer que l'on peut trouver N de la forme

$$\mathrm{N} = \mathrm{Diag}(n_{11}, k_1 n_{11}, k_1 k_2 n_{11}, \ldots, k_1 \cdots k_{n-1} n_{11}),$$

où les k_i sont dans $\mathbb{N}$.

4. Déduire de ce qui précède que $\mathrm{G} = \mathrm{GL}_n(\mathbb{Z})$.

(École polytechnique)

$\rhd$ **Solution.**

1. Soit A, B et C dans $\mathcal{M}_n(\mathbb{Z})$.

Comme $\mathrm{I} \in \mathrm{G}$, car G est un sous-groupe, et que $\mathrm{A} = \mathrm{IAI}$, on a $\mathrm{A}\mathcal{R}\mathrm{A}$: la relation $\mathcal{R}$ est réflexive.

Supposons $\mathrm{A}\mathcal{R}\mathrm{B}$. Il existe alors P et Q dans G tels que $\mathrm{A} = \mathrm{PBQ}$.

Mais alors, on a $B = P^{-1}AQ^{-1}$, où P^{-1} et Q^{-1} sont dans G : $\mathcal{R}$ est symétrique.

Supposons $A\mathcal{R}B$ et $B\mathcal{R}C$. Il existe donc P, Q, R et S dans G tels que $A = PBQ$ et $B = RCS$. On en déduit que $A = (PR)C(SQ)$ et $A\mathcal{R}C$, puisque PR et SQ sont dans G. La relation est transitive. C'est donc une relation d'équivalence.

2. • Notons $T_{ij}(a) = I + aE_{ij}$ pour $1 \leqslant i \neq j \leqslant n$ et $a \in \mathbb{Z}$. Il s'agit là d'une matrice de transvection. Rappelons rapidement l'effet de la multiplication par $T_{ij}(a)$: si $M \in \mathcal{M}_n(\mathbb{Z})$ est de colonnes $(C_1, \ldots, C_n)$ et de lignes $(L_1, \ldots, L_n)$, la matrice $T_{ij}(a)M$ est la transformée de M par l'opération élémentaire $L_i \leftarrow L_i + aL_j$. De même, la matrice $MT_{ij}(a)$ est la transformée de M par l'opération élémentaire $C_j \leftarrow C_j + aC_i$. La multiplication à gauche par $I - 2E_{ii}$ correspond à $L_i \leftarrow -L_i$, et la multiplication à droite à $C_i \leftarrow -C_i$.

Il est possible de trouver dans G une matrice réalisant la permutation de deux lignes ou deux colonnes. En effet, le lecteur vérifiera aisément que la matrice $(I - 2E_{ii})T_{ij}(-1)T_{ji}(1)T_{ij}(-1) \in G$ $(1 \leqslant i, j \leqslant n,\ i \neq j)$ effectue, par multiplication à gauche, l'opération élémentaire $L_i \leftrightarrow L_j$. De même, $T_{ji}(-1)T_{ij}(1)T_{ij}(-1)(I - 2E_{ii}) \in G$ effectue par multiplication à droite l'opération $C_i \leftrightarrow C_j$. Comme les transpositions engendrent le groupe symétrique, G contient donc toutes les matrices de permutation.

Il en résulte que dans la classe d'équivalence de $A \in GL_n(\mathbb{Z})$, on trouve toutes les matrices obtenues à partir de A par une succession d'opérations élémentaires sur les lignes et les colonnes telles que nous venons de les décrire.

• On remarque que si A est en relation avec B, alors $B \neq 0$ et $d(B)$ est donc défini. L'ensemble des $d(B)$, pour B décrivant la classe d'équivalence de A, est une partie non vide de $\mathbb{N}^*$. Elle admet donc un plus petit élément. Prenons $N = (n_{ij})_{1 \leqslant i,j \leqslant n}$ dans la classe de A telle que $d(N)$ soit ce plus petit élément.

Soit $(i_0, j_0) \in [\![1, n]\!]$ tel que $|n_{i_0 j_0}| = d(N)$. Quitte à effectuer l'opération élémentaire $L_{i_0} \leftrightarrow L_1$, on peut supposer $i_0 = 1$: on reste bien dans la classe de A et $d(N)$ est inchangé. Quitte à effectuer l'opération $C_{j_0} \leftrightarrow C_1$, on peut également supposer que $j_0 = 1$. Enfin, quitte à effectuer l'opération $C_1 \leftarrow -C_1$, on peut supposer $n_{11} > 0$. On a donc trouvé N dans la classe de A telle que $d(N)$ soit minimal avec $d(N) = n_{11}$.

