

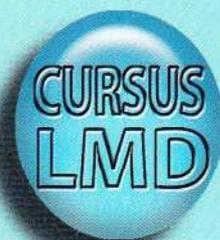
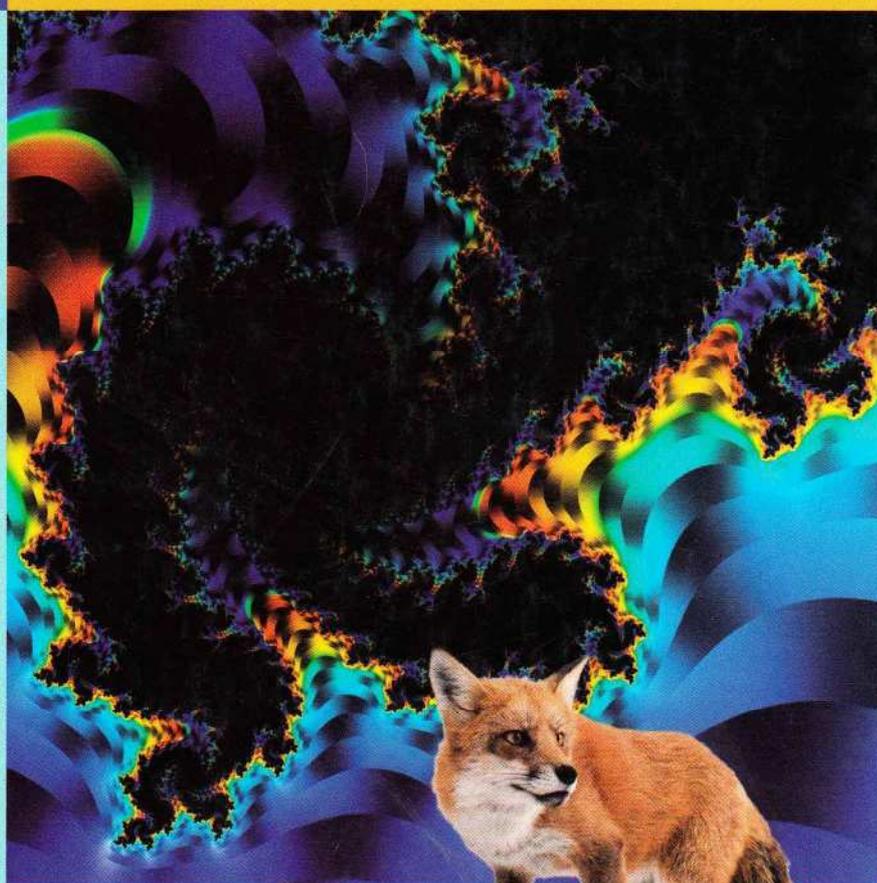
Mathématiques appliquées

L3



Sous la direction de :
**Alain Yger et
Jacques-Arthur Weil**

Rémi Abgrall
Sophie Abgrall
Didier Aussel
Jean-Pierre Dedieu
Robert Deville
Charles Dossal
Jean-Charles Faugère
Patrick Fischer
Philippe Gaborit
Khodor Khadra
Alain-Yves Le Roux
Marie-Noëlle Le Roux
Pierre Maréchal
Pierre Pesneau
Mohab Safey El Din
Philippe Thieullen
Jacques-Arthur Weil
Alain Yger



**Cours complet avec 500 tests
et exercices corrigés**

PEARSON
Education

Table des matières

Avant-propos	xxi
Remerciements	xxii
Partie I – Analyse numérique	1
1 Algèbre linéaire et calcul scientifique	3
I Les sources d’erreurs numériques dans un ordinateur : le calcul en flottant	7
II Des rappels et compléments d’algèbre linéaire	9
II.1 Déterminant	9
II.2 Valeurs propres	11
II.3 Normes	12
II.4 Résultats supplémentaires	16
II.5 Conditionnement d’un système linéaire	18
III Les calculs de produits matrice-vecteur et matrice-matrice dans un ordinateur . .	21
III.1 Exploitation des structures de données	21
III.2 À propos du coût de calcul du produit matrice-matrice	25
IV La résolution de systèmes linéaires : les méthodes directes	26
IV.1 Motivation	26
IV.2 La méthode de Gauss et quelques variantes	28
IV.3 Propriétés supplémentaires	33
IV.4 Les méthodes QR/QL	40
V La résolution de systèmes linéaires : les méthodes itératives	44
V.1 Un aperçu des méthodes itératives	44
V.2 Méthode de Gauss-Seidel	51
V.3 Cas des matrices non négatives	54
V.4 La méthode du gradient conjugué	57
V.5 Le théorème de Perron-Frobenius et ses conséquences	64
VI Le calcul de valeurs propres et de vecteurs propres	68
VI.1 Introduction : pourquoi calculer des valeurs propres ?	68
VI.2 Conditionnement du problème de valeurs propres	68
VI.3 Calcul de la plus grande valeur propre	71
VI.4 Calcul de vecteurs propres : méthode de la puissance inverse	73
VII Exercices	74
Complément 1 La traque suivant un dictionnaire	76

