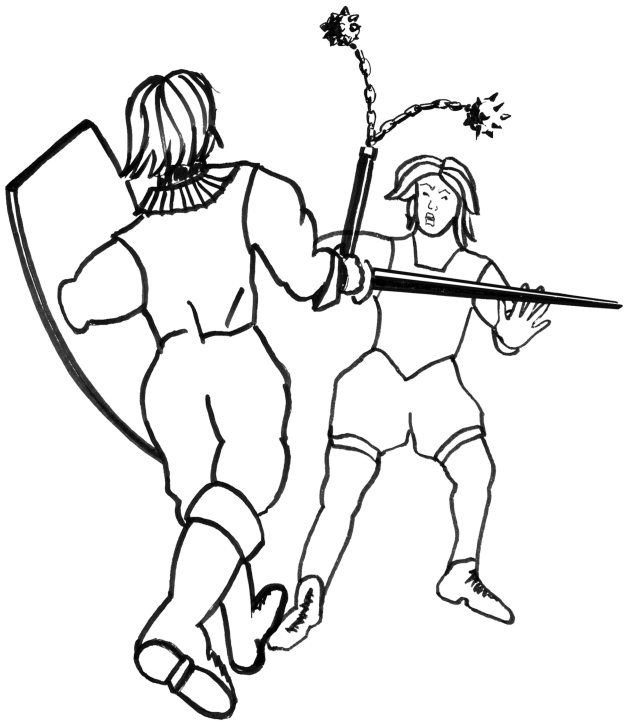
Mathématiques en devenir

101. — Jacques Faraut. *Analyse sur les groupes de Lie. Une introduction*
102. — Patrice Tauvel. *Corps commutatifs et théorie de Galois*
103. — Jean Saint Raymond. *Topologie, calcul diff. et variable complexe*
104. — Clément de Seguins Pazzis. *Invitation aux formes quadratiques*
105. — Bruno Ingrao. *Coniques projectives, affines et métriques*
106. — Wolfgang Bertram. *Calcul différentiel topologique élémentaire*
107. — Henri Lombardi & Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini*
108. — Frédéric Testard. *Analyse mathématique. La maîtrise de l'implicite*
109. — Grégory Berhuy. *Modules : théorie, pratique... et un peu d'arithmétique*
110. — Bernard Candelpergher. *Théorie des probabilités. Une introduction élémentaire*
111. — Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries. Tome premier*
112. — Gema-Maria Díaz-Toca, Henri Lombardi et Claude Quitté. *Modules sur les anneaux commutatifs*
113. — Philippe Caldero et Jérôme Germoni. *Histoires hédonistes de groupes et de géométries. Tome second* – encores
114. — Alain Debreil. *Groupes finis et treillis de leurs sous-groupes*
115. — François Rouvière. *Initiation à la géométrie de Riemann*
116. — Nikolaï Nikolski. *Matrices et opérateurs de Toeplitz*
117. — Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome premier*
118. — Martine et Hervé Queffélec. *Analyse complexe et applications*
119. — Alain Debreil, Jean-Denis Eiden, Rached Mneimné et Tuong-Huy NGuyen. *Formes quadratiques et géométrie*
120. — Christian Leruste.*Topologie algébrique–Une introduction, et au-delà*
121. — Grégory Berhuy. *Algèbre : le grand combat*
122. — Philippe Caldero et Jérôme Germoni. *Nouvelles histoires hédonistes de groupes et de géométries. Tome second*
123. — Jacques Faraut. *Analyse sur les groupes de Lie, une introduction.* Nouvelle édition revue et augmentée
124. — Charles-Michel Marle. *Géométrie symplectique et géométrie de Poisson*
125. — Pascal Boyer. *Petit compagnon des nombres et de leurs applications*
126. — Laurent Le Floch et Frédéric Testard. *Probabilités 1 – Le hasard* est *la nécessité*

Grégory Berhuy

Algèbre : le grand combat

Deuxième édition



Calvage & Mounet

Grégory Berhuy est professeur à l'université de Grenoble Alpes.
Ses domaines de recherche de prédilection couvrent entre autres l'étude des invariants des structures algébriques, et l'application de l'algèbre non commutative à la communication sans fil.

gregory.berhuy@univ-grenoble-alpes.fr

Mathematics Subject Classification (2010) – Primary :

13AXX General commutative ring theory
13CXX Theory of modules and ideals
13EXX Chain conditions, finiteness conditions
13FXX Arithmetic rings and other special rings
15A21 Canonical forms, reductions, classification
15A36 Matrices of integers
16DXX Modules, bimodules and ideals
16PXX Chain conditions, growth conditions, and other forms of finiteness
18XX Category theory. Homological algebra
19AXX Grothendieck groups and K_0

Le dessin en page de titre est d'Isabella Bembo.
La « Greg's massue » est de Maya Tayara.

ISBN 978-2-916352-83-1

⊗ Imprimé sur papier permanent

Deuxième édition, 2020

Cet ouvrage est dédicacé :

— *à mes ~~victimes~~ étudiants passés, présents et futurs*

— *à mon ancien enseignant et collègue Georges Gras, qui m'a révélé la beauté de l'algèbre et l'existence des idéaux maximaux*

— *à mon ancien enseignant et collègue Henri Lombardi, qui m'a révélé la beauté de l'algèbre et la non-existence des idéaux maximaux*

— *à ma mère, fan de la première heure, et qui vante en la moindre occasion à qui veut bien l'entendre la qualité et l'utilité de mes ouvrages… comme presse-papiers.*

Table des matières

Partie 1. Phase d'approche : rappels et compléments

I. Théorie des ensembles

1. Applications 3
2. Relations d'équivalence 6
3. Lois internes, structures algébriques 11
4. Ensembles ordonnés 15
5. Exercices 16

II. Arithmétique dans $\mathbb{Z}$

1. Divisibilité dans $\mathbb{Z}$ 21
2. Division euclidienne, algorithme d'Euclide 23
3. Entiers premiers entre eux 26
4. Décomposition en facteurs premiers 27
5. pgcd et ppcm d'une famille quelconque d'entiers 29
6. Arithmétique modulaire 30
7. Exercices 33

III. Rappels et compléments d'algèbre linéaire

1. Généralités 37
2. Familles libres, génératrices, bases 40
3. Somme d'espaces vectoriels 44
4. Matrices représentatives, changement de base 46
5. Formes linéaires, droites et hyperplans 48
6. Exercices 53

IV. Déterminant
1. Introduction éclair au groupe symétrique . . . 57
2. Formes multilinéaires alternées, déterminant . . . 62
3. Déterminant d'un endomorphisme . . . 65
4. Déterminant d'une matrice . . . 67
5. Transvections et dilatations . . . 73
6. Exercices . . . 84

V. Un peu de géométrie
1. Affinités vectorielles . . . 89
2. Espaces euclidiens, espaces hermitiens . . . 93
3. Isométries d'un espace euclidien : premiers résultats . . . 99
4. Structure des endomorphismes normaux . . . 106
5. Espaces euclidiens orientés . . . 112
6. Exercices . . . 119

Partie 2. Groupes : il faut agir !!