• Soit $2 \leqslant j \leqslant n$. Opérons la division euclidienne de n_{1j} par n_{11}. Il existe $q \in \mathbb{Z}$ et $0 \leqslant r \leqslant n_{11} - 1$ tels que $n_{1j} = n_{11}q + r$. Effectuons l'opération élémentaire, $C_j \leftarrow C_j - qC_1$. Le coefficient d'indice $(1, j)$ de la matrice obtenue, toujours équivalente à A, est r. Comme $r < d(N)$ la minimalité de $d(N)$ impose $r = 0$. Donc $n_{11} | n_{1j}$.

On montre de même en agissant sur les lignes que n_{11} divise les n_{i1}.

• En effectuant pour chaque $2 \leqslant j \leqslant n$, l'opération $C_j - q_j C_1$ où q_j est le quotient de n_{1j} par n_{11}, on trouve dans la classe de A une nouvelle matrice $N' = (n'_{ij})_{1 \leqslant i,j \leqslant n}$, avec $n'_{11} = n_{11}$, les $n'_{1j} = 0$, $n'_{i1} = n_{i1}$ et $n'_{ij} = n_{ij} - q_j n_{i1} \equiv n_{ij} \pmod{n_{11}}$ pour $2 \leqslant i, j \leqslant n$.

Soit $2 \leqslant i, j \leqslant n$. On effectue sur la matrice N' l'opération élémentaire $C_1 \leftarrow C_1 + C_j$. On obtient alors une nouvelle matrice $N'' = (n''_{ij})_{1 \leqslant i,j \leqslant n}$ dans la classe de A, avec toujours $n''_{11} = n_{11} = d(N)$.

Ce qui était valable pour N le reste pour N'' : n_{11} divise encore les $n''_{i1} = n_{i1} + n'_{ij} \equiv n'_{ij} \equiv n_{ij} \pmod{n_{11}}$. Autrement dit, n_{11} divise n_{ij}.

3. À partir de la matrice N construite à la question 2, on construit une matrice équivalente telle que $n_{i1} = 0$ si $i \geqslant 2$ et $n_{1j} = 0$ si $j \geqslant 2$. Pour cela, on effectue, pour $i \geqslant 2$, les opérations élémentaires $L_i \leftarrow L_i - \dfrac{n_{i1}}{n_{11}} L_1$, ce qui amène des 0 sur les termes de la première colonne, sauf le premier, puis, pour $j \geqslant 2$, les opérations élémentaires $C_j \leftarrow C_j - \dfrac{n_{j1}}{n_{11}} C_1$, ce qui amène des 0 sur les termes de la première ligne, sauf le premier (sans toucher à la première colonne). Ceci est possible, car tous les termes de la matrice sont divisibles par n_{11} et le restent après chacune de ces transformations. D'après ce qui précède, on peut donc trouver dans la classe de A une matrice que nous noterons encore N du type

$$N = \begin{pmatrix} n_{11} & 0 \ \dots \ 0 \\ 0 & \\ \vdots & \boxed{n_{11} A'} \\ 0 & \end{pmatrix}.$$

Il est naturel de procéder par récurrence sur n, pour démontrer le résultat demandé. La propriété est évidente si $n = 1$. On suppose qu'elle est vérifiée au rang $n - 1$ et on la démontre pour une matrice de taille n.

• Si $A' = 0$, on prend simplement $k_i = 0$ pour tout $1 \leqslant i \leqslant n - 1$.

