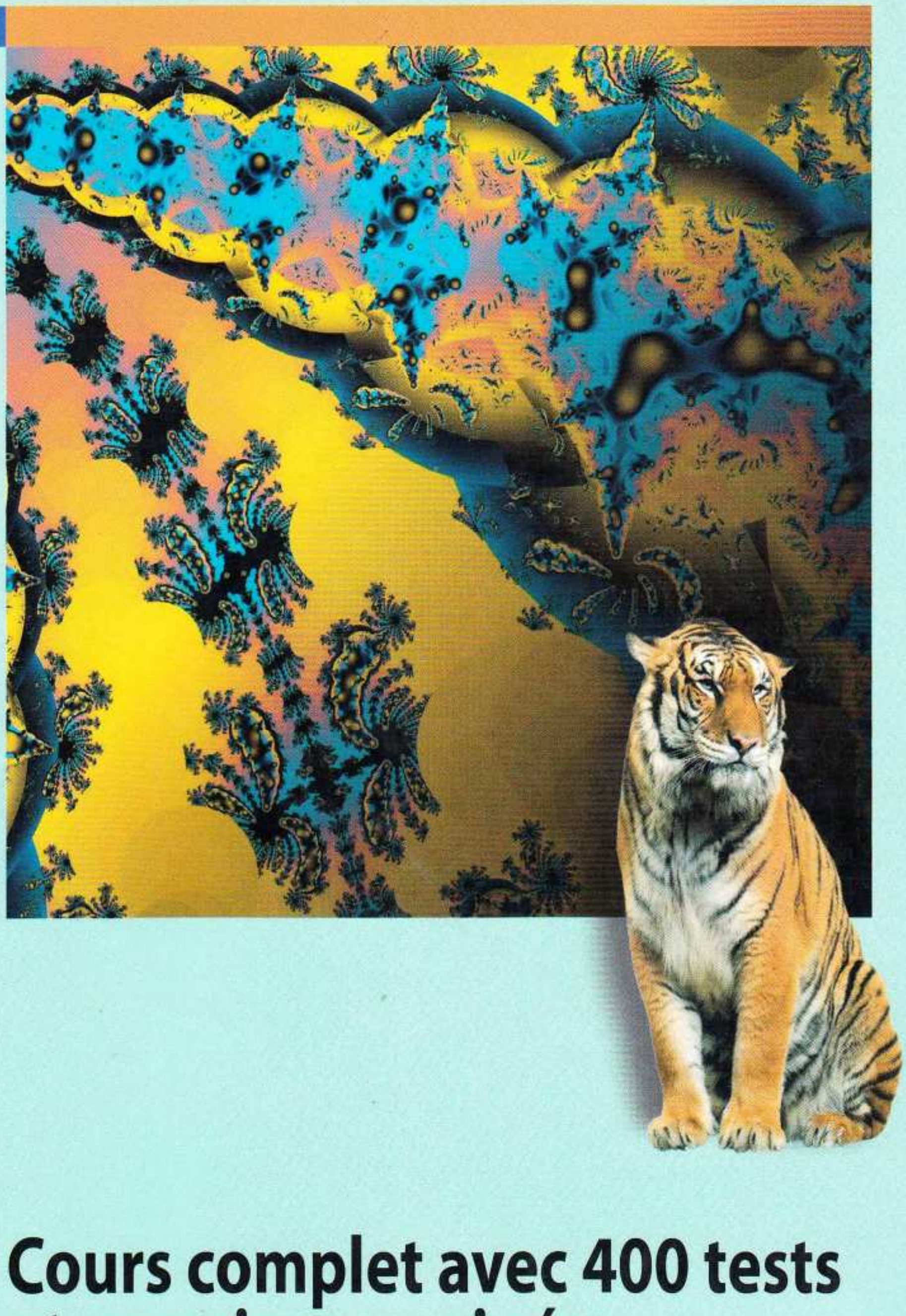
Mathématiques L3
Algèbre

Sous la direction de
Aviva Szpirglas

François Arnault
Gilles Bailly-Maitre
Yves Benjamin
Philippe du Bois
Lionel Ducos
Aurélien Galateau
Henri Lombardi
Cécile Poirier
Claude Quitté
Maxime Rebout
Matthieu Romagny
Julien Roques



