

053088  
080390

# MATHÉMATIQUES

## 2<sup>e</sup> cycle

Cours et exercices corrigés

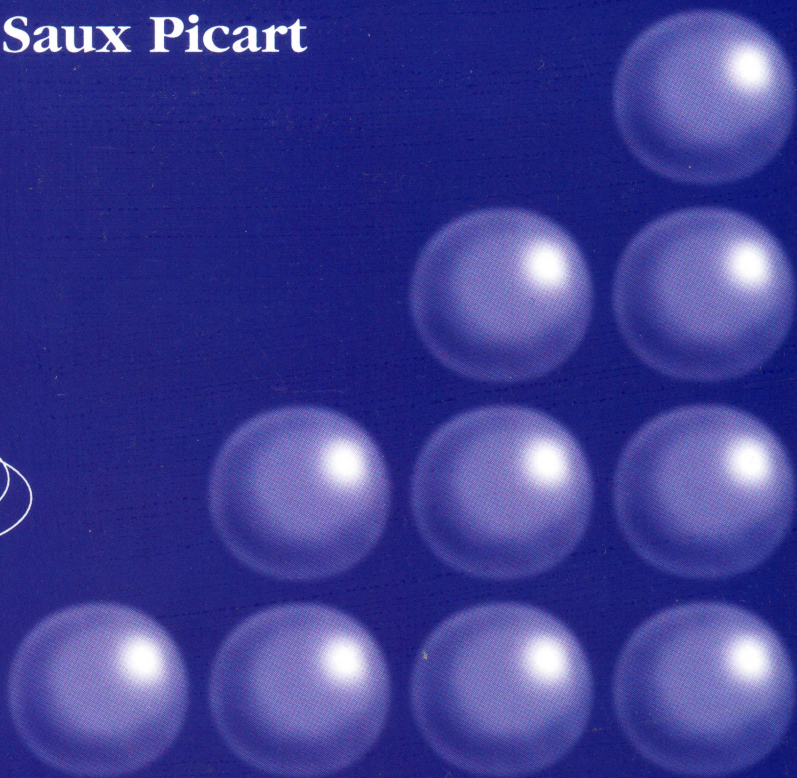
Collection dirigée par  
Charles-Michel Marle  
Philippe Pilibossian

# COURS DE CALCUL FORMEL

# Algorithmes fondamentaux

Philippe Saux Picart

ellipses

A decorative graphic in the bottom right corner of the cover, consisting of a grid of 15 spheres arranged in 3 rows and 5 columns. The spheres are rendered with a gradient and a highlight, giving them a three-dimensional appearance. The grid is partially obscured by the text 'ellipses' and its logo.

M508

MATHÉMATIQUES POUR LE 2<sup>E</sup> CYCLE

Collection dirigée par Charles-Michel MARLE et Philippe PILIBOSSIAN

053088

(5)



COURS DE CALCUL FORMEL

# Algorithmes fondamentaux

Philippe SAUX PICART

Agrégé des universités

*Maître de conférences à l'université de Bretagne Occidentale*



# Table des matières

## Chapitre I : Algorithmique

I.1	Calcul formel : quelques généralités . . . . .	1
I.1.1	Calcul formel et numérique . . . . .	1
I.1.2	Quelques points délicats . . . . .	2
I.2	De la complexité des calculs . . . . .	3
I.2.1	Complexité d'un algorithme . . . . .	4
I.3	De la conception d'un algorithme . . . . .	7
I.3.1	Procédure récursive ou itérative? . . . . .	8
I.3.2	Diviser pour gagner . . . . .	9
I.3.3	Prouver un algorithme . . . . .	12
	Exercices . . . . .	14

## Chapitre II : Codage et Arithmétique élémentaire

II.1	Bases de numération et codage informatique . . . . .	17
II.2	Arithmétique des nombres entiers . . . . .	20
II.2.1	Addition et soustraction . . . . .	21
II.2.2	Multiplication . . . . .	23
II.2.3	Division . . . . .	24
II.3	Arithmétique des polynômes . . . . .	29
II.3.1	Codage des polynômes . . . . .	29
II.3.2	Opérations polynômiales . . . . .	30
II.3.3	La multiplication de polynômes selon la méthode de <i>Karatsuba</i> . . . . .	31
	Exercices . . . . .	33