Complément 2	Inversion et Parcimonie	81
2	Interpolation et approximation	87
I	Interpolation	87
I.1	L'interpolation polynomiale	87
I.2	Étude de l'erreur d'interpolation	90
I.3	Base de Newton et différences divisées	92
I.4	Fonctions-spline	95
II	Approximation hilbertienne et polynômes orthogonaux	100
II.1	L'approximation hilbertienne	101
II.2	Le procédé d'orthogonalisation de Gram-Schmidt	103
II.3	Polynômes orthogonaux	103
II.4	Les polynômes de Legendre	105
II.5	Les polynômes de Tchebychev	106
II.6	Polynômes orthogonaux et équations différentielles	107
II.7	Fonctions harmoniques et polynômes de Legendre	109
III	Approximation uniforme	111
III.1	Le théorème de Weierstrass	111
III.2	Courbes de Bézier et algorithme de De Casteljau	113
III.3	La théorie de Tchebychev	116
IV	Approximation des formes linéaires	117
IV.1	Un exemple simple : le calcul des dérivées	118
IV.2	Intégration approchée	120
IV.3	Exemples	122
IV.4	Formules d'erreur	124
IV.5	La formule de la moyenne	125
IV.6	Formules de Gauss	128
IV.7	Formules composites	131
IV.8	La formule de sommation d'Euler	133
IV.9	La méthode d'intégration de Romberg	137
V	Approximation des racines d'équations et de systèmes d'équations	140
V.1	Le théorème des approximations successives	141
V.2	Résolution numérique d'une équation d'une variable	143
V.3	Résolution numérique de systèmes d'équations	147
V.4	Zéros réels d'un polynôme	151
VI	Exercices	156
VI.1	Interpolation	156
VI.2	Polynômes orthogonaux	157

VI.3	Approximation uniforme	158
VI.4	Intégration approchée	158
VI.5	Résolution d'équations	159
3	Résolution numérique des équations différentielles et des équations aux dérivées partielles	161
I	La méthode d'Euler	162
I.1	Généralités	162
I.2	Définition de la méthode d'Euler	163
I.3	Majoration de l'erreur de discrétisation	164
I.4	Comportement asymptotique de l'erreur	166
I.5	Contrôle du pas	167
II	Les méthodes à un pas	168
II.1	Introduction	168
II.2	Notions de consistance, stabilité, convergence	168
II.3	Convergence des méthodes à un pas	169
II.4	Étude de l'erreur de discrétisation	172
II.5	Exemples de méthodes à un pas	177
II.6	Étude des méthodes de Runge-Kutta	181
III	Les méthodes multipas	187
III.1	Exemples de méthodes multipas	188
III.2	Formulation générale des méthodes multipas. Notions de consistance, stabilité, convergence.	190
III.3	Convergence des méthodes multipas	191
III.4	Ordre d'une méthode multipas. Étude de l'erreur de discrétisation	197
III.5	Méthodes de prédiction-correction	204
IV	La résolution d'équations différentielles raides	207
IV.1	Introduction	207
IV.2	Domaine de stabilité absolue	208
V	Une introduction à la méthode des éléments finis pour les problèmes elliptiques	212
V.1	Généralités	213
V.2	Formulation variationnelle	214
V.3	Approximation du problème de Dirichlet faible par une méthode d'éléments finis	217
V.4	Le problème de Neumann	220
VI	Une introduction aux problèmes paraboliques	222
VI.1	Introduction	222
VI.2	Semi-discrétisation en espace	222
VI.3	Discrétisation complète	223

