MATHÉMATIQUES

2e cycle

Cours et exercices corrigés

Collection dirigée par

Charles-Michel Marle

Philippe Pilibossian

Algèbre et théorie des nombres

Cryptographie
Primalité

Sabah Al Fakir

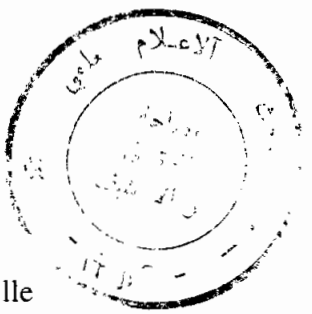
ellipses

MATHÉMATIQUES POUR LE 2E CYCLE

Collection dirigée par Charles-Michel MARLE et Philippe PILIBOSSIAN

ALGÈBRE ET THÉORIE DES NOMBRES

Cryptographie – Primalité



Sabah AL FAKIR

Professeur émérité

Université scientifique et technique de Lille

ellipses

Dans la même collection *Mathématiques pour le 2e cycle*

- *Algèbre et théorie des nombres. Cryptographie - Primalité*, Sabah Al Fakir, 288 pages.
- *Algèbre linéaire*, Francette Bories-Longuet, 160 pages.
- *Algèbre linéaire numérique. Cours et exercices*, Grégoire Allaire et Sidi Mahmoud Kaber, 256 pages.
- *Analyse complexe et distributions*, Alain Yger, 400 pages.
- *Calcul différentiel*, Gilles Christol, Anne Cot, Charles-Michel Marle, 224 pages.
- *Cours d'algèbre*, Renée Elkik, 192 pages.
- *Cours de calcul formel. Algorithmes fondamentaux*, Philippe Saux Picart, 192 pages.
- *Cours de calcul formel. Corps finis - Systèmes polynomiaux - Applications*, Philippe Saux Picart et Érie Rannou, 224 pages.
- *Distributions - Espaces de Sobolev, Applications*, Marie-Thérèse Lacroix-Sonrier, 160 pages.
- *Éléments d'analyse convexe et variationnelle*, Dominique Azé, 240 pages.
- *Éléments d'intégration et d'analyse fonctionnelle*, Aziz El Kacimi Alaoui, 256 pages.
- *Géométrie différentielle avec 80 figures*, Catherine Doss-Bachelet, Jean-Pierre Françoise et Claude Piquet, 208 pages.
- *Intégration et théorie de la mesure - Une approche géométrique*, Paul Krée, 240 pages.
- *Introduction à Scilab. Exercices pratiques corrigés d'algèbre linéaire*, Grégoire Allaire et Sidi Mahmoud Kaber, 240 pages.
- *Les groupes finis et leurs représentations*, Gérard Rauch, 192 pages.
- *Logique, ensemble, catégories. Le point de vue constructif*, Pierre Ageron, 128 pages.
- *Précis d'analyse réelle. Topologie - Calcul différentiel - Méthodes d'approximations*, vol. 1, Vilmos Komornik, 208 pages.
- *Précis d'analyse réelle. Analyse fonctionnelle - Intégrale de Lebesgue - Espaces fonctionnels*, vol. 2, Vilmos Komornik, 256 pages.
- *Quelques aspects des mathématiques actuelles*, ouvrage collectif, 256 pages.
- *Théorie de Galois*, Ivan Gozard, 224 pages.
- *Topologie*, Gilles Christol, Anne Cot, Charles-Michel Marle, 192 pages.

ISBN 2-7298-1480-9

Présentation de la Collection

Mathématiques pour le deuxième cycle

Depuis 1997, cette collection se propose de mettre à la disposition des étudiants de licence et de maîtrise de mathématiques des ouvrages couvrant l'essentiel des programmes actuels des universités françaises. Certains de ces ouvrages pourront être utiles aussi aux étudiants qui préparent le CAPES ou l'agrégation, ainsi qu'aux élèves des grandes écoles.