CURSUS LMD

Cours complet avec 400 tests
et exercices corrigés

PEARSON
Education

Table des matières

Les auteurs iii

Avant-propos xv

Présentation xvi

Remerciements xviii

Partie I – Ensembles, cardinalité 1

1 Ensembles 3

I Rappels et quelques compléments . . . 3

I.1 Parties . . . 3

I.2 Relations . . . 4

I.3 Fonctions . . . 5

I.4 Familles et produits . . . 5

I.5 Peut-on tout faire avec des ensembles ? . . . 5

II Ensembles ordonnés . . . 6

II.1 Relations d'ordre . . . 6

II.2 Ordres sur $\mathbb{N} \times \mathbb{N}$ . . . 7

II.3 Bornes et éléments extrémaux . . . 8

II.4 Segments . . . 9

II.5 Homomorphismes d'ensembles ordonnés . . . 10

II.6 Bons ordres . . . 10

II.7 Récurrence transfinie . . . 12

III Exercices . . . 13

2 Axiomes, cardinaux 15

I Théorie axiomatique - Zermelo-Fraenkel . . . 15

I.1 Les axiomes (presque) simples . . . 15

I.2 Les axiomes techniques . . . 16

I.3 Conséquences . . . 17

I.4 Entiers naturels . . . 17

I.5 Classes ou ensembles . . . 18

I.6 Les axiomes facultatifs . . . 18

I.7 Hypothèses équivalentes à l'axiome du choix . . . 19

II Cardinaux . . . 21

II.1 Théorème de comparabilité . . . 21
II.2 Équipotence . . . 23
II.3 Ensembles dénombrables . . . 25
II.4 Ensembles non dénombrables . . . 28
II.5 Arithmétique cardinale . . . 28
III Exercices . . . 29
Complément Les ordinaux . . . 31

Partie II – Plus d'algèbre linéaire et de géométrie **37**

3 Algèbre bilinéaire **39**
I Applications et formes bilinéaires . . . 42
I.1 Généralités . . . 42
I.2 Dualité . . . 47
I.3 Orthogonalité . . . 54
I.4 Isotropie . . . 60
I.5 Sous-espaces totalement isotropes maximaux . . . 64
I.6 Adjoint d'un endomorphisme . . . 64
II Formes symétriques et formes quadratiques . . . 67
II.1 Définitions associées aux formes symétriques et premières propriétés . . . 67
II.2 Endomorphismes particuliers . . . 75
II.3 Classification des formes quadratiques . . . 79
III Formes sesquilinéaires et hermitiennes . . . 84
III.1 Généralités . . . 85
III.2 Formes à symétrie hermitienne et formes quadratiques hermitiennes . . . 86
IV Exercices . . . 90
Complément 1 Théorème de Witt . . . 92
Complément 2 Formes antisymétriques – Matrices symplectiques . . . 96

4 Géométrie affine **103**
I Compléments de géométrie . . . 104
I.1 Rappels . . . 104
I.2 Compléments sur les barycentres . . . 108
I.3 Compléments sur les applications affines . . . 111
I.4 Topologie d'un espace affine réel de dimension finie . . . 113
I.5 Hyperplans affines et demi-espaces . . . 115
I.6 Compléments de géométrie euclidienne . . . 118

II Convexité 120
II.1 Ensembles convexes 120
II.2 Enveloppe convexe 122
II.3 Intérieur et adhérence 126
II.4 Hyperplan d'appui et projection 128
II.5 Points extrémaux 131
II.6 Fonctions convexes 133
II.7 Application de la convexité au théorème de Jung 135
II.8 Polyèdres convexes 136
III Exercices 149
Complément 1 Matrices bistochastiques 151
Complément 2 Théorème de Morley 156