• Si $A' \neq 0$, d'après l'hypothèse de récurrence, il existe des matrices P et Q de taille $n - 1$ qui sont produits de matrices de taille $n - 1$ du type $I - 2E_{ii}$, $T_{ij}(a)$ ou de leur inverse et $k_1, \dots, k_n$ dans N tels que $PA'Q = N'$ où $N' = \mathrm{Diag}(k_1, k_1 k_2, \dots, k_1 \dots k_{n-1})$. Comme on a $(I - 2E_{ii})^{-1} = I - 2E_{ii}$ et $T_{ij}(a)^{-1} = T_{ij}(-a)$, la matrice P est produit de matrices de taille $n - 1$ du type $I - 2E_{ii}$ ou $T_{ij}(a)$. Si $M = I - 2E_{ii}$ ou $M = T_{ij}(a)$, la matrice

$$\begin{pmatrix} 1 & 0 \ \dots \ 0 \\ 0 & \\ \vdots & \boxed{M} \\ 0 & \end{pmatrix}$$

est une matrice de taille n faisant partie des générateurs de G décrit par l'énoncé. Il s'ensuit que, d'après la règle de multiplication des matrices

par blocs, la matrice $\mathrm{P}' = \begin{pmatrix} 1 & 0 \ \dots \ 0 \\ 0 & \\ \vdots & \boxed{\mathrm{P}} \\ 0 & \end{pmatrix}$ est dans G. De même, $\mathrm{Q}' = \begin{pmatrix} 1 & 0 \ \dots \ 0 \\ 0 & \\ \vdots & \boxed{\mathrm{Q}} \\ 0 & \end{pmatrix}$ est dans G. Il en résulte que $\mathrm{P}'\mathrm{N}\mathrm{Q}'$ est encore dans la classe de A. Ainsi, on a

$$\mathrm{P}'\mathrm{N}\mathrm{Q}' = \begin{pmatrix} n_{11} & 0 \ \dots \ 0 \\ 0 & \\ \vdots & \boxed{n_{11}\mathrm{P}\mathrm{A}'\mathrm{Q}} \\ 0 & \end{pmatrix} = \begin{pmatrix} n_{11} & 0 \ \dots \ 0 \\ 0 & \\ \vdots & \boxed{n_{11}\mathrm{N}'} \\ 0 & \end{pmatrix}$$
$$= \mathrm{Diag}(n_{11}, k_1 n_{11}, k_1 k_2 n_{11}, \dots, k_1 \dots k_{n-1} n_{11}).$$

C'est le résultat recherché.

4. On garde les notations de la question précédente. Si on prend $\mathrm{A} \in \mathrm{GL}_n(\mathbb{Z})$, alors $\mathrm{N} \in \mathrm{GL}_n(\mathbb{Z})$ et $\det \mathrm{N} = \pm 1$. Les coefficients n_{11} et les k_i sont forcément égaux à 1. La matrice A est donc équivalente à I_n et $\mathrm{A} \in \mathrm{G}$. On conclut que $\boxed{\mathrm{G} = \mathrm{GL}_n(\mathbb{Z})}$. $\lhd$

Puisque G *est égal à* $\mathrm{GL}_n(\mathbb{Z})$, *la relation* $\mathcal{R}$ *coïncide avec la notion de matrices équivalentes dans* $\mathcal{M}_n(\mathbb{Z})$. *La question 2 de l'exercice démontre que toute matrice est équivalente à une matrice de la forme* $\mathrm{Diag}(d_1, d_2, \dots, d_n)$, *où* $d_1, \dots, d_n$ *sont des entiers naturels tels que* $d_1 | d_2 | \cdots | d_n$. *Signalons qu'on a le résultat d'unicité suivant : soit* $(d_i)_{1 \leqslant i \leqslant n}$, $(d'_i)_{1 \leqslant i \leqslant n}$ *deux suites d'entiers naturels telles que* $d_1 | d_2 | \cdots | d_n$ *et* $d'_1 | d'_2 | \cdots | d'_n$. *Si les matrices* $\mathrm{Diag}(d_1, d_2, \dots, d_n)$ *et* $\mathrm{Diag}(d'_1, \dots, d'_n)$ *sont équivalentes, alors* $d_i = d'_i$ *pour tout* i. *Autrement dit, une classe d'équivalence est paramétrée par une suite de* n *entiers naturels* $(d_i)_{1 \leqslant i \leqslant n}$ *telle que* $d_1 | d_2 | \cdots | d_n$.

Le lecteur est invité à regarder comment ce résultat se généralise aux matrices à coefficients dans un anneau principal quelconque.