VI.4	Discrétisation avec intégration numérique	224
VI.5	Un autre exemple de problème parabolique : le problème de Black-Scholes	224
VII	L'hyperbolicité et les ondes	229
VII.1	Les équations quasi linéaires du premier ordre	229
VII.2	Les caractéristiques	229
VII.3	La formulation conservative et le problème de Riemann	232
VII.4	La discrétisation des équations quasi linéaires	234
VIII	Exercices	237
Complément 1	Les systèmes à deux ondes	241
Complément 2	Les équilibres et l'environnement	247
Complément 3	Une équation de Hamilton-Jacobi	253
Partie II – Algorithmique et programmation		259
4	Algorithmique	261
I	Généralités	261
II	Notion de complexité	263
III	Algorithmes de tri	265
III.1	Tri sélection	266
III.2	Tri insertion	266
III.3	Tri à bulles	268
III.4	Tri fusion	269
III.5	Tri rapide	270
IV	Introduction à la gestion dynamique de la mémoire	272
IV.1	Notion de pointeur	272
IV.2	Allocation dynamique	272
V	Un type abstrait de données : le dictionnaire	273
V.1	Type abstrait de données et structure de données associée	273
V.2	Stockage par tableau	274
V.3	Stockage par liste chaînée	276
VI	Exercices	280
5	Programmation en Fortran 90 pour le calcul scientifique	283
I	Quelques règles d'écriture générales en Fortran 90	283
II	Les types	285
II.1	Le type entier (INTEGER)	285
II.2	Le type réel (REAL)	285
II.3	Le type complexe (COMPLEX)	286

II.4	Le type chaîne de caractères (CHARACTER)	286
II.5	Le type logique (LOGICAL)	286
II.6	Les types structures ou types dérivés (TYPE)	287
II.7	Le type tableau (DIMENSION)	287
III	Les expressions et affectations	288
III.1	Les expressions numériques scalaires	288
III.2	Les expressions logiques	290
III.3	Les expressions constantes	291
IV	Les instructions de contrôle	291
IV.1	L'instruction IF structurée	291
IV.2	L'instruction SELECT CASE	292
IV.3	La boucle avec compteur DO	293
IV.4	La boucle DO WHILE (tant que)	294
V	Les tableaux	295
V.1	Généralités	295
V.2	Exemples de déclarations de tableaux à plusieurs dimensions	295
V.3	Rang, étendue, profil et taille d'un tableau	296
V.4	Les opérations relatives aux tableaux ou à des sections de tableaux	296
V.5	Stockage et optimisation dans le parcours d'un tableau	300
VI	Les entrées-sorties standard et les fichiers	302
VI.1	Les principaux descripteurs de format	303
VI.2	Lecture et écriture dans un fichier	305
VI.3	Quelques remarques générales	306
VI.4	Quelques remarques sur la lecture et l'écriture de tableaux	307
VII	Les procédures : sous-programmes et fonctions	308
VII.1	Introduction	308
VII.2	Notions de variable locale, variable globale, argument	309
VII.3	Notion de procédure externe	309
VII.4	Notion de procédure interne	311
VII.5	Les interfaces	312
VII.6	Tableaux transmis en argument	313
VIII	L'allocation dynamique des tableaux	318
IX	Les modules et la genericité	319
IX.1	Notion de module	319
IX.2	Les procédures génériques	321
IX.3	Surdéfinition d'opérateurs	321
X	La gestion dynamique et les pointeurs	323

X.1	Présentation de la notion de pointeur	323
X.2	Pointeurs sur les tableaux	324
XI	Quelques fonctions intrinsèques de Fortran 90 liées aux tableaux	324
XII	Exercices	325
Partie III – Algèbre appliquée		329
6	De l’algèbre linéaire à la résolution des systèmes polynomiaux	331
I	Introduction et généralités	331
II	Liens entre algèbre et géométrie : projection et élimination	333
II.1	Idéaux et équations : définitions et premières propriétés	333
II.2	Idéaux et variétés : géométrie des solutions des systèmes d’équations . . .	335
II.3	Notion de dimension	337
II.4	Anneaux-quotients : définition et propriétés	338
II.5	Des idéaux de dimension zéro à l’algèbre linéaire	341
II.6	Notion de degré et multiplicité	344
III	Résolution des systèmes polynomiaux en deux variables – Introduction du résultant	347
III.1	Introduction	347
III.2	Résultant – définition et propriétés	349
III.3	Algorithmes de calcul du résultant	353
III.4	Algorithme de résolution de systèmes d’équations en 2 variables	357
IV	Algorithme de division pour les polynômes en plusieurs variables	360
IV.1	Ordres monomiaux	361
IV.2	Monômes et termes de tête	362
IV.3	Réduction d’un polynôme	363
IV.4	Réduction totale d’un polynôme	366
V	Définition et propriétés des Bases de Gröbner	367
V.1	Définition d’une base de Gröbner	367
V.2	Algorithme de Buchberger	368
V.3	Caractérisation d’une base de Gröbner	370
V.4	Propriétés des bases de Gröbner	373
VI	Algèbre linéaire dans les anneaux-quotients – Résolution des systèmes de dimension zéro	374
VI.1	Calcul d’une représentation matricielle des endomorphismes de multiplication	375
VI.2	Propriétés des endomorphismes de multiplication	378
VI.3	Calcul des paramétrisations rationnelles	380