5 Géométrie projective **159**
I Espace vectoriel engendré par un espace affine 159
II Espaces projectifs 162
II.1 Espaces projectifs et applications projectives 162
II.2 Droite projective et birapport 168
II.3 Dualité 171
II.4 Quadrilatère complet, théorèmes de Pappus et de Desargues 174
II.5 Complexification 177
II.6 Structure euclidienne 179
III Coniques projectives 181
III.1 Coniques projectives complexes 182
III.2 Coniques projectives sur un corps quelconque 184
III.3 Tangentes aux coniques propres 187
III.4 Pôles et polaires 189
III.5 Classification des coniques affines réelles propres 195
IV Exercices 198
Complément 1 Géométrie plane elliptique 201
Complément 2 Géométrie plane hyperbolique 203
Complément 3 Droite projective complexe – Groupe circulaire – Inversion 211

Partie III – Groupes **215**

6 Théorie des groupes **217**
I Généralités sur les groupes 218

I.1 Définition d'un groupe 218
I.2 Sous-groupes 220
I.3 Morphismes de groupes 222
I.4 Isomorphismes de groupes, automorphismes 224
I.5 Sous-groupe engendré par une partie 225
II Sous-groupes distingués et groupes quotients 226
II.1 Classes à gauche, classes à droite 227
II.2 Sous-groupes distingués et groupe quotient 228
II.3 Centre et groupe dérivé 230
II.4 Sous-groupes du quotient et théorèmes d'isomorphisme 231
III Génération de groupes 233
III.1 Groupes monogènes, groupes cycliques 233
III.2 Groupes libres 234
III.3 Présentation d'un groupe 236
IV Action d'un groupe sur un ensemble 237
IV.1 Définitions 237
IV.2 Exemples : groupe symétrique et action d'un groupe sur lui-même 239
IV.3 Équation aux classes et formule de Burnside 240
V Produits de groupes 243
V.1 Produits directs 243
V.2 Produits semi-directs 245
V.3 Critère de dévissage 246
VI Groupes abéliens de type fini 249
VI.1 Structure des groupes abéliens de type fini 249
VI.2 Automorphismes des groupes cycliques 256
VI.3 Sous-groupes discrets de $\mathbb{R}^n$ 259
VII Le groupe symétrique 263
VII.1 Propriétés élémentaires du groupe symétrique 264
VII.2 Le groupe alterné 266
VII.3 Automorphismes de $\mathfrak{S}_n$ 270
VIII Sous-groupes de Sylow 272
VIII.1 Sous-groupes de Sylow 272
VIII.2 Les théorèmes de Sylow 273
VIII.3 Quelques applications et compléments 275
IX Exercices 279
Complément 1 Algorithme de Todd-Coxeter 281
Complément 2 Géométrie diophantienne 286

7 **Groupes et algèbre linéaire** **293**
I Le groupe linéaire . . . 294
I.1 Définitions et caractérisation . . . 294
I.2 Le groupe spécial linéaire . . . 296
I.3 Générateurs . . . 297
I.4 Centre et commutateurs . . . 301
I.5 Propriétés de groupes . . . 308
I.6 Topologie du groupe linéaire . . . 310
II Groupe orthogonal . . . 314
II.1 Groupe orthogonal général . . . 314
II.2 L'espace euclidien canonique . . . 323
III Groupe unitaire . . . 337
III.1 Cas général . . . 337
III.2 Le groupe unitaire canonique . . . 340
IV Décompositions du groupe linéaire . . . 341
IV.1 Décomposition de Dunford . . . 341
IV.2 Décomposition polaire . . . 342
IV.3 Décomposition d'Iwasawa . . . 347
V Exercices . . . 348
Complément 1 À propos de l'exponentielle . . . 349
Complément 2 Empilement optimal de disques dans le plan . . . 366
Complément 3 Action de $\mathsf{PSL}_2(\mathbb{Z})$ sur le demi-plan de Poincaré . . . 372
Complément 4 Le groupe symplectique . . . 380