Nous avons voulu rendre ces livres accessibles à tous : les sujets traités sont présentés de manière simple et progressive, tout en respectant scrupuleusement la rigueur mathématique. Chaque volume comporte un exposé du cours avec des démonstrations détaillées de tous les résultats essentiels, des énoncés d'exercices et leurs solutions.

L'Algèbre et la Théorie des Nombres ont une place privilégiée en mathématiques : ces théories, proches de fondements, étudient des objets et des opérations qui apparaissent, sous des réalisations diverses, dans toutes les branches des mathématiques. Monsieur Sabah Al Fakir leur consacre un ouvrage en deux tomes, dans lequel il a su placer sa très grande expérience de l'enseignement. Il a mis l'accent sur les méthodes effectives, qui permettent la construction explicite des objets dont on prouve l'existence. Certaines applications pratiques importantes, notamment à la cryptographie et aux codes correcteurs d'erreurs, sont également présentées. Nul doute que cet ouvrage, que nous sommes heureux d'acueillir dans notre collection, rendra de grands services tant aux étudiants qu'aux chercheurs.

Charles–Michel Marle — Philippe Pilibossian

À Antoine, Camille et Julien.

Avant–propos

Ce livre est issu de plusieurs années d'enseignement des modules d'Algèbre et de Théorie des nombres en Licence et Maîtrise à l'Université Scientifique de Lille. Il est destiné aux étudiants du second cycle, ainsi qu'aux candidats aux concours du Capes et de l'Agrégation. Des impératifs de volume ont imposé de le diviser en deux tomes, le premier étant plutôt destiné aux étudiants en Licence et Capes et le second à ceux de la Maîtrise et aux agrégatifs.

La tendance actuelle, qui rejoint les préoccupations des mathématiciens du XVIIIème et XIXème siècle est de se soucier du caractère effectif ou constructif des résultats et méthodes, par exemple de ne pas se contenter de prouver l'existence d'un objet mais aussi de l'exhiber quand c'est possible.

Cette politique a un coût qui se mesure en approfondissement notable des théories, les algorithmes de calcul pratique étant souvent issus de résultats profonds.

Nous avons l'avantage par rapport aux prédécesseurs de disposer de logiciels de calcul formel performants. Nous avons privilégié le logiciel *Maple*, plus accessible que *Mathematica* ou *Pari*. Ainsi, en fin de chapitre, nous signalons des commandes *Maple* qui réalisent des calculs et algorithmes expliqués dans le chapitre.

Ce livre traite en majeure partie de la théorie algébrique des nombres et de ses applications à la cryptographie et au codage correcteur d'erreurs. Nous n'avons cependant pas résisté au plaisir d'introduire le lecteur à la beauté des méthodes analytiques et transcendantes.

Notre méthode a été d'aller du particulier au général. Ainsi, la manipulation des entiers et les problèmes qui en résultent ou qui sont légués par les anciens motivent les structures introduites. Par exemple, la caractérisation des entiers qui sont la somme de deux carrés conduit à l'adjonction du nombre i à $\mathbb{Z}$, les équations de Fermat, à l'adjonction des racines de l'unité. La généralisation de cette méthode aboutit à la théorie des extensions algébriques et aux anneaux d'entiers algébriques.

Les solutions des exercices proposés en fin de chapitre sont reportées à la fin de chaque tome. Nous recommandons aux étudiants de consacrer un temps suffisant à la résolution personnelle de ces exercices.

Introduction au tome premier

Le premier chapitre porte en exergue la phrase fameuse de Kronecker « *Dieu créa les entiers naturels ; tout le reste est l'œuvre de l'homme* ». Dans ce chapitre, nous voulons prouver la justesse de cette phrase. A partir d'un ensemble $\mathbb{N}$ satisfaisant les axiomes de Peano-Dedekind, nous définissons les opérations sur $\mathbb{N}$ et construisons les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$, respectivement ensemble des entiers relatifs, ensemble des nombres rationnels, ensemble des nombres réels et ensemble des nombres complexes. Chemin faisant, nous introduisons les structures algébriques fondamentales que sont les monoïdes, les groupes, les anneaux et les corps, ainsi que la notion moderne de catégories, qui vise à unifier des constructions et définitions données dans des branches diverses des mathématiques. Nous étudions l'arithmétique de $\mathbb{Z}$ et de $\mathbb{Q}$. Finalement, une note historique détaillée introduit aux problèmes qui sont sans doute à l'origine des théories algébrique et analytique des nombres, comme les problèmes anciens de constructions à la règle et au compas, les équations de Fermat et le problème des nombres congruents.