Pour terminer, on peut noter que l'exercice a aussi prouvé que l'ensemble formé des matrices de transvections $\mathrm{T}_{ij}(a)$ *à coefficients entiers et des matrices* $\mathrm{I} - 2\mathrm{E}_{ii}$, *qui sont des matrices de symétries hyperplanes, engendre le groupe* $\mathrm{GL}_n(\mathbb{Z})$. *On se reportera au chapitre sur le groupe linéaire, dans le tome 2 d'algèbre, pour des compléments et des utilisations de ce résultat.*

On peut donner de l'exercice précédent une belle application : la classification des groupes abéliens finis. Cet exercice complète l'exercice 2.20

du chapitre sur les groupes, qui étudiait l'unicité de la décomposition en produit de groupes cycliques. On suppose connus les définitions et résultats de l'exercice 7.19.

7.22. Structure des groupes abéliens finis

On rappelle le résultat établi à l'exercice précédent : pour toute matrice A de $\mathcal{M}_n(\mathbb{Z})$, il existe P et Q dans $\mathrm{GL}_n(\mathbb{Z})$ et un n-uplet $(d_1, \ldots, d_n) \in \mathbb{N}^n$ tels que

$$d_1|d_2|\cdots|d_n \quad \text{et} \quad \mathrm{PAQ} = \mathrm{Diag}(d_1, d_2, \ldots, d_n).$$

1. Soit G un sous-groupe de $\mathbb{Z}^n$. Montrer qu'il existe une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de $\mathbb{Z}^n$, un entier $r \geqslant 0$ et $(d_1, \ldots, d_r) \in (\mathbb{N}^*)^r$, vérifiant $d_1|d_2|\cdots|d_r$ et tels que $(d_1\varepsilon_1, d_2\varepsilon_2, \ldots, d_r\varepsilon_r)$ soit une base de G.

2. On considère un groupe abélien fini H. Montrer qu'il existe un entier $r \geqslant 0$ et des entiers $d_1, \ldots, d_r$, supérieurs à 2, avec $d_1|d_2|\cdots|d_r$ tels que

$$\mathrm{H} \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_r\mathbb{Z}.$$

▷ **Solution.**

1. D'après l'exercice 7.19, il existe $r \geqslant 0$ et une base $(e_1, \ldots, e_r)$ de G. Considérons la matrice A de $\mathcal{M}_n(\mathbb{Z})$ dont les vecteurs colonnes sont $e_1, \ldots, e_r, 0, \ldots, 0$. Le rang de A, vue comme matrice à coefficients rationnels, est r, car ses r premières colonnes sont $\mathbb{Z}$-libres et donc $\mathbb{Q}$-libres. D'après l'exercice précédent, il existe $(d_1, \ldots, d_n) \in \mathbb{N}^n$, vérifiant $d_1|d_2|\cdots|d_n$ et P et Q dans $\mathrm{GL}_n(\mathbb{Z})$ tels que

$$\mathrm{PAQ} = \mathrm{Diag}(d_1, d_2, \ldots, d_n) = \mathrm{D}.$$

Le rang de la matrice PAQ est r, comme celui de A. La matrice D a donc r termes non nuls sur sa diagonale. La condition $d_1|d_2|\cdots|d_r$ entraîne que $d_i \geqslant 1$ si $i \leqslant r$ et $d_{r+1} = 0$ dans le cas où $r < n$.

Considérons les vecteurs-colonnes $\varepsilon_1, \ldots, \varepsilon_n$ de P^{-1}. La matrice de passage de la base canonique $\mathcal{B}_0$ de $\mathbb{Z}^n$ (qui est celle de $\mathbb{Q}^n$) à $(\varepsilon_1, \ldots, \varepsilon_n)$ est P^{-1}, qui appartient à $\mathrm{GL}_n(\mathbb{Z})$. Le système $(\varepsilon_1, \ldots, \varepsilon_n)$ est donc une base de $\mathbb{Z}^n$, toujours d'après l'exercice 7.19. La matrice du système $(d_1\varepsilon_1, \ldots, d_r\varepsilon_r, 0, \ldots, 0)$, dans la base $\mathcal{B}_0$, est alors $\mathrm{P}^{-1}\mathrm{D}$. Notons $(\mathrm{C}_1, \ldots, \mathrm{C}_n)$ les vecteurs-colonnes de $\mathrm{P}^{-1}\mathrm{D}$. On a ainsi

$$\mathrm{C}_1 = d_1\varepsilon_1, \ \ldots, \mathrm{C}_r = d_r\varepsilon_r, \ \mathrm{C}_{r+1} = \cdots = \mathrm{C}_n = 0.$$