VI. Propriétés élémentaires des groupes
1. Généralités . . . 125
2. Sous-groupes . . . 132
3. Sous-groupes engendrés par une partie . . . 141
4. Théorème de Lagrange, ordre d'un élément . . . 144
5. Interlude : formule d'inversion de Möbius . . . 152
6. Groupes monogènes, groupes cycliques . . . 154
7. Exercices . . . 157

VII. Groupes opérant sur un ensemble
1. Actions de groupe . . . 169
2. Premières applications . . . 177
3. Coloriages . . . 182
4. Exercices . . . 192

VIII. Groupe symétrique, groupe alterné
1. Préliminaires . . . 199
2. Décomposition en produit de cycles . . . 202
3. Systèmes de générateurs . . . 212
4. Signature, groupe alterné . . . 213
5. Structure des groupes symétrique et alterné . . . 217
6. Exercices . . . 220

IX. Groupes quotient
1. Définition 235
2. Théorème de factorisation 239
3. Suites de composition 246
4. Présentations de groupes 262
5. Exercices 283

X. Produits directs et semi-directs
1. Préliminaires 291
2. Produits directs 293
3. Produits semi-directs 297
4. Exercices 307

XI. Actions de groupe et structure des groupes finis
1. Théorème de Sylow 311
2. Actions primitives et critère de simplicité d'Iwasawa 315
3. Exercices 328

XII. Thème et variations sur les groupes abéliens
1. Torsion dans un groupe abélien 339
2. Exposant d'un groupe 343
3. Caractères linéaires d'un groupe abélien fini 346
4. Groupes abéliens libres 350
5. Structure des groupes abéliens de type fini 357
6. Groupes abéliens divisibles 364
7. Exercices 376

XIII. Petite classification des groupes finis ; épisodes précédents
1. Quelques théorèmes de classification 381
2. Groupes finis d'ordre $\leqslant 15$ 383

Partie 3. Anneaux : la loi des irréductibles

XIV. Propriétés élémentaires des anneaux et des corps

1. Généralités 387
2. Éléments remarquables d'un anneau 394
3. Anneaux intègres, corps 398
4. Idéaux 403
5. Produit direct d'anneaux 410
6. Anneaux de polynômes 414
7. Polynômes symétriques 432
8. Exercices 443

XV. Anneaux quotient, théorème chinois

1. Anneaux quotient, théorème de factorisation 455
2. Idéaux premiers, maximaux 459
3. Théorème chinois 463
4. Exercices 472

XVI. L'anneau $\mathbb{Z}/n\mathbb{Z}$ en long, en large et en travers

1. Échauffement 485
2. Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$ 488
3. Carrés de $\mathbb{Z}/n\mathbb{Z}$ 492
4. Symboles de Legendre et de Jacobi 497
5. Exercices 511

XVII. Divisibilité dans les anneaux

1. Divisibilité, éléments irréductibles et premiers 515
2. Arithmétique des anneaux principaux 524
3. Anneaux euclidiens 529
4. Anneaux noethériens 537
5. Anneaux factoriels 542
6. Exercices 550

XVIII. Matrices à coefficients dans un anneau euclidien

1. Déterminant : le retour 569
2. Équivalence de matrices 572
3. Modules sur un anneau 584
4. Théorème de la base adaptée et applications 592
5. Exercices 605

XIX. Polynômes irréductibles et applications
1. Polynômes irréductibles et racines 609
2. Quelques critères d'irréductibilité 616
3. Factorialité de $A[X]$ 622
4. Irréductibilité d'un polynôme bicarré 629
5. Polynômes cyclotomiques et applications 640
6. Polynômes irréductibles sur $\mathbb{F}_p$, corps finis 651
7. Exercices 662

XX. Idéaux de $A[X]$
1. Principalité des idéaux de $A[X]$ 667
2. Noethérianité de $A[X]$ 671
3. Idéaux premiers de $A[X]$, A principal 675
4. Exercices 679

XXI. Séries formelles
1. Premières propriétés 681
2. Composition et dérivation de séries formelles 689
3. Séries formelles usuelles 706
4. Quelques applications des séries formelles 714
5. Exercices 720

XXII. Complétion I-adique
1. Complété I-adique 727
2. Propriétés métriques 734
3. Complétion en un idéal principal 744
4. Exercices 754

Partie 4. Des corps ! Des corps partout !

XXIII. Constructions à la règle et au compas et théorie des corps
1. Préliminaires 761
2. Extensions de corps 767
3. Extensions algébriques, transcendantes 778
4. Quelques problèmes de construction à la règle et au compas . . 787
5. Et après... 801
6. Exercices 803

XXIV. Polynômes et racines
1. Existence de racines dans une extension et applications 807
2. Corps de rupture, corps des racines d'un polynôme 816
3. Clôture algébrique d'un corps 823
4. Entiers algébriques 829
5. Exercices 835

XXV. Plongements et extensions séparables
1. Plongements 844
2. Propriétés des extensions séparables 851
3. Polynômes séparables 857
4. Traces et normes 861
5. Exercices 868

XXVI. Extensions galoisiennes
1. Extensions normales 875
2. Extensions galoisiennes 878
3. Le groupe de Galois d'un polynôme 885
4. Extensions cyclotomiques 893
5. Théorie de Kummer 898
6. Exercices 902

XXVII. Nul n'est censé ignorer Galois
1. Théorie de Galois 913
2. Résolubilité des équations par radicaux 922
3. Constructions à la règle et au compas : le retour 929
4. Exercices 931

Partie 5. Algèbre linéaire : réduisons en miettes !

XXVIII. Réduction des endomorphismes
1. Polynômes d'endomorphismes 941
2. Diagonalisation 954
3. Trigonalisation, décomposition de Dunford 961
4. Décomposition de Jordan 976
5. Exponentielle de matrices 987
6. Exercices 999

XXIX. Décomposition de Frobenius

1. Sous-espace stable engendré par un vecteur 1013
2. Endomorphismes cycliques 1016
3. Décomposition de Frobenius : approche classique 1019
4. Décomposition de Frobenius : calcul pratique 1025
5. Commutant et bicommutant d'un endomorphisme 1038
6. Exercices 1043

XXX. Dualité

1. Introduction 1049
2. Formes linéaires et bilinéaires, espace dual 1052
3. Interlude : espaces vectoriels quotient 1061
4. Dualité entre sous-espaces 1063
5. Bases duales 1070
6. Adjoint d'un endomorphisme 1075
7. Exercices 1083

Partie 6. Représentations : agissons dans l'espace !

XXXI. Représentations linéaires des groupes finis : introduction

1. Modules simples, modules indécomposables 1093
2. Représentations linéaires : définitions et premiers exemples . . . 1097
3. Interlude : produit tensoriel 1112
4. Opérations sur les représentations 1117
5. Théorème de Maschke 1123
6. Exercices 1128

XXXII. Théorie des caractères

1. Caractère d'une représentation 1137
2. Orthogonalité des caractères et conséquences 1146
3. Table des caractères d'un groupe fini 1166
4. Décomposition en somme de représentations irréductibles 1173
5. Propriétés d'intégralité et applications 1182
6. Degré des représentations irréductibles 1190
7. Exercices 1197

Bibliographie **1203**
Index **1207**

Avant-propos

Petit plaidoyer totalement partial pour l'étude de l'algèbre.–

Nous voudrions commencer cet ouvrage par un petit plaidoyer en faveur de cette discipline mal-aimée des étudiants qu'est l'algèbre. Les étudiants se plaignent souvent de sa difficulté à cause de son haut niveau d'abstraction. Bien souvent, les objets manipulés ne leur paraissent pas assez concrets, et l'utilité de l'étude des structures algébriques, semblant absconses, leur échappe complètement. Pourquoi donc s'embêter à classifier les groupes finis d'ordre donné ou chercher toutes leurs représentations irréductibles, pourquoi s'acharner à savoir si tel groupe est résoluble ou si tel anneau est factoriel, pourquoi calculer la réduite de Jordan d'un endomorphisme et autres joyeusetés ? Pourquoi un tel besoin quasi irrépressible chez le mathématicien de généraliser à l'extrême, sinon pour torturer les étudiants par pur plaisir sadique [1] ?