## Chapitre III : Anneaux factoriels et euclidiens

III.1	Anneaux factoriels . . . . .	35
III.1.1	Structure d'anneau . . . . .	35
III.1.2	Divisibilité . . . . .	36
III.1.3	Anneaux factoriels . . . . .	36
III.1.4	Une classe d'anneaux factoriels . . . . .	39
III.2	Anneaux euclidiens . . . . .	40
III.2.1	Définitions . . . . .	40

III.2.2	Des exemples . . . . .	40
III.2.3	Divisibilité dans un anneau euclidien . . . . .	43
III.3	L'algorithme d'Euclide . . . . .	44
III.3.1	La méthode de base . . . . .	45
III.3.2	Algorithme d'Euclide étendu . . . . .	46
III.3.3	Le pgcd de plus de deux éléments . . . . .	48
III.4	Analyse de l'algorithme d'EUCLIDE dans $\mathbb{Z}$ . . . . .	49
III.4.1	Taille des coefficients de BÉZOUT . . . . .	49
III.4.2	Complexité . . . . .	51
III.5	Recherche du pgcd dans un anneau de polynômes . . . . .	53
III.5.1	Pseudo-division . . . . .	53
III.5.2	Polynômes primitifs . . . . .	55
III.5.3	Calcul du pgcd. . . . .	56
	Exercices . . . . .	58

#### Chapitre IV : L'ensemble $\mathbb{Z}/n\mathbb{Z}$ et applications

IV.1	Généralités . . . . .	62
IV.1.1	Définitions et calculs . . . . .	62
IV.1.2	Les inversibles . . . . .	64
IV.2	Systèmes congruents . . . . .	66
IV.2.1	Cas de deux équations . . . . .	67
IV.2.2	Cas général . . . . .	69
IV.2.3	Numérotation mixte . . . . .	70
IV.2.4	Algorithme de GARNER . . . . .	72
IV.3	Calculs modulaires . . . . .	74
IV.3.1	Calcul modulaire du pgcd de deux polynômes . . . . .	76
IV.4	Quelques applications en arithmétique . . . . .	81
IV.4.1	Calcul de l'indicateur d'EULER . . . . .	81
IV.4.2	Racine carrée de -1 dans $\mathbb{Z}/p\mathbb{Z}$ . . . . .	83
IV.5	Une petite initiation à la cryptographie . . . . .	87
	Exercices . . . . .	93

#### Chapitre V : Calculs Polynomiaux

V.1	Interpolation dans $\mathbb{K}[X]$ . . . . .	96
V.1.1	Systèmes congruents de polynômes . . . . .	97
V.1.2	Interpolation d'HERMITE . . . . .	100
V.1.3	Application à la factorisation de polynômes de $\mathbb{Z}[X]$ . . . . .	101
V.2	Calculs dans $\mathbb{K}[X_1, \dots, X_n]$ . . . . .	102
V.2.1	Réduire le nombre d'indéterminées . . . . .	103
V.2.2	Calculs par homomorphismes . . . . .	103
V.2.3	PGCD de polynômes en plusieurs indéterminées. . . . .	106

Exercices . . . . .	108
<b>Chapitre VI : Séries Formelles</b>	
VI.1 L'anneau des séries formelles . . . . .	110
VI.1.1 Généralités . . . . .	110
VI.1.2 Dérivation . . . . .	114
VI.1.3 Séries génératrices . . . . .	116
VI.2 Suites récurrentes linéaires . . . . .	117
VI.3 Suites P-récurrentes et équations différentielles dans $\mathbb{K}[[X]]$ . . . . .	120
VI.3.1 Séries formelles $\Delta$ -finies . . . . .	120
VI.3.2 L'algèbre des séries formelles $\Delta$ -finies . . . . .	124
VI.4 Une application combinatoire : les nombres de CATALAN . . . . .	128
Exercices . . . . .	130
<b>Chapitre VII : Systèmes d'équations</b>	
VII.1 Résolution de systèmes linéaires . . . . .	134
VII.1.1 Généralités . . . . .	134
VII.1.2 Résolution avec divison : la méthode du pivot de GAUSS . . . . .	136
VII.1.3 Résolution sans division . . . . .	137
VII.1.4 Résolution avec division exacte : la méthode de BAREISS . . . . .	138
VII.1.5 Complexité . . . . .	141
VII.2 Résultants . . . . .	143
VII.3 Applications . . . . .	147
VII.3.1 Résolutions de petits systèmes polynômiaux . . . . .	147
VII.3.2 Intégration de fractions rationnelles . . . . .	151
Exercices . . . . .	156
<b>Annexe : Programmation avec Maple V</b> . . . . .	159
<b>Bibliographie</b> . . . . .	173
<b>Index</b> . . . . .	175