L'égalité $\mathrm{P}^{-1}\mathrm{D} = \mathrm{AQ}$ entraîne que $\mathrm{C}_1, \ldots, \mathrm{C}_n$ sont des combinaisons linéaires à coefficients entiers de $e_1, \ldots, e_r$ et appartiennent donc à G. Le

système $(C_1, \ldots, C_r)$ est $\mathbb{Z}$-libre, car $\mathbb{Q}$-libre, puisque $\operatorname{rg} AQ = \operatorname{rg} A = r$. Enfin, on conclut de l'égalité $A = (C_1|\cdots|C_r|0|\cdots|0)Q^{-1}$, que les colonnes de A, c'est-à-dire les vecteurs $e_1, \ldots, e_r$, sont combinaisons linéaires à coefficients entiers de $C_1, \ldots, C_r$. Il en résulte que $C_1, \ldots, C_r$ engendrent G tout entier. Le système $(C_i)_{1 \leqslant i \leqslant r} = (\delta_i \varepsilon_i)_{1 \leqslant i \leqslant r}$ constitue donc une base du groupe G.

Conclusion. On a trouvé une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de $\mathbb{Z}^n$, des entiers $d_i \geqslant 1$ tels que $d_1|d_2|\cdots|d_r$ et $(d_1\varepsilon_1, d_2\varepsilon_2, \ldots, d_r\varepsilon_r)$ soit une base de G.

2. On note $x_1, \ldots, x_n$ les éléments de H et on considère le morphisme de groupes

$$f : (k_1, \ldots, k_n) \in \mathbb{Z}^n \longmapsto k_1x_1 + \cdots + k_nx_n \in \mathrm{H}.$$

L'application f est surjective et d'après le théorème d'isomorphisme, on a $\mathbb{Z}^n / \operatorname{Ker} f \simeq \mathrm{H}$.

D'après la question précédente, il existe une base $(\varepsilon_1, \ldots, \varepsilon_n)$ de $\mathbb{Z}$, des entiers non nuls $d_1, \ldots, d_r$ tels que $d_1|d_2|\cdots|d_r$ et $(d_1\varepsilon_1, \ldots, d_r\varepsilon_r)$ est une base de $\operatorname{Ker} f$. Considérons l'application φ qui, à $X \in \mathbb{Z}^n$, associe le système de coordonnées de X dans la base $(\varepsilon_1, \ldots, \varepsilon_n)$. Il s'agit d'un automorphisme du groupe $\mathbb{Z}^n$, pour lequel on a $\varphi(\mathbb{Z}^n) = \mathbb{Z}^n$ et $\varphi(\operatorname{Ker} f) = d_1\mathbb{Z} \times \cdots \times d_r\mathbb{Z} \times \{0\}^{n-r}$.

Le lecteur se convaincra facilement que dans ces conditions, on obtient

$$\mathrm{H} \simeq \mathbb{Z}^n / \operatorname{Ker} f \simeq \varphi(\mathbb{Z}^n)/\varphi(\operatorname{Ker} f) = \mathbb{Z}^n / \left(d_1\mathbb{Z} \times \cdots \times d_r\mathbb{Z} \times \{0\}^{n-r}\right)$$

et donc

$$\mathrm{H} \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_r\mathbb{Z}) \times \mathbb{Z} \times \cdots \times \mathbb{Z}.$$

Comme H est fini, on a nécessairement $r = n$ et

$$\mathrm{H} \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z}).$$

En notant s le plus petit entier tel que $d_s \geqslant 2$ (qui est défini dès que H n'est pas réduit à l'élément neutre), il vient

$$\boxed{\mathrm{H} \simeq (\mathbb{Z}/d_s\mathbb{Z}) \times \cdots \times (\mathbb{Z}/d_n\mathbb{Z})}$$

et la suite $(d_s, d_{s+1}, \ldots, d_n)$ a les propriétés voulues. $\lhd$

On se reportera à l'exercice 2.20 du chapitre 2 (Groupes) pour une démonstration de l'unicité des d_i.

Le résultat suivant tient plus de l'arithmétique que de la théorie des matrices. Il démontre que dans la résolution d'un système linéaire de m équations à n inconnues, avec $n > m$, et dont les coefficients sont entiers, on peut toujours trouver des solutions «pas trop grandes».