Avant de tenter de répondre à ces questions, essayons de définir succinctement ce qu'est l'algèbre. La définition la plus juste, du point de vue où l'on se place, est sans doute la suivante : c'est l'étude des structures algébriques. Ici, on entend par structure algébrique un ensemble muni d'une ou plusieurs lois de composition internes ou externes, éventuellement muni d'un ordre ou une topologie, le tout satisfaisant un certain nombre d'axiomes. Ainsi, les groupes, les anneaux, les corps, les espaces vectoriels ou les représentations sont des structures algébriques. Une fois les structures définies, on définit souvent la notion de sous-structure, mais surtout les flèches entre deux telles structures, appelées « morphismes », qui sont « les applications compatibles avec les lois internes et externes ». Ce sont d'ailleurs les morphismes qui constituent la part importante de la théorie, plus que les objets eux-mêmes, puisque ce sont eux qui établissent les relations entre les objets, à travers la notion de structure quotient, par exemple. Une notion cruciale découlant directement de la notion de morphisme est la notion d'isomorphisme. Elle permet d'identifier des objets a priori différents mais structurellement identiques, et jouissant alors de propriétés similaires à tout

1. D'aucuns diront que la réponse est contenue dans la question.

point de vue. De manière un peu vague, deux structures isomorphes sont en fait deux façons de voir le même objet, mais dont on aurait étiqueté les éléments différemment. Par exemple, tous les espaces vectoriels de dimension n sur un même corps sont isomorphes, et une propriété vraie pour l'un est aussi vraie pour tous les autres, même si leurs éléments sont de natures différentes. D'ailleurs, après le choix d'une base, tout espace vectoriel de dimension n se comporte comme K^n : l'étiquetage des éléments se fait via les coordonnées dans la base choisie, mais le comportement des éléments vis-à-vis des opérations est exactement le même que celui des vecteurs de K^n muni de ses opérations usuelles. Un des problèmes fondamentaux en algèbre est alors de classifier les objets à isomorphismes près. Pour résumer, ce qui compte, ce n'est pas tant les objets, mais les flèches entre les objets [2].

Passons maintenant aux difficultés d'appréhender cette théorie. En ce qui concerne le problème du manque de palpabilité des objets, cela provient en grande partie d'un manque de pratique de l'abstraction, les étudiants étant confrontés aux objets abstraits et aux joies de la démonstration de théorèmes formels extrêmement tardivement. Autrement dit, pour maîtriser une nouvelle notion/discipline, il faut s'exercer. Ce principe frappé au coin du bon sens s'applique bien évidemment dans la vie de tous les jours (pratique d'un sport, d'un instrument, d'une langue, de la danse, etc.). Il n'y a aucune raison pour les mathématiques y échappent. Cela dit, la difficulté avec l'algèbre, et de manière plus générale avec les mathématiques, est que les définitions et théorèmes exposés en cours ou dans les ouvrages sont le fruit d'un long cheminement intellectuel, qui s'est déroulé parfois sur plusieurs dizaines d'années. Par conséquent, on ignore souvent le problème concret qui a motivé l'introduction de telle ou telle notion à l'origine. Par exemple, l'algèbre linéaire trouve essentiellement sa source dans l'étude des systèmes d'équations dites linéaires et également dans la géométrie. C'est Descartes qui fût le premier à utiliser des coordonnées pour résoudre des problèmes géométriques comme la détermination de l'intersection de deux droites, en termes d'équation linéaire, établissant dès lors un pont entre deux branches mathématiques jusqu'alors séparées : l'algèbre et la géométrie. Il faut attendre le dix-neuvième siècle et Gauss pour qu'une étude approfondie des systèmes linéaires soit faite. Camille Jordan résout également définitivement le problème de la réduction d'endomorphisme. Il faut noter que la notion d'espace vectoriel n'avait toujours pas été dégagée à ce moment là ! Une première tentative de formalisation de cette notion a été effectuée par Grassmann en 1844, dans son traité « La théorie de l'extension linéaire ».

2. Ce point de vue a d'ailleurs été poussé à l'extrême et avec succès à travers la théorie des catégories.

Ce traité, passé relativement inaperçu, contient déjà l'essentiel de la théorie telle que nous la pratiquons aujourd'hui. Enfin, en 1888, Peano, en se basant sur les travaux de Grassmann, axiomatise définitivement la théorie. On pourrait constater la même chose avec d'autres branches de l'algèbre. La théorie des groupes trouve ainsi son origine première dans le problème de résolubilité des équations polynomiales par radicaux et les travaux de Galois. La notion de groupe est également utilisée par Klein pour étudier les nouvelles géométries ayant émergé (géométrie hyperbolique, géométrie projective). Kummer introduit également un groupe abélien dans ses tentatives de démonstration du grand théorème de Fermat. Néanmoins, il faudra attendre 1882 pour qu'émerge la première définition axiomatique d'un groupe abstrait. Notons au passage que l'étude des anneaux prend également sa source dans les travaux de Dedekind sur le théorème de Fermat. C'est finalement Noether qui établira les fondements de la théorie des anneaux commutatifs unitaires. [3]

Vu la diversité des contextes dans lesquels toutes ces notions sont apparues historiquement, on comprend mieux pourquoi la mise en place d'une théorie générale est indispensable. D'ailleurs, établir une théorie unificatrice possède plusieurs avantages : éclairer sous un nouveau jour les cas particuliers qui ont motivé son élaboration, obtenir des résultats valables pour tous les objets de la théorie considérée (ce qui évite de redémontrer la même chose dans des dizaines de cas particuliers), mettre à disposition de nouveaux outils plus puissants pouvant être utiles pour démontrer de nouveaux théorèmes, créer des passerelles entre diverses branches des mathématiques, etc. Le prix à payer est souvent une montée dans l'abstraction, mais c'est un mal nécessaire pour pouvoir utiliser une artillerie efficace. Une image qui fonctionne plutôt bien est celle du randonneur complètement perdu : afin de retrouver plus facilement son chemin, il va chercher à prendre de la hauteur et à atteindre un point de vue plus élevé, pour avoir accès à un panorama complet des alentours, avant de redescendre pour revenir sur le bon chemin. Un des exemples les plus frappants est celui du grand théorème de Fermat : pour arriver finalement à une démonstration, il a fallu étudier les structures algébriques d'objets dont on aurait eu peine à imaginer l'existence au temps de Fermat. C'est ainsi que la théorie des anneaux, la théorie des nombres et de nouveaux pans de la géométrie algébrique se sont développés. Comme dans d'autres situations en mathématiques, le fait d'intégrer le problème de Fermat dans un cadre plus général et apparemment beaucoup plus difficile a permis de grandes avancées, parce que l'on dispose alors de tout un outillage développé pour ce cadre.