VII Exercices	381
Complément Algorithme de changement de base FGLM	383
7 Introduction à la théorie algébrique des codes correcteurs d'erreurs	389
I Théorie élémentaire des codes correcteurs	391
I.1 Formalisation mathématique	391
I.2 Encodage	392
I.3 Distance de Hamming	394
I.4 Décodage par maximum de vraisemblance	396
I.5 Décodage par syndrome	397
II Constructions élémentaires de codes et bornes	400
II.1 Constructions génériques à partir de codes donnés	400
II.2 Constructions de familles de codes classiques	402
II.3 Bornes	406
III Quelques rappels sur les corps finis	409
IV Codes cycliques et codes BCH	411
IV.1 Théorie élémentaire des codes cycliques	411
IV.2 Borne BCH	414
IV.3 Codes BCH	416
IV.4 Codes de Reed-Solomon cycliques	417
V Décodage des codes BCH	417
V.1 Algorithme de Peterson	417
V.2 Décodage par l'algorithme d'Euclide étendu	421
VI Codes de Reed-Solomon, codes alternants et codes de Goppa	422
VI.1 Codes de Reed-Solomon et algorithme de Welch-Berlekamp	422
VI.2 Codes alternants	425
VI.3 Codes de Goppa binaires	426
VII Décodage en liste des codes de Reed-Solomon	430
VII.1 Introduction au décodage en liste	430
VII.2 Algorithme de Sudan	431
VIII Exercices	433
8 Introduction à la cryptographie	435
I Un rapide historique de la cryptographie	437
I.1 Transpositions : la scytale grecque	437
I.2 Substitutions : le chiffrement de César	437
I.3 Substitutions monoalphabétiques	437
I.4 Chiffrement de Vigenère	439

I.5	Chiffrement produit (substitutions mêlées aux transpositions)	439
I.6	Chiffrement par blocs	440
I.7	Chiffrement de Vernam (chiffrement à flot)	440
I.8	Chiffrement mécanique	441
II	Chiffrement à clé secrète	441
II.1	Chiffrement par blocs	441
II.2	Chiffrement à flot	447
III	Rappels d'arithmétique	451
III.1	Inversion modulo N et calcul modulaire	451
III.2	Générateurs de $(\mathbb{Z}/N\mathbb{Z})^*$	453
IV	Chiffrement à clé publique : R.S.A.	454
IV.1	Algorithme R.S.A.	454
IV.2	Mise en œuvre des calculs	455
IV.3	La sécurité de R.S.A.	457
IV.4	Génération de nombres premiers	458
V	Échange de clés et chiffrement basés sur le logarithme discret	459
V.1	Échange de clés de Diffie-Hellman	460
V.2	Chiffrement d'El Gamal	461
VI	Fonctions de hachage	462
VI.1	Définitions	462
VI.2	Attaque par paradoxe des anniversaires	463
VI.3	Fonction de hachage itérée	464
VI.4	Fonctions de chiffrement spécialisées	465
VII	Signature	467
VII.1	Définition	467
VII.2	Signatures	467
VII.3	Infrastructure de gestion de clé	469
VIII	Authentification	470
VIII.1	Authentification par chiffrement symétrique	470
VIII.2	Authentification à clé publique	471
VIII.3	Schémas à divulgation nulle de connaissance (<i>zero-knowledge</i>)	471
IX	Codes correcteurs d'erreurs et cryptographie à clé publique	472
IX.1	Un problème difficile en théorie des codes	473
IX.2	Décodage d'un code aléatoire par ensemble d'informations	473
IX.3	Schéma de chiffrement de McEliece	474
X	Exercices	475

Partie IV – Analyse et mathématiques appliquées	479
9 Optimisation	481
I Modélisation, vocabulaire et classification	482
I.1 Premières notions	482
I.2 Modélisation et classification	483
II Notations et résultats préliminaires	484
III Problèmes sans contrainte	487
III.1 Existence et unicité	487
III.2 Conditions d'optimalité	490
III.3 Approche numérique	494
III.4 Méthode de Wolfe de minimisation unidimensionnelle	495
III.5 Convergence de la méthode du gradient	497
III.6 Quelques expérimentations numériques	499
IV Optimisation avec contraintes	500
IV.1 Existence et unicité	500
IV.2 Conditions d'optimalité	501
IV.3 Contraintes d'égalité	503
IV.4 Contraintes égalité-inégalité	505
IV.5 Approche numérique	510
V Rudiments d'optimisation linéaire	512
V.1 Introduction	512
V.2 Solutions de base	514
V.3 Existence d'une solution	518
V.4 Dualité	521
VI Exercices	527
Complément Méthodes d'optimisation non linéaire pour l'optimisation linéaire .	529