La collection *Mathématiques 2<sup>e</sup> cycle* 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 et de nombreux exercices. Les auteurs de ces ouvrages ont tous une grande expérience de l'enseignement des mathématiques au niveau supérieur.

Le calcul formel a connu un développement rapide durant les vingt dernières années. C'est un outil calculatoire digne d'intérêt pour tout ingénieur ou chercheur. Il fait partie des programmes de l'agrégation de mathématiques et des concours d'entrée à plusieurs grandes écoles. Aujourd'hui, des calculatrices de poche dérivent, intègrent, réalisent des calculs matriciels de manière formelle. Les algorithmes qui sous-tendent ce développement sont purement algébriques.

Au travers de quelques résultats d'algèbre élémentaire, nous essayons de montrer comment l'algèbre et l'informatique sont deux disciplines qui se fécondent l'une l'autre. Cet ouvrage n'est pas un cours d'algèbre classique : il veut sensibiliser les étudiants aux problèmes que l'on rencontre au contact des ordinateurs et veille à ce que les solutions données aux problèmes rencontrés soient réellement utilisables en pratique.

La démarche suivie consiste à montrer comment construire une solution effective à un problème donné puis à en déduire un algorithme efficace. Cet algorithme sera ensuite appliqué à des exemples non triviaux dont on cherchera à évaluer la complexité.

Cette approche nous semble fructueuse sur plus d'un plan : elle permet de prendre contact avec le monde des mathématiques appliquées et d'enseigner les structures algébriques sous une forme extrêmement concrète. Par exemple, on prendra conscience de la pertinence de la notion d'anneau euclidien en voyant comment on peut effectuer des calculs identiques dans des ensembles aussi différents que les entiers de Gauss et les anneaux de polynômes sur un corps. Voilà qui simplifie les tâches et donne du sens à l'abstraction. C'est là une profonde conviction que nous désirons faire partager dans ce livre.



La collection *Mathématiques 2<sup>e</sup> cycle* 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 et de nombreux exercices. Les auteurs de ces ouvrages ont tous une grande expérience de l'enseignement des mathématiques au niveau supérieur.

Le calcul formel a connu un développement rapide durant les vingt dernières années. C'est un outil calculatoire digne d'intérêt pour tout ingénieur ou chercheur. Il fait partie des programmes de l'agrégation de mathématiques et des concours d'entrée à plusieurs grandes écoles. Aujourd'hui, des calculatrices de poche dérivent, intègrent, réalisent des calculs matriciels de manière formelle. Les algorithmes qui sous-tendent ce développement sont purement algébriques.

Au travers de quelques résultats d'algèbre élémentaire, nous essayons de montrer comment l'algèbre et l'informatique sont deux disciplines qui se fécondent l'une l'autre. Cet ouvrage n'est pas un cours d'algèbre classique : il veut sensibiliser les étudiants aux problèmes que l'on rencontre au contact des ordinateurs et veille à ce que les solutions données aux problèmes rencontrés soient réellement utilisables en pratique.

La démarche suivie consiste à montrer comment construire une solution effective à un problème donné puis à en déduire un algorithme efficace. Cet algorithme sera ensuite appliqué à des exemples non triviaux dont on cherchera à évaluer la complexité.

Cette approche nous semble fructueuse sur plus d'un plan : elle permet de prendre contact avec le monde des mathématiques appliquées et d'enseigner les structures algébriques sous une forme extrêmement concrète. Par exemple, on prendra conscience de la pertinence de la notion d'anneau euclidien en voyant comment on peut effectuer des calculs identiques dans des ensembles aussi différents que les entiers de Gauss et les anneaux de polynômes sur un corps. Voilà qui simplifie les tâches et donne du sens à l'abstraction. C'est là une profonde conviction que nous désirons faire partager dans ce livre.