Dans le second chapitre, nous "manipulons" les nombres premiers, un peu comme un physicien expérimente en laboratoire pour tirer des conjectures. C'est ce qui nous conduit

à étudier la répartition des nombres premiers et à développer les outils que sont les fonctions arithmétiques, notamment la fonction Zêta de Riemann et le produit de convolution de ces fonctions.

Les troisième et quatrième chapitres portent respectivement les titres de *Bases de l'Algèbre* et *Bases de l'Arithmétique*, même si dans la pratique il est impossible de séparer algèbre, arithmétique et même analyse. Le troisième chapitre comporte grosso-modo quatre parties. La première traite de la théorie des groupes, des groupes quotients, des théorèmes d'isomorphisme et d'un critère de cyclicité des groupes finis. La deuxième partie traite des anneaux commutatifs, du spectre, des anneaux quotients, des anneaux de fractions, de la structure des groupes des unités des anneaux quotients de $\mathbb{Z}$ et du Théorème chinois. La troisième partie s'occupe des anneaux de polynômes à une ou plusieurs variables, des polynômes homogènes et symétriques, et des applications à la géométrie algébrique. La quatrième partie traite des modules, des modules et anneaux nœthériens. Nous y démontrons le théorème de la base de Hilbert qui dit que si un anneau A est nœthérien, il en est de même de l'anneau $A[X]$. Pour cela, nous utilisons la notion de bases de Gröbner, convenablement étendue.

Dans le quatrième chapitre, nous comparons entre elles les propriétés d'un anneau d'être euclidien, principal ou factoriel et introduisons la notion de dimension. La caractérisation des entiers qui sont la somme de deux carrés nous conduit à étudier l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, à démontrer sa factorialité, ainsi qu'à étudier le comportement des nombres premiers de $\mathbb{Z}$ dans $\mathbb{Z}[i]$, problèmes que nous rencontrerons dans les anneaux des entiers algébriques des corps de nombres. De ces problèmes, nous sommes tout naturellement amenés à étudier les symboles de Legendre-Jacobi, la loi de réciprocité quadratique et la détermination des racines carrées d'un nombre modulo un nombre premier. Nous démontrons finalement que tout entier positif est la somme de quatre carrés.

Le chapitre 5 s'occupe de la structure des modules de type fini sur les anneaux principaux. Nous y démontrons le théorème de la base adaptée par deux méthodes, l'une abstraite utilisant l'axiome de choix et l'autre constructive utilisant la réduction des matrices à certaines formes désignées, à l'aide des opérations dites élémentaires. Nous obtenons, comme applications, la structure des groupes abéliens de type fini et la réduction des matrices à la forme de Jordan (entre autres).

Dans le chapitre 6, nous jetons les fondations de la procédure consistant à adjoindre un élément satisfaisant une équation algébrique. Nous obtenons la classification des éléments d'une extension d'un corps en éléments algébriques et transcendants, et la classification des premiers par leur degré. Nous prouvons également l'existence des clôtures algébriques et intégrales, et le théorème de l'élément primitif. Enfin, nous appliquons ces résultats généraux à l'étude des corps finis et à la factorisation des polynômes sur ces corps.

Ces résultats sont exploités dans le chapitre 7 pour caractériser les points du plan complexe qui sont constructibles à la règle et au compas à partir du réseau des points entiers. Nous en déduisons l'impossibilité des problèmes anciens : la duplication du cube, la trisection d'un angle et la quadrature du cercle.