Essayons finalement de répondre à la question que beaucoup d'étudiants se posent légitimement : à quoi ça sert ? Mentionnons tout de suite la princi-

3. Toutes ces informations historiques sont tirées d'articles de Wikipédia.

pale force de l'algèbre, à savoir son ubiquité. Il est en effet intéressant de souligner que les diverses branches de l'algèbre ne sont pas compartimentées. Bien au contraire, il existe des passerelles entre elles et vers d'autres disciplines, ce qui permet une variété d'applications dans divers domaines.

La théorie des groupes illustre parfaitement notre propos. La notion de groupe apparaît naturellement dès qu'il s'agit d'étudier les symétries d'un objet. Elle intervient ainsi en géométrie puisque beaucoup d'exemples de groupes sont de nature géométrique, mais aussi en chimie (simplification des calculs de structure électronique, classification des états électroniques ou vibratoires d'une molécule ou d'un solide), en physique théorique (théorie de la relativité, théorie de l'unification) via la théorie des représentations. La théorie des groupes est aussi intimement liée à la théorie des corps via la théorie de Galois. Cette dernière théorie permet par exemple de donner une jolie caractérisation de la constructibilité d'un nombre à la règle et au compas, ou de la résolubilité d'une équation polynomiale par radicaux en termes de théorie des groupes. Une autre application de la théorie de Galois moins connue des étudiants (car plus pointue), mais omniprésente dans la recherche mathématique, est la résolution des problèmes dits « de descente ». De manière très floue, un problème de descente est un problème du type suivant : on considère un ensemble d'objets mathématiques et une relation d'équivalence sur ces objets. On se donne deux objets définis sur un corps K, et l'on suppose que les deux objets sont équivalents lorsque l'on les considère comme des objets définis sur un corps L contenant K. Les deux objets sont-il équivalents sur K ? Par exemple, considérons le problème suivant : soient $M, M' \in \mathrm{M}_n(K)$ deux matrices. On suppose qu'il existe une matrice $Q \in \mathrm{GL}_n(L)$ telle que $M' = QMQ^{-1}$, où L est un corps contenant K. Existe-t-il une matrice $P \in \mathrm{GL}_n(K)$ telle que $M' = PMP^{-1}$? Il est bien connu que la réponse est positive, et la démonstration la plus classique ne nécessite pas de théorie de Galois (cf. corollaire XXIX-4.9). On peut alors légitimement se poser la question de savoir si c'est encore le cas lorsque l'on remplace le groupe linéaire par le groupe spécial linéaire ou le groupe orthogonal. La réponse est cette fois négative, et la théorie de Galois permet de caractériser précisément les matrices M' pour lesquelles cela devient vrai, à M fixé. Enfin, dans un registre plus ludique, la théorie des groupes permet de résoudre certains casse-têtes célèbres comme le Rubik's cube ou le jeu du taquin.

De manière plus générale, la théorie des groupes se révèle un outil indispensable dans l'étude des structures mathématiques, quelles qu'elles soient. En effet, pour comprendre un objet mathématique, il est toujours utile d'étudier son groupe d'automorphismes. Il est aussi naturel d'essayer de faire agir un groupe sur cet objet et d'étudier les orbites et stabilisateurs associés. On obtient alors à la fois de plus amples renseignements sur l'objet lui-même et

sur le groupe qui agit. Enfin, lorsque l'on s'attaque au problème de classification d'objets mathématiques à isomorphisme près, problème qui s'avère extrêmement ardu en général, il est toujours utile d'associer un groupe à chaque objet, de sorte que deux objets isomorphes aient des groupes associés isomorphes. Cette approche est souvent fructueuse, surtout lorsque le groupe associé est abélien, puisque les groupes abéliens sont des objets particulièrement bien compris et dans lesquels il est facile de calculer. Ce principe est illustré de manière extrêmement frappante en topologie. À tout espace topologique X et tout point $x \in X$, on peut associer un groupe abélien $H_k(X, X \setminus \{x\})$ pour tout entier $k \geqslant 0$, de sorte que, si $h : X \xrightarrow{\sim} Y$ est un homéomorphisme, on a un isomorphisme de groupes

$$h_* : H_k(X, X \setminus \{x\}) \xrightarrow{\sim} H_k(Y, Y \setminus \{h(x)\}).$$

Ces groupes peuvent être calculés dans certains cas, grâce à des théorèmes généraux. Par exemple, on peut démontrer que $H_k(\mathbb{R}^n, \mathbb{R}^n \setminus \{x\})$ est trivial si $k \neq n$, et est isomorphe à $\mathbb{Z}$ si $k = n$, et cela pour tout $x \in \mathbb{R}^n$. On en déduit aisément le résultat non trivial suivant, dont il serait difficilement concevable (voire impossible) d'avoir une démonstration à la main : pour tous entiers $n, m \geqslant 1$, les espaces topologiques $\mathbb{R}^n$ et $\mathbb{R}^m$ sont homéomorphes si, et seulement si, $n = m$.

L'algèbre linéaire quant à elle s'invite aussi bien dans les autres branches de l'algèbre qu'en analyse (équations différentielles ou aux dérivées partielles, espaces fonctionnels), en mécanique, en théorie des graphes, en théorie du codage (codes linéaires auto-correcteurs), dans l'étude des systèmes dynamiques discrets, en probabilités (chaînes de Markov), en informatique, etc. C'est aussi un excellent outil pour étudier les groupes, grâce à la théorie des représentations linéaires. Par exemple, la table des caractères permet de déterminer tous ses groupes distingués ou de décider de la simplicité d'un groupe (cf. théorèmes XXXII-1.8 et XXXII-1.10), ou de démontrer des théorèmes de structure (cf. théorèmes XXXII-5.4 et XXXII-5.5). Mentionnons aussi le théorème XXXII-2.20, dont la seule démonstration connue utilise la théorie des représentations linéaires. D'autre part, comme déjà mentionné plus haut, la théorie des représentations a des applications en chimie et en physique théorique.

Enfin, la théorie des anneaux possède un pouvoir d'ubiquité similaire à la théorie des groupes ou de l'algèbre linéaire. Cette théorie trouve son origine en théorie des nombres, avec les travaux de Dedekind visant à démontrer le théorème de Fermat, le point de départ étant que si x, y, $z \in \mathbb{Z}$ et p est un nombre premier impair, l'égalité $x^p + y^p = z^p$, peut se retraduire dans l'anneau $\mathbb{Z}[\zeta_p] = \{P(\zeta_p) \mid P \in \mathbb{Z}[X]\}$ sous la forme

$$(x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y) = z^p,$$

où $\zeta_p = e^{\frac{2i\pi}{p}}$.

La notion d'anneau intervient également de manière déterminante en géométrie algébrique, mais aussi en logique formelle (algèbres de Heyting, de Boole, algèbres cylindriques, etc.), en théorie des représentations linéaires (si V est une représentation irréductible d'un groupe G, l'anneau des endomorphismes de V est un anneau à division), en algèbre linéaire (théorie des polynômes annulateurs). Récemment, la théorie des anneaux à division a trouvé des applications en théorie des codes Wifi, et a servi à construire des codes performants pour la transmission de données sans fil (téléphone portable, box Wifi). Enfin, la théorie des anneaux a permis d'étudier globalement les formes quadratiques sur un corps K, en introduisant l'anneau de Witt $W(K)$, ce qui a insufflé un nouvel essor à la théorie des formes quadratiques et a contribué à la découverte de nombreux résultats.