8 **Groupes et géométrie** **385**
I Le groupe affine . . . 385
I.1 Généralités, rappels . . . 386
I.2 Le groupe des homothéties-translations . . . 387
II Le groupe des isométries . . . 389
II.1 Généralités . . . 389
II.2 Les isométries planes . . . 395
II.3 Les isométries de l'espace . . . 398
II.4 Image d'une partie par une isométrie . . . 404
II.5 Isométries conservant une partie . . . 406
II.6 Sous-groupes finis de $\mathrm{Is}(\mathcal{E})$ . . . 408
III Les polytopes réguliers de l'espace et leurs groupes de rotation . . . 414
III.1 Généralités sur les polytopes réguliers . . . 414
III.2 Classification des polytopes réguliers à similitude près . . . 418

III.3 Le tétraèdre régulier et son groupe d'isométries 421
III.4 Le cube et son groupe d'isométries 422
III.5 L'octaèdre régulier et son groupe de rotations 425
III.6 L'icosaèdre régulier et son groupe de rotations 426
III.7 Le dodécaèdre régulier et son groupe de rotations 432
III.8 Les sous-groupes finis de SO_3 434
IV Exercices 437
Complément 1 Dual d'un convexe, d'un polyèdre 439
Complément 2 Groupes de frise 446

Partie IV – Anneaux et modules **455**

9 Anneaux **457**
I Rappels 458
I.1 Notations, exemples fondamentaux 458
I.2 Idéaux 460
I.3 Morphismes d'anneaux 460
I.4 Anneaux quotients 461
I.5 Arithmétique 462
II Ces êtres étranges qui vivent dans les anneaux 462
II.1 Éléments centraux 463
II.2 Diviseurs de zéro 464
II.3 Éléments réguliers 465
II.4 Éléments nilpotents 467
II.5 Caractéristique d'un anneau 467
II.6 Éléments irréductibles 468
III Étude des idéaux 470
III.1 Opérations entre idéaux 471
III.2 Générateurs d'un idéal 472
III.3 Idéaux des anneaux euclidiens 474
III.4 Arithmétique des idéaux 477
III.5 Radical d'un idéal 484
III.6 Idéaux maximaux 486
III.7 Idéaux premiers 487
III.8 Idéaux de $A/\mathcal{I}$ 489
IV Corps des fractions 491
IV.1 Construction 492

IV.2 Propriétés . . . 493
V Localisation . . . 494
VI Anneaux noethériens . . . 498
VI.1 Définitions équivalentes . . . 498
VI.2 Fabrication d'anneaux noethériens . . . 499
VI.3 Anneaux artiniens . . . 501
VII Arithmétique . . . 502
VII.1 Irréductibles ou premiers ? . . . 503
VII.2 Pgcd-ppcm . . . 504
VII.3 Éléments premiers entre eux . . . 505
VII.4 Anneaux à pgcd . . . 506
VII.5 Anneaux de Bézout . . . 510
VII.6 Anneaux factoriels . . . 511
VII.7 Anneaux de Bézout factoriels ? . . . 516
VIII Quelques conséquences amusantes . . . 517
VIII.1 L'équation $x^2 + y^2 = z^2$ . . . 517
VIII.2 L'équation $x^4 + y^4 = z^4$ . . . 518
VIII.3 Les sommes de deux carrés . . . 519
VIII.4 L' anneau $\mathbb{Z}\left[i\sqrt{d}\right]$ . . . 520
IX Exercices . . . 521
Complément Les nombres presque premiers . . . 523

10 Polynômes **533**
I Polynômes à une indéterminée . . . 534
I.1 Polynômes à coefficients dans un anneau . . . 534
I.2 Polynômes à coefficients dans un corps . . . 535
I.3 Polynômes à coefficients dans un anneau factoriel . . . 547
I.4 Critères d'irréductibilité des polynômes . . . 549
II Polynômes à plusieurs indéterminées . . . 554
II.1 Algèbre $A[X_1, \ldots, X_n]$ . . . 554
II.2 Formules d'Euler et de Taylor . . . 557
III Polynômes symétriques . . . 558
III.1 Relations entre coefficients et racines . . . 559
III.2 Théorème de structure . . . 559
III.3 Sommes de Newton . . . 561
IV Élimination . . . 563
IV.1 Résultant de deux polynômes . . . 564
IV.2 Applications algébriques du résultant . . . 567