Le chapitre 8 comporte deux parties. La première traite de la théorie de la cryptographie à clés publiques et de la signature numérique, à travers les deux systèmes RSA et d'ElGamal. Ces systèmes nous conduisent à discuter le problème de la factorisation des grands entiers et celui du logarithme discret. La deuxième partie s'occupe des tests de primalité et spécialement du test de Lucas-Lehmer, bien adapté aux nombres de Mersenne, et du test commercial de Miller-Rabin.

Le chapitre 9 est une introduction à la théorie des approximations d'un nombre algébrique par les nombres rationnels. Une bonne moitié de ce chapitre détaille la théorie des

fractions continues et des nombres dont la fraction continue est périodique. Ce qui nous permet de résoudre les équations de Pell-Fermat $x^2 - dy^2 = \pm N$. La deuxième moitié s'occupe de l'inégalité de Liouville, des nombres transcendants de Liouville et des équations de Thue. Nous calculons finalement la fraction continue de la base de l'exponentielle et démontrons la transcendance de ce nombre.
Dans le chapitre 10, nous étudions les corps quadratiques, c'est-à-dire les sous-corps de $\mathbb{C}$, de degré 2 sur $\mathbb{Q}$. Nous introduisons les notions de trace et norme algébrique, et caractérisons les entiers d, sans facteur carré, tels que l'anneau des entiers algébriques soit euclidien pour la norme algébrique. Nous nous servons des résultats du chapitre 9 pour l'étude des éléments inversibles de ces anneaux et donnons des applications aux équations de Fermat.
Dans le chapitre 11, nous esquissons la preuve du théorème de Schneider qui dit que si α est un nombre complexe différent de 0, 1 et -1, alors α et e^{α} ne sont pas algébriques en même temps. Cette preuve est une combinaison passionnante d'arguments analytiques et algébriques. Nous obtenons comme corollaire que les nombres e et π sont transcendants.
Pour finir, nous consacrons une première annexe à un exposé sur la théorie naïve des ensembles : ensembles finis et infinis, cardinaux et ordinaux. Nous examinons quelques formes de l'axiome de choix dans la théorie axiomatique de Zermelo-Fraenkel. Les suites de Goodstein nous fournissent un exemple d'un énoncé de l'arithmétique de Peano-Dedekind, qui ne peut pas être démontré sans recourir à l'infini. Dans une deuxième annexe, nous étudions les valuations sur un corps et trouvons toutes les valuations sur le corps des nombres rationnels.

Introduction au second tome

Dans ce second tome, nous commençons par des compléments sur la théorie des groupes et celle des anneaux de polynômes. Ainsi, nous étudions les groupes d'opérateurs avec des applications aux groupes symétriques et groupes linéaires. Nous définissons aussi le résultant de deux polynômes et appliquons cette notion à la théorie de l'élimination en géométrie algébrique. Nous sommes alors armés pour attaquer la théorie de Galois et la caractérisation des équations résolubles par radicaux, auxquelles nous consacrons deux gros chapitres. Nous nous intéressons au problème du calcul pratique du groupe de Galois et aux algorithmes donnés dans le logiciel *Maple*. Le chapitre suivant traite des corps de nombres, des extensions cyclotomiques et de leurs anneaux d'entiers. Nous consacrons enfin un gros chapitre à la théorie des codes correcteurs d'erreurs : codes linéaires, codes cycliques et codes géométriques.

Remerciements

Il m'est agréable de remercier mes amis et collègues qui m'ont aidé à l'accomplissement de ce travail. André Pillons, avec qui j'ai discuté l'architecture du premier tome et qui, avec Bernard Callenaere, a relu les premiers chapitres. Je remercie tout particulièrement Jean-Pierre Lafon qui a prêté son attention critique et amicale à une bonne partie de cet ouvrage et mon ancien professeur Jean Lefebvre qui a relu tout le manuscrit : tous deux m'ont en effet suggéré maintes améliorations. Je remercie aussi l'équipe des éditions *Ellipses* et, en particulier, les directeurs de la collection Charles–Michel Marle et Philippe Pilibossian qui ont suivi attentivement la progression du manuscrit et apporté une aide technique précieuse.

sfakir@club-internet.fr Sabah AL FAKIR

Table des matières