De manière générale, l'utilisation des structures algébriques permet souvent de démontrer des résultats de manière simple et élégante, une fois que l'on a les bons outils (comme la résolution d'un problème de constructibilité à la règle et au compas, qui est purement géométrique, grâce à la théorie des corps et des groupes, ou comme la résolution d'une question topologique difficile à coup de groupes d'homologie). On pourrait continuer indéfiniment la liste des applications des notions présentées dans cet ouvrage. Nous espérons que ce panorama réduit suffira à convaincre le lecteur du bien-fondé de l'étude des structures algébriques et de la beauté de cette théorie.

Prérequis.–

Le texte qui suit est un cours d'algèbre s'adressant à des lecteurs ayant acquis les notions mathématiques de base de première et deuxième années de Licence. Même si des rappels seront faits dans la première partie, nous supposerons que le lecteur maîtrise quelques notions simples de théorie des ensembles, l'arithmétique dans $\mathbb{Z}$, et surtout l'algèbre linéaire et matricielle de base. Le lecteur ne se sentant pas au point sur tout ou partie de ces notions est vivement encouragé à d'abord consolider ses connaissances sur les points précédents avant de s'attaquer à la lecture de cet ouvrage.

À qui s'adresse ce livre ?–

Ce livre est une version extrêmement étoffée de notes de cours d'algèbre donnés par l'auteur en L3 et en M1 à l'université de Grenoble Alpes. Il couvre entre autres l'intégralité du bagage algébrique minimum que devrait avoir acquis un étudiant en L3 et en M1 (sans parler des agrégatifs !). Il contient également des résultats qui permettent d'approfondir certaines thématiques ou de redécouvrir des notions classiques sous une nouvelle perspective, et qui pourront intéresser les candidats à l'agrégation interne ou externe.

Cet ouvrage est donc « multi-niveaux ». Aussi certains chapitres s'adressent-ils spécifiquement aux étudiants de M1, d'autres encore aux candidats à l'agrégation.
La répartition du contenu de cet ouvrage par niveaux, totalement subjective, peut se résumer comme suit.

• **L3**

- toute la partie 1 ;

- l'intégralité des chapitres VI, VII et VIII, exception faite de la section §3, qui peut être passée sans que cela ne nuise à la compréhension de la suite ;

- les sections §1 et §2 du chapitre IX ;

- le chapitre X, au moins jusqu'au corollaire X-3.11 ;

- la section §1 du chapitre XI ;

- la section §2 du chapitre XII, et éventuellement, à titre de compléments, la section §3 et le théorème XII-5.3 ;

- le chapitre XIII ;

- le chapitre XIV, au moins jusqu'à l'exemple XIV-6.32 inclus ;

- le chapitre XV dans son intégralité, sauf peut-être le lemme XV-2.4 et le théorème XV-2.5, qui peuvent être passés en première lecture ;

- les sections §1 et §2 du chapitre XVI ;

- les sections §1, §2 et §3 du chapitre XVII ;

- les sections §1, §2, §3 et §4 du chapitre XXVIII, et le début de la section §5 jusqu'au lemme XXVIII-5.6 inclus.

• **M1**

- tout ce qui précède ;

- la section IX-3, du moins ce qui concerne les groupes résolubles (le théorème de Jordan-Hölder pouvant être passé) ;

- l'intégralité des chapitres XIV, XV,XVII, XVIII ;

- le chapitre XIX, sauf la section §4, qui est extrêmement technique et dont l'importance des résultats est plutôt anecdotique ;

- éventuellement le chapitre XXI ;

- l'intégralité des chapitres XXIII à XXVII ;

- les sections §1, §2 et §4 du chapitre XXIX ;

- l'intégralité des chapitres XXX à XXXII.

• **Agrégation**

- l'intégralité de ce livre.

Notons néanmoins que cet ouvrage n'est **pas** un livre de préparation à l'agrégation. Tous les résultats s'adressant spécifiquement aux agrégatifs dans cet ouvrage (i.e. ceux contenus dans les chapitres/sections non mentionnés ci-dessus) doivent plutôt être vus comme des prolongements naturels aux notions abordées, et destinés à étoffer la culture générale mathématique du lecteur, même si certains peuvent être utilisés comme des points de développement dans les leçons (comme ceux concernant le symbole de Legendre-Jacobi, la démonstration classique de l'existence de la décomposition de Frobenius, ceux exposés dans le chapitre XX, ou même ceux de certains exercices). D'autres résultats en revanche, comme ceux sur l'irréductibilité de certains polynômes bicarrés (Chapitre XIX, § 4), ont probablement des démonstrations trop longues et/ou trop techniques pour pouvoir être utilisés comme points de développement, mais méritaient néanmoins d'avoir leur place dans cet ouvrage, pour leur originalité ou leur intérêt mathématique.

Contenu et notes bibliographiques.–

La première partie propose des rappels et de compléments. Dans le chapitre I, on fait de brefs rappels sur les applications, ainsi que sur les relations d'équivalence et les relations d'ordre. On introduit aussi brièvement les structures algébriques (groupes, anneaux, corps) qui seront étudiées dans cet ouvrage. Le chapitre II fournit des rappels de base sur l'arithmétique dans $\mathbb{Z}$ et l'arithmétique modulaire. Au passage, on introduit l'anneau $\mathbb{Z}/n\mathbb{Z}$, qui sera étudié plus en profondeur dans la troisième partie. On pourra retrouver toutes les notions abordées dans les chapitres I et II dans [3]. Le lecteur désireux d'en savoir un peu plus sur la théorie des ensembles pourra se référer à [28] ou [39]. [3]. En particulier, on trouvera une construction axiomatique de $\mathbb{N}$ dans les références précédentes. Dans le chapitre III, on rappelle les résultats d'algèbre linéaire qui seront utiles dans toute la suite, en proposant des généralisations au cas des espaces vectoriels de dimension infinie lorsque c'est possible. On étudie également succinctement les formes linéaires. Dans le chapitre IV, après une introduction éclair au groupe symétrique, on construit le déterminant d'un endomorphisme, et l'on démontre ses principales propriétés. On achève ce chapitre en étudiant les transvections et les dilatations d'un espace vectoriel de dimension finie. Le lecteur ayant besoin de se rafraîchir la mémoire sur les notions abordées dans ces chapitres pourra consulter [3] ou [27] avec profit. Le chapitre V expose quelques résultats classiques de géométrie vectorielle. Après avoir caractérisé les affinités vectorielles, on propose de brefs rappels sur les espaces euclidiens et hermitiens. On détermine alors la structure des endomorphismes normaux d'un espace euclidien ou hermitien. En particulier, on obtient la structure des isométries de tels espaces, ainsi que le théorème

de diagonalisation d'une matrice symétrique réelle en base orthonormée. Ce chapitre s'achève par quelques considérations sur les espaces euclidiens orientés. On définit la notion d'orientation, de base orthonormée, puis le produit mixte et le produit vectoriel. Le lecteur pourra retrouver tous les résultats sur les espaces euclidiens et leurs démonstrations dans [27].