7.23. Lemme de Siegel

Soit n et m dans $\mathbb{N}^*$, avec $n > m$. $A = (a_{ij})_{\substack{1\leqslant i\leqslant m\\ 1\leqslant j\leqslant n}} \in \mathcal{M}_{m,n}(\mathbb{Z})$. On suppose qu'il existe une entier $\alpha > 0$ tel que $|a_{i,j}| \leqslant \alpha$, pour tout $(i,j) \in [\![1,m]\!] \times [\![1,n]\!]$.

Montrer qu'il existe $X \subset \mathbb{Z}^n$, $X \neq 0$, tel que $AX = 0$ et tel que, si $X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, on ait, pour tout $j \in [\![1,n]\!]$

$$|x_j| \leqslant (n\alpha)^{\frac{m}{n-m}} + 1.$$

(École normale supérieure)

▷ **Solution.**

• Remarquons, pour commencer, que le système linéaire $AX = 0$ admet des solutions non nulles dans $\mathbb{Q}^n$, puisqu'il a m équations et n inconnues avec $m < n$. Si $X \in \mathbb{Q}^n$ est une solution non nulle, en multipliant X par un entier convenable (par exemple le produit des dénominateurs des coordonnées de X), on obtient une solution dans $\mathbb{Z}^n$. La question consiste à trouver une solution entière «assez petite».

• Si on trouve deux vecteurs distincts de $\mathbb{Z}^n$, X et X′ qui vérifient $AX = AX'$, on obtient un vecteur du noyau de A, à savoir $X - X'$. L'idée de la démonstration est la suivante : choisir des vecteurs de $\mathbb{Z}^n$ dans une partie bornée de $\mathbb{R}^n$ et en choisir suffisamment pour être sûr d'en trouver – par une application du principe des tiroirs de Dirichlet – deux qui ont la même image par A. On notera $\|\ \|$ la norme infinie, que ce soit dans $\mathbb{R}^n$ ou dans $\mathbb{R}^m$.

• On va commencer par estimer $\|AX\|$ en fonction de $\|X\|$. On note

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{et} \quad Y = AX = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}.$$

On a pour tout $i \in [\![1,m]\!]$, $|y_j| = \left|\sum_{j=1}^{n} a_{ij}x_j\right| \leqslant \sum_{j=1}^{n} |a_{ij}||x_j| \leqslant n\alpha\|X\|$ et donc

$$\|AX\| \leqslant n\alpha\|X\|.$$

• Soit $M \in \mathbb{N}$. On note B_M la boule fermée de $\mathbb{R}^n$, centrée en 0, de rayon M pour la norme $\|\ \|$. Un vecteur $X \in \mathbb{Z}^n$ est dans B_M si et

seulement si, pour tout $1 \leqslant i \leqslant n$, $|x_i| \leqslant \mathrm{M}$. Pour chaque coordonnée, on a exactement $2\mathrm{M}+1$ possibilités de sorte que

$$\mathrm{Card}\,(\mathrm{B}_{\mathrm{M}} \cap \mathbb{Z}^n) = (2\mathrm{M}+1)^n.$$

D'après le point précédent, l'image par A de $\mathrm{B}_{\mathrm{M}} \cap \mathbb{Z}^n$ est incluse dans l'intersection de $\mathbb{Z}^m$ et de la boule fermée de $\mathbb{R}^m$ de rayon $n\alpha\mathrm{M}$. Cet ensemble est de cardinal $(1+2n\alpha\mathrm{M})^m$.

Par le lemme des tiroirs, on est donc assuré de trouver deux vecteurs distincts X et X′ de $\mathrm{B}_{\mathrm{M}} \cap \mathbb{Z}^n$, tels que $\mathrm{AX} = \mathrm{AX}'$, dès lors que

$$(2n\alpha\mathrm{M}+1)^m < (2\mathrm{M}+1)^n.$$

Pour cela, il suffit que $(2\mathrm{M}+1)^n \geqslant (n\alpha)^m(2\mathrm{M}+1)^m$, ce qui équivaut à

$$2\mathrm{M} \geqslant (n\alpha)^{\frac{m}{n-m}} - 1.$$

Pour M ainsi choisi, la solution $\mathrm{X}-\mathrm{X}'$ du système vérifie, par inégalité triangulaire, $\|\mathrm{X}-\mathrm{X}'\| \leqslant 2\mathrm{M}$. Il nous suffit donc de choisir M tel que

$$2\mathrm{M} \in \left[(n\alpha)^{\frac{m}{n-m}} - 1, (n\alpha)^{\frac{m}{n-m}} + 1\right]$$

pour conclure (c'est possible car un segment de longueur 2 contient toujours un entier pair). ◁

Siegel a utilisé ce résultat pour prouver la transcendance de certains nombres réels.