10 Analyse harmonique appliquée : signaux et images	537
I Les signaux déterministes, les processus stochastiques discrets	537
I.1 Signaux déterministes : de l'analogique au digital	537
I.2 La transformation de Fourier et l'ubiquité des gaussiennes	540
I.3 Le problème de l'échantillonnage	543
I.4 Processus stochastiques discrets	545
II Les outils algorithmiques	547
II.1 La transformation de Fourier discrète : pourquoi et comment ?	547
II.2 Filtres digitaux et filtres analogiques	557
III Les analyses temps-échelles et temps-fréquences	570

III.1	L'analyse continue en temps-échelles	570
III.2	Du mécanisme de la vision à JPEG2000	573
III.3	L'analyse temps-fréquences	582
IV	Exercices	588
Complément 1	Mathématiques et médecine nucléaire	591
Complément 2	Images et familles géométriques	596
Complément 3	Analyse de la turbulence bidimensionnelle	601

Partie V – Probabilités et statistique 607

11 Probabilités 609

I	Les espaces de probabilité	609
I.1	Tribu des événements d'une expérience aléatoire	609
I.2	Probabilités	611
I.3	Le lemme de Borel-Cantelli	614
II	Les variables aléatoires	616
II.1	Variables aléatoires	616
II.2	Fiabilité	621
III	L'indépendance de variables aléatoires	623
III.1	Indépendance	623
III.2	Corrélation	626
III.3	Loi d'une somme de v. a. r. indépendantes	627
IV	Quelques situations concrètes	628
IV.1	Le schéma de Bernoulli	628
IV.2	Renouvellement : le processus de Poisson	631
IV.3	Approximation de lois	632
V	Les théorèmes limites en probabilités	635
V.1	Divers modes de convergence en probabilité	636
V.2	Lois des grands nombres	637
V.3	Application à l'estimation	640
V.4	Utilisation de la transformée de Laplace	642
V.5	Fonctions génératrices	645
VI	Les fonctions caractéristiques et le théorème limite central	646
VI.1	Fonctions caractéristiques	647
VI.2	La loi de Gauss	648
VI.3	Le théorème de Paul Lévy	649
VI.4	Le théorème limite central	651

VI.5	Intervalles de confiance asymptotiques	652
VII	Les chaînes de Markov	654
VII.1	Définition et exemples	654
VII.2	Processus stochastiques, temps d'arrêt	657
VII.3	Temps de retour : récurrence et transience	658
VII.4	Mesures invariantes	659
VII.5	Comportement asymptotique	662
VII.6	Périodicité	664
VII.7	Annexe : matrices stochastiques et chaînes de Markov	665
VIII	L'explication d'une variable aléatoire par une autre variable aléatoire	667
VIII.1	Régression linéaire	667
VIII.2	Espérance conditionnelle	669
IX	Les martingales	672
IX.1	Définition, théorème d'arrêt, inégalité de Doob	672
IX.2	Convergence des martingales	674
IX.3	Retour sur la loi des grands nombres	677
IX.4	Applications	678
X	Exercices	683
12	Statistique	689
I	Statistique descriptive	690
I.1	Introduction au modèle statistique	690
I.2	Représentation graphique	691
I.3	Indicateurs numériques	693
II	Statistique inférentielle	701
II.1	Approche probabiliste	701
II.2	Estimateur et estimation ponctuelle	708
II.3	Estimation par intervalle	714
III	Tests d'hypothèse	724
III.1	Introduction aux tests d'hypothèse	725
III.2	Tests usuels gaussiens	730
III.3	Tests du chi-deux	738
IV	Résultats rigoureux en statistique	743
IV.1	Rappels sur les lois conditionnelles	743
IV.2	Statistique exhaustive	747
IV.3	Construction et qualité des estimateurs	752
IV.4	Théorie de Neyman-Pearson	759
V	Exercices	764

Partie VI – Annexes	769
1 Prise en main d'un logiciel de calcul scientifique (Matlab, Scilab)	771
2 Prise en main d'un logiciel de calcul formel	789
3 Tables statistiques	801
Partie VII – Solutions des tests	813
Partie VIII – Solutions des exercices	847
Index	881