La deuxième partie concerne la théorie des groupes. Le chapitre VI expose les notions élémentaires, à savoir groupes, sous-groupes, morphismes, sous-groupes engendrés par une partie, groupes cycliques et monogènes, ordre d'un élément et d'un sous-groupe. Le chapitre VII introduit une notion centrale dans la théorie, à savoir la notion de groupe agissant sur un ensemble, et qui fait le lien entre la théorie des groupes et la géométrie. On donne alors les premières applications des actions de groupe. La dernière section applique les résultats de ce chapitre à un problème de combinatoire. Dans le chapitre VIII, on étudie la structure du groupe symétrique et du groupe alterné (générateurs, sous-groupes distingués). Le chapitre IX introduit la théorie des groupes-quotient. Après avoir démontré le théorème de factorisation et ses corollaires, on s'intéresse ensuite aux diverses suites de composition associées à un sous-groupe. On démontre entre autres l'existence d'une suite de Jordan-Hölder, ainsi que quelques résultats classiques sur les groupes (super)-résolubles. Enfin, on introduit la notion de groupe libre et présentation d'un groupe par générateurs et relations. Dans le chapitre X, on introduit la notion de produit direct externe et interne, ainsi que la notion plus délicate de produit semi-direct. On démontre alors quelques critères simples pour déterminer si un groupe est isomorphe à un produit (semi-)direct. Le chapitre XI donne deux belles applications des actions de groupe à la structure des groupes finis : un critère de simplicité d'un groupe, dû à Iwasawa, et le théorème de Sylow, qui démontre l'existence de p-sous-groupes d'un groupe fini d'ordre maximal (où p est un nombre premier). Ce dernier théorème, joint aux résultats du chapitre précédent, permet déjà d'obtenir pas mal de résultats de classification de groupes finis d'ordre donné. Le chapitre XII s'articule autour des groupes abéliens, et contient des résultats classiques autour de cette notion : existence d'un élément d'un groupe abélien fini dont l'ordre est égale à l'exposant du groupe, structure des groupes abéliens de type fini, structure des groupes abéliens divisibles. Les notions et résultats abordés dans cette partie sont extrêmement classiques, et peuvent être retrouvés dans n'importe quel ouvrage consacré à la théorie des groupes, comme par exemple [21], [36] ou [46].

La troisième partie est consacrée à la théorie des anneaux. Dans le chapitre XIV, on introduit la notion d'anneau, ainsi que ses éléments remarquables (diviseurs de zéro, éléments inversibles, nilpotents, idempotents). On donne aussi une condition nécessaire et suffisante pour qu'un anneau soit isomorphe au produit direct de deux anneaux non triviaux. On définit

également l'anneau des polynômes à coefficients dans un anneau, et l'on étudie ses premières propriétés. Enfin, on démontre le théorème de structure des polynômes symétriques en n indéterminées. Le chapitre XV s'intéresse aux anneaux-quotient, et aux résultats classiques inhérents à cette notion : théorème de factorisation, caractérisation des idéaux premiers et maximaux en termes d'anneau-quotient, théorème chinois. Dans le chapitre XVI, on étudie l'anneau $\mathbb{Z}/n\mathbb{Z}$ de manière approfondie. Après avoir déterminé les éléments nilpotents et idempotents de cet anneau, on décrit explicitement la structure du groupe des éléments inversibles. On s'intéresse ensuite aux carrés de $\mathbb{Z}/n\mathbb{Z}$. Au passage, on introduit les symboles de Legendre et de Jacobi, et l'on propose une démonstration de la loi de réciprocité quadratique fondée sur le calcul modulaire. Le chapitre XVII est consacré à l'étude des propriétés arithmétiques des anneaux. On s'intéresse d'une part à la généralisation des notions de pgcd et ppcm, et d'autre part à la généralisation du théorème fondamental de l'arithmétique. Pour cela, on introduit la notion d'élément irréductible d'un anneau, et l'on étudie l'existence et l'unicité d'une factorisation d'un élément non nul en produit d'un inversible et d'éléments irréductibles, d'abord dans le cadre agréable des anneaux principaux, puis dans un cadre général. Cela conduit à la notion d'anneau factoriel. On démontre alors des analogues des résultats classiques de l'arithmétique. Au passage, on étudie brièvement les anneaux noethériens. Dans ce chapitre, on étudie aussi les anneaux euclidiens, c'est-à-dire les anneaux possédant un analogue de la division euclidienne. On généralise alors l'algorithme d'Euclide à de tels anneaux. Le chapitre XVIII est consacré à l'étude de l'équivalence de matrices à coefficients dans un anneau A (deux matrices de même taille étant équivalentes si l'on peut passer de l'une à l'autre par des opérations élémentaires sur les lignes et les colonnes). Lorsque A est euclidien, on montre que l'on peut réduire toute matrice à l'aide d'opérations élémentaires en une matrice d'une forme particulière, appelée forme normale de Smith. Après avoir brièvement introduit la notion de A-module (qui généralise de façon naturelle la notion d'espace vectoriel sur un corps), on en déduit alors une méthode systématique pour résoudre les systèmes linéaires à coefficients dans A. On montre aussi que, lorsque A est euclidien, le groupe $\mathrm{GL}_n(A)$ des éléments inversibles de l'anneau $\mathrm{M}_n(A)$ est engendré par les matrices de transvection et de dilatation. On applique aussi la théorie développée dans ce chapitre pour démontrer de manière plus élégante le théorème de structure des groupes abéliens de type fini. Nous avons choisi sciemment de passer sous silence le théorème de structure des modules de type fini sur un anneau euclidien (ou même sur un anneau principal), y compris lorsque nous parlerons de décomposition de Frobenius dans le chapitre XXIX. Le lecteur intéressé par une exposition plus complète de la théorie des modules pourra se référer à [8], ainsi qu'aux exercices. Le chapitre XIX se concentre tout particulièrement

sur les éléments irréductibles de l'anneau $A[X]$ des polynômes à coefficients dans un anneau A. On commence par souligner que cette notion est bien plus délicate que dans le cas des polynômes à coefficients dans un corps. On donne ensuite quelques critères d'irréductibilité classiques (critère de réduction modulo un idéal, critère d'Eisenstein). On montre ensuite que si A est factoriel, il en est de même de l'anneau $A[X]$. On montre ensuite les limites des critères d'irréductibilité démontrés précédemment, en exhibant une famille de polynômes de degré 4 dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$, mais qui sont réductibles modulo tout idéal de $\mathbb{Z}$. On définit ensuite une famille très importante de polynômes irréductibles de $\mathbb{Q}[X]$, à savoir les polynômes cyclotomiques. On les utilise ensuite pour démontrer une version faible du théorème de la progression arithmétique de Dirichlet, et pour démontrer que tout anneau à division fini est commutatif. Enfin, on démontre l'existence de polynômes irréductibles de tous degrés sur $\mathbb{F}_p$, et l'on élucide la structure des corps finis. On décrit enfin l'algorithme de Berlekamp, qui permet de factoriser de manière redoutablement efficace les polynômes à coefficients dans $\mathbb{F}_p$ en produit de polynômes irréductibles. Dans le chapitre XX, on s'intéresse plus particulièrement aux idéaux de l'anneau $A[X]$. On détermine en particulier sous quelles conditions ces idéaux sont de type fini/principaux. On décrit également tous les idéaux premiers et maximaux de $A[X]$ lorsque A est un anneau principal. Dans le chapitre XXI, on étudie les propriétés des séries formelles à coefficients dans un anneau A. En particulier, on définit diverses opérations sur les séries formelles comme la dérivation ou l'évaluation. On introduit ensuite quelques séries formelles usuelles et l'on donne quelques applications des séries formelles à la combinatoire. Le lecteur pourra trouver d'autres applications des séries formelles dans [3] ou [1], ainsi que dans les exercices. Enfin, dans le chapitre XXII, on définit de manière algébrique le complété d'un anneau A par rapport à un idéal I. Cette construction permet à la fois d'apporter un nouvel éclairage sur les propriétés des séries formelles, et de construire l'anneau des entiers p-adiques, un anneau extrêmement important en théorie des nombres. Au passage, on fait le lien avec la complétion d'un anneau par rapport à une distance, bien connue en topologie. La plupart des résultats traités dans cette partie peuvent se retrouver dans [1], [26] et [34]. Le lecteur désirant approfondir ses connaissances sur la théorie des nombres p-adiques pourra consulter [4] ou [25].