Index

A

algébrique (nombre), 108
algèbre, 293–298, 307–317
  simple, 294
anneau
  commutatif, 84–85
  des entiers de Gauss, 98–103
  des nombres décimaux, 90
  euclidien, 94, 98
  factoriel, 91, 255
  principal, 90–98, 255
  régulier, 85
  $\mathbb{Z}[X]$, 90
approximation par des rationnels, 247
arithmétique (fonction), 150–155
automorphismes
  de $K[X]$, 244
  de $\mathcal{L}(E)$, 293
  de $\mathbb{Q}(\sqrt{2})$, 106
  de $\mathcal{S}_n$, 74
  intérieurs, 48, 74

B

base (d'un groupe abélien), 350
Beatty (théorème de), 33
Bell (nombres de), 14
Bernstein (inégalité de), 225, 241
Bezout (théorème de), 124, 255
Bohl-Sierpinski-Weyl (théorème de), 31
Bruhat (décomposition de), 347
Burnside (formule de), 289

C

carrés
  somme de deux, 100, 158–161
    dans $\mathbb{R}[X]$, 194
  somme de quatre, 162
  somme de trois, 164
Cauchy (lemme de), 46
centre d'un p-groupe, 47
commutant, 282
commutateur, 58
congruence, 144, 145
conjugaison (classe de), 47, 49, 53
contenu (d'un polynôme), 188
corps, 43, 106–115, 129
  fini, 16–20
  cyclotomique, 196
crible (formule du), 9, 156
cyclique
  groupe, 41, 43, 64, 129
cyclotomique
  corps, 190
  polynôme, 135, 190

D

Davenport-Cassels (lemme de), 164
dérangements, 7–14
dérivations, 311–317
Descartes (règle de), 237
diédral (groupe), 57
diophantienne (équation), 165
Dirichlet (théorème de la progression arithmétique de), 135
discriminant, 183
distingué (sous-groupe), 52
diviseur (d'un polynôme), 197
diviseur de zéro, 82
divisibilité, 120, 174, 175
drapeau, 263, 347
dualité, 298–302
  dans $\mathcal{M}_n(K)$, 329–331, 335
Ducci (problème de), 147

E

Eisenstein (critère de), 188–191
endomorphisme
  cyclique, 283
  nilpotent, 270–271
Eneström-Kakeya (théorème de), 233
équation aux classes, 46, 52, 54
Erdös, 153
espace vectoriel
  quotient, 260, 267, 269, 273
  sur un corps fini, 17–20
euclidien (anneau), 94, 98
Euler (indicatrice d'), 130, 135, 150
exposant d'un groupe abélien, 43
extension quadratique, 104

F

factoriel (anneau), 91, 255
factorisation, 266
  bilatère, 321
Fermat
  grand théorème, 166
  nombres de, 132
  petit théorème, 126–129
Fibonacci (suite de), 6
Fitting (décomposition de), 277

fonction
arithmétique, 150–155
de Möbius, 150, 156
multiplicative, 103, 153
polynomiale, 193–198, 200, 202–206
somme des diviseurs, 151–153
symétrique des racines, 206–214
zêta, 207
fractions rationnelles, 240–244
Frobenius (théorème de), 52
Frobenius-König (théorème de), 345

G

Gauss
anneau des entiers de, 98–103
lemme de, 256
pivot de, 347, 354
théorème de, 31
Gauss-Lucas (théorème de), 229, 232
générateurs
de S_n , 67
du groupe modulaire, 60
groupe
multiplicatif d'un corps, 43, 129
abélien fini (théorème de structure), 64, 358
cyclique, 41, 43, 64, 129
dérivé, 57
des rotations, 54
diédral, 57
libre de type fini, 352
modulaire, 60
opérant sur un ensemble, 45–47, 289, 339
ordonné, 78
quotient, 39–41, 64
symétrique, 46, 66–77

H

Hilbert
matrice de, 242
polynômes, 198, 205
homothétie vectorielle, 268–270
Howie (théorème de), 27