V Fractions rationnelles 576
V.1 Corps $\mathsf{K}(\mathsf{X})$ des fractions rationnelles 576
V.2 Décomposition en éléments simples 578
V.3 Applications de la décomposition en éléments simples 583
V.4 Déterminants de Hankel 585
VI Exercices 586
Complément 1 Application géométrique du résultant 588
Complément 2 Sous-variétés algébriques de $\mathbb{C}^n$ et idéaux de $\mathbb{C}[\mathsf{X}_1, \ldots, \mathsf{X}_n]$ 596
Complément 3 Polynômes cyclotomiques 599
Complément 4 Polynômes invariants sous le groupe alterné 602
Complément 5 Groupe des K-automorphismes de $\mathsf{K}(\mathsf{X})$ 607

11 Modules **609**
I Quelques bases pour fixer les idées 609
I.1 Définition 610
I.2 Petit tour d'horizon 611
I.3 Morphismes 612
II Sous-modules 613
III Modules quotients 614
IV Modules de type fini 616
V Modules noethériens 619
VI Opérations sur les sous-modules 620
VII Torsion 624
VIII Modules libres 625
VIII.1 Familles libres 625
VIII.2 Bases 626
IX Modules libres et de type fini 629
IX.1 Déterminant 629
IX.2 Structure des modules libres de type fini 633
IX.3 Endomorphismes de A^n 635
X Modules sur un anneau principal 637
X.1 Généralités et première décomposition 637
X.2 Décomposition des modules de torsion 640
X.3 Théorème de la base adaptée 647
XI Applications 652
XI.1 Structure des groupes commutatifs de type fini 652
XI.2 Invariants de similitude 653

XII Exercices 657
Complément 1 Idéaux inversibles – Anneaux de Dedekind 659
Complément 2 Principe local-global 679
Complément 3 Vision des mathématiques constructives sur les modules 695

Partie V – Éléments de théorie des corps **709**

12 Corps **711**

I Extensions de corps 713
I.1 Nombres algébriques – Nombres transcendants 714
I.2 Extensions algébriques 716
I.3 Extensions transcendantes 717
I.4 Corps de rupture 718
II Utilisation de l'algèbre linéaire 719
II.1 Degré d'une extension 719
II.2 Constructions à la règle et au compas 722
II.3 Corps de décomposition – Extensions normales – Extensions séparables . 727
III Utilisation de la théorie des groupes 732
III.1 Automorphismes de corps – Groupe de Galois 733
III.2 Résolution par radicaux 738
IV Clôture algébrique de $\mathbb{Q}$ 745
V Exercices 746
Complément Correspondance de Galois 748

13 Corps finis **759**

I Clôture algébrique de $\mathbb{F}_p$ 759
II Existence et unicité du corps à p^n éléments 760
II.1 Unicité à isomorphisme près du corps à p^n éléments 760
II.2 Existence du corps à p^n éléments 761
II.3 Groupe multiplicatif du corps à p^n éléments 761
III Sous-corps de $\mathbb{F}_{p^n}$ 763
III.1 Sous-corps et extensions 763
III.2 Automorphismes des corps finis 763
III.3 Nouvelle construction de la clôture algébrique de $\mathbb{F}_p$ 764
IV Polynômes irréductibles de $\mathbb{F}_p[X]$ 764
IV.1 Existence d'un polynôme irréductible de degré n dans $\mathbb{F}_p[X]$ 765
IV.2 Corps finis *via* la caractéristique nulle 766
IV.3 Dénombrement des polynômes irréductibles 766

IV.4 Exemples de corps finis . . . 767
V Polygones réguliers constructibles à la règle et au compas . . . 768
VI Théorème de Wedderburn . . . 773
VII Exercices . . . 775
Complément Quaternions . . . 777

Partie VI – Solutions des tests **783**

Partie VII – Solutions des exercices **795**

Bibliographie **823**

Index général **825**

Index des notations **833**