La quatrième partie est consacrée à la célèbre théorie de Galois. Dans le chapitre XXIII, on commence par motiver l'étude des extensions de corps en montrant comment ces objets interviennent naturellement dans un problème a priori purement géométrique, à savoir le problème de la construction à la règle et au compas. Ces considérations géométriques nous conduisent à introduire la notion d'élément algébrique sur un corps. Après avoir montré quelques résultats de théorie des extensions, nous résolvons

des problèmes classiques de construction à la règle et au compas, en particulier la construction des polygones réguliers. Nous achevons ce chapitre en expliquant comment ces constructions amènent tout naturellement à de nouvelles questions de théorie des corps, et à la nécessité de disposer d'un corps dans laquelle tout polynôme non constant de $K[X]$ se factorise en produit de polynômes de degré 1. Le chapitre XXIV rentre dans le vif du sujet, et se préoccupe de l'existence éventuelle de racines d'un polynôme non constant $P \in K[X]$ dans un corps L contenant K. Cela aboutit à la notion de corps de rupture et de corps des racines. On en déduit entre autres une nouvelle façon de démontrer l'existence de corps finis de cardinal donné. On montre également que $\mathbb{C}$ est algébriquement clos. On s'intéresse ensuite à l'existence et l'unicité d'une clôture algébrique d'un corps K. Enfin, on introduit la notion d'élément entier sur un anneau, ce qui nous permet ensuite de comparer les relations entre irréductibilité dans $A[X]$ et irréductibilité dans $K_A[X]$, où A est un anneau intègre et K_A est son corps des fractions. Le chapitre XXV étudie les extensions de corps dites séparables. On montre alors que ces extensions ont de bonnes propriétés vis-à-vis du prolongement des morphismes de corps à valeurs dans un corps algébriquement clos. Dans le chapitre XXVI, on introduit la notion d'extension galoisienne, et l'on donne quelques familles classiques d'extensions galoisiennes (extensions cyclotomiques, extensions de Kummer). Dans le chapitre XXVII, on établit une correspondance bijective entre l'ensemble des sous-extensions d'une extension galoisienne et l'ensemble des sous-groupes de son groupe d'automorphismes. On revient alors sur le problème de construction à la règle et au compas. Pour finir, on s'intéresse au problème qui est historiquement à l'origine de la théorie de Galois et de la théorie des groupes, à savoir le problème de la résolubilité d'une équation polynomiale par radicaux. Le lecteur désireux de découvrir d'autres ouvrages consacrés à la théorie de Galois pourra consulter [13], [13], [43] ou [44], ainsi que [45] pour un aspect historique complet de la question de la résolubilité des équations par radicaux et des travaux d'Évariste Galois.

La cinquième partie de cet ouvrage est essentiellement dévolue à la réduction des endomorphismes. Dans le chapitre XXVIII, après avoir introduit la notion de polynôme annulateur, on donne les critères classiques de diagonalisabilité et trigonalisabilité d'un endomorphisme, puis on s'intéresse à la décomposition de Dunford et à la réduction de Jordan. La dernière partie du chapitre est consacrée à l'étude de l'exponentielle de matrices. Le chapitre XXIX établit l'existence d'une décomposition d'un espace vectoriel V en somme directe de sous-espaces u-cycliques (où u est un endomorphisme de V). Cela conduit à la notion d'invariants de similitudes d'un endomorphisme. L'existence d'une telle décomposition est établie de deux manières, d'une part en utilisant la dualité, et d'autre part en utilisant l'algorithme

de réduction des matrices à coefficients dans l'anneau euclidien $K[X]$. On donne alors un algorithme qui permet de décider si deux endomorphismes de V donnés sont semblables ou non. On donne ensuite quelques applications de la décomposition de Frobenius à l'étude du commutant et du bicommutant d'un endomorphisme. Enfin, dans le chapitre XXX, on étudie la dualité en dimension quelconque. Plus précisément, étant donné une application bilinéaire $b : E \times F \longrightarrow K$, on donne des conditions nécessaires et suffisantes pour l'on ait une correspondance bijective entre les sous-espaces de E et ceux de F (via les sous-espaces orthogonaux à gauche et à droite relatifs à b). On étudie également l'existence de bases duales et d'endomorphismes adjoints. Les résultats sur la réduction des endomorphismes sont de grands classiques, et peuvent être retrouvés un peu partout dans la littérature, comme par exemple [1] ou [7]. Le lecteur retrouvera certains résultats du chapitre sur la dualité dans [5].

Enfin, la sixième et dernière partie de ce livre fournit une introduction à la théorie des représentations linéaires des groupes finis. Le chapitre XXXI introduit la notion de représentation linéaire d'un groupe fini sur un corps K, ainsi que la notion importante de représentation irréductible. On définit ensuite plusieurs opérations sur les représentations linéaires (somme, produit tensoriel, carrés symétrique et alterné, etc.). On montre alors que, sous certaines hypothèses, toute représentation linéaire se décompose en somme directe de sous-représentations irréductibles. L'ultime chapitre XXXII expose la théorie des caractères, qui est le cœur de la théorie des représentations. On démontre, entre autres, que lorsque K est un corps algébriquement clos de caractéristique nulle, le caractère d'une représentation la caractérise à isomorphisme près. On démontre également (sous les mêmes hypothèses) certaines relations d'orthogonalité entre les caractères des représentations irréductibles. On donne aussi quelques applications de la théorie des caractères à la théorie des groupes, dont le théorème $p^a q^b$ de Burnside. On fournit enfin quelques résultats sur le degré des représentations irréductibles, ainsi qu'une méthode explicite pour décomposer une représentation donnée en somme directe de sous-représentations irréductibles. Nous n'avons pas abordé la notion de représentation induite, notion très importante pour construire des représentations irréductibles via le critère de Mackey. Le lecteur désireux d'approfondir ce sujet pourra consulter [2], [17], [31], [35] ou [41]. Un autre thème intéressant est la détermination des représentations irréductibles du groupe symétrique. Le lecteur intéressé pourra se référer aux ouvrages [2], [31] ou [35] pour de plus amples renseignements. Tous les résultats de cette partie peuvent se retrouver dans les références mentionnées ci-dessus.

Notons également que la majeure partie du contenu de cet ouvrage peut être retrouvée dans [6], [17], [26], [30] ou [34].