I

idéal
de $\mathcal{L}(E)$, 295–298
maximal, 88
premier, 106
principal, 87
indicatrice d'Euler, 130, 135, 150
indice
de nilpotence, 270, 311
d'un sous-groupe, 46, 47, 50
inégalité
de Bernstein, 225
de Landau, 234
de Markov, 225
de Schur, 225
de Sylvester, 272
interpolation, 199–202
inversibilité, 82
involutions, 19, 125
irréductible
d'un anneau, 91, 98–103
fraction, 118
polynôme de $\mathbb{Z}[X]$, 188–191

K

Kronecker (théorème de), 213
Kurschak (théorème de), 138

L

Lagrange (interpolation de), 199–202
Laguerre (théorème de), 217
Landau (inégalité de), 234
Legendre (théorème de), 139
Lie (crochet de), 336
Liouville (théorème de), 179, 180
Lucas
congruences de, 144
théorème de, 144

M

Markov (inégalité de), 225
Maschke (théorème de), 292
Mason (théorème de), 180
matrice
de Cauchy, 242
de dilatation, 347, 354
de Hilbert, 242
de transvection, 347, 354
équivalente, 320–323
dans $\mathcal{M}_n(\mathbb{Z})$, 354
inversible dans $\mathcal{M}_n(\mathbb{Z})$, 352
monotone, 341
positive, 341
stochastique, 343
maximal (idéal), 88
Möbius (fonction de), 150, 156
modulaire (groupe), 60
monotone (matrice), 341
morphisme
de conjugaison, 48
de groupes, 38, 39, 69, 70

N

Newton (formules de), 209
nilpotent (endomorphisme), 270–271
nombre algébrique sur un corps, 108

P

Paify-Erdös (théorème de), 140
partitions, 20
pivot de Gauss, 347, 354
point visible, 122
polynôme
  cyclotomique, 190
  de Hilbert, 198, 205
  de Tchebychev, 222–228
  interpolateur, 199–202
  positif, 194–197
  primitif, 188
  scindé, 211, 215–224
positive (matrice), 341
positivement génératrice (famille), 302–306
premier
  idéal, 106
  nombre, 130, 134, 137
principal
  anneau, 90–255
  idéal, 87
produits d'entiers consécutifs, 123
projecteur, 284–298
Prüfer (groupes de), 59
pseudo-inverse, 274

Q

quotient
  espace vectoriel, 260, 267, 269, 273
  groupe, 39–41, 64

R

racines d'un polynôme, 206, 214, 231
rang, 267, 320
  théorème du, 272–280
  endomorphismes de $\mathcal{M}_n(\mathbb{C})$ conservant le rang, 323–328
  matrices de rang 1, 325
relation d'équivalence, 16
résultant, 182
rotation, 54
Rough-Hurwitz (critère de), 235

S

Schur (inégalité de), 225
scindé (polynôme), 211, 215–224
série génératrice, 9, 14, 210
Siegel (lemme de), 360
Sophie Germain (théorème de), 167
sous-espace vectoriel
  de $\mathcal{M}_n(K)$, 331
  stable, 269, 286, 292
sous-groupe
  d'un groupe libre de type fini, 352
  d'indice infini, 50
  distingué, 52
  fini de $\mathbb{Q}/\mathbb{Z}$, 40
  fini de $SO_3(\mathbb{R})$, 54
stable
  partie de $\mathbb{N}$ (pour l'addition), 124
  sous-espace, 269, 286, 292
  supplémentaire, 292
stochastique (matrice), 343
Sturm (théorème de), 238
supplémentaire, 261
  stable, 292
Sylvester (inégalité de), 272
symétrique
  fonction des racines, 206–214
  groupe, 46, 66–77

T

Tchebychev (polynômes de), 222–228
théorème
  des deux carrés, 160
  des quatre carrés, 162
trace, 328–331, 339
transcendance de e, 249

V

valeurs absolues
  sur $C[X]$, 112
  sur $\mathbb{Q}$, 114
valuation, 110
  p-adique, 138–139, 143

W

Wilson (théorème de), 128

Z

$\zeta(2)$, 207

IMPRIMÉ EN GRANDE-BRETAGNE
PAR CAMBRIDGE UNIVERSITY PRESS
DÉPÔT LÉGAL OCTOBRE 2007