Chaque chapitre s'achève par une série d'exercices de niveaux variés. En ce qui concerne les chapitres mélangeant plusieurs niveaux, les exercices nécessitant une connaissance des sections spécifiques au niveau M1 ou Agreg [4] seront signalés. Nous encourageons le lecteur à essayer de les résoudre, quitte à sécher dessus un bon moment en ce qui concerne les exercices un peu plus difficiles, car comme disait Paul Langevin : « le concret, c'est de l'abstrait rendu familier par l'usage ».

Quelques conseils pour travailler son cours.–

Les conseils qui suivent sont évidemment valables pour n'importe quel cours, qu'ils soit suivi en amphi ou qu'il soit étudié en autodidacte à l'aide d'un livre. Chaque étudiant est bien entendu différent, et il n'y a pas de recette universelle pour maîtriser un cours de mathématiques. Néanmoins, il y a quand même quelques conseils frappés au coin du bon sens [5] qui peuvent faciliter l'apprentissage.

(1) S'aménager des conditions de travail propices (que ce soit seul ou en groupe) : couper télé, radio, téléphone portable, internet, afin de pouvoir mieux se concentrer.

(2) Apprendre les définitions et les théorèmes principaux à la virgule près (chaque mot et l'ordre de chaque mot ayant son importance dans un énoncé mathématique). Connaître les exemples classiques des objets que l'on a défini.

(3) Savoir faire les exercices d'application directe du cours.

(4) S'attaquer aux exercices moins évidents, quitte à sécher dessus un bon moment. On apprend les maths en les faisant (et l'on éprouve généralement une grande satisfaction personnelle lorsque l'on trouve finalement). Il est absolument inefficace d'abandonner au bout de dix minutes. Pour progresser, il faut être patient et tenace.

(5) Une fois cela fait, et seulement à ce moment-là, on peut reprendre chaque énoncé important du cours et essayer de répondre (dans la mesure du possible) aux questions suivantes : pourquoi a-t-on fait telle ou telle hypothèse ? Où intervient-elle dans la démonstration ? Le résultat est-il encore vrai si l'on affaiblit les hypothèses, ou si l'on en enlève ? Si ce n'est pas le cas, peut-on produire un contre-exemple ?

C'est très bien pour comprendre les choses en profondeur.

(6) Si possible, essayer de comprendre les étapes essentielles et l'articulation d'une démonstration d'un théorème important. Savoir refaire une démonstration courte.

4. Suivant le découpage présenté plus haut.
5. Tout du moins selon l'auteur...

Il faut prendre conscience que l'on ne peut pas tout comprendre à fond sur le moment, et accepter que l'on puisse ne pas maîtriser une démonstration tout de suite. Il faut parfois un an de recul sur une notion pour vraiment la digérer.

(7) Souvent, quand on lit une démonstration du cours ou la solution d'un exercice, on a le sentiment d'avoir bien compris. Il faut savoir que neuf fois sur dix, il n'en est rien. Pour voir si c'est vraiment le cas, nous conseillons au lecteur d'essayer de ré-expliquer la dite démonstration ou solution à des collègues. C'est un test qui ne trompe pas : s'il y avait des points obscurs ou doutes, cela se ressentira lors de la tentative d'explication. Comme on dit souvent : ce qui se conçoit bien s'énonce clairement.

Comment aborder un exercice.–

Enfonçons le clou : on apprend les maths en les faisant, et en se trompant, et certainement pas en lisant linéairement un ouvrage, une page Web ou une solution rédigée d'exercice. Voici quelques principes de base pour éviter de rester bloqué devant un exercice.

(1) Lire l'énoncé en entier pour identifier le but de l'exercice [6].

(2) Identifier de quoi ça parle, et lister les théorèmes à disposition sur le sujet.

(3) Repérer les hypothèses, ainsi que les mots du style « en déduire ». Cela donne une bonne indication sur la manière de procéder.

(4) Lorsque que l'on doit faire une démonstration, ne pas hésiter à écrire les hypothèses, et la conclusion, pour visualiser d'où l'on part et où l'on veut arriver. Cela aide souvent pour savoir comment démarrer.

(5) Lorsque l'on rédige une démonstration, il faut savoir justifier chaque étape. Si ce n'est pas le cas, c'est qu'il y a un problème...

(6) Bien faire apparaître où l'on utilise les hypothèses de l'énoncé dans la rédaction d'une démonstration. Si une hypothèse n'est pas utilisée, il y a deux possibilités : soit l'énoncé est mal fait (ce qui peut arriver), soit il y a une ou plusieurs erreurs dans la démonstration en question (ce qui est le cas le plus probable).

(7) Se forcer à bien rédiger et à écrire des phrases mathématiquement complètes et grammaticalement correctes, **même au brouillon.** Il est extrêmement facile de prendre de mauvaises habitudes de rédaction.

6. Dit comme ça, le conseil a l'air complètement idiot, mais c'est en fait vital pour ne pas perdre de vue le but final !

Parmi les principes de bonne rédaction, on peut citer : ne pas utiliser d'abréviation, ne pas mélanger symboles mathématiques et français, n'écrire un signe « $\Longleftrightarrow$ » que si l'on est certain d'avoir une équivalence logique, dire où l'on utilise les hypothèses, vérifier que l'on n'utilise pas la conclusion souhaitée pour la démontrer, etc.

(8) Faire des exercices dont on ne dispose pas du corrigé, pour ne pas être tenté d'aller y jeter un coup d'œil [7].

(9) Comme déjà évoqué précédemment, essayer d'expliquer sa proposition de solution d'un exercice à des collègues permet de déceler des erreurs ou des points mal rédigés.

Remerciements.–

L'idée d'écrire cet ouvrage m'est venue lorsque j'ai eu vent à plusieurs reprises que certains de mes anciens étudiants utilisaient encore mes polycopiés de cours de L3 et de M1 pour préparer l'agrégation de mathématiques, mais qu'ils n'étaient hélas pas autorisés à utiliser les dits polycopiés pour passer leurs épreuves orales. Je les remercie donc pour m'avoir encouragé directement ou indirectement à entreprendre cette trèèèèès longue entreprise de rédaction. Merci aussi à toutes mes victimes estudiantines, dont les commentaires m'ont permis d'améliorer mes cours au fil des années. Je tiens aussi à remercier tous mes relecteurs. Sans leurs conseils avisés et leurs suggestions pertinentes, cet ouvrage ne serait pas ce qu'il est [8]. Merci donc à Vincent Beck, Alain Debreil, Christophe Derras, Sébastien Gerekens, Éloi Mehr, Éric Pite, Étienne Rousée et Rémi Saint-Romain.

Enfin, merci du fond du cœur à Alain Debreil, Rached Mneimné et à toute l'équipe de C&M pour le travail éditorial titanesque qu'ils ont accompli avec courage et abnégation, ainsi que pour leur patience d'ange face à mes caprices d'auteur.

Cette deuxième édition a été l'occasion de quelques ajouts et autres corrections, et d'une amélioration sensible de la mise en page.

7. Cela tombe bien, dans cet ouvrage, aucune correction n'est donnée : cela ne sert à rien, et ce n'est pas rentable.

8. En particulier, il n'y aurait pas eu de chapitres sur la complétion I-adique, ou sur la théorie de Galois.