

Loïc Foissy
Alain Ninet

Agrégation
de
Mathématiques
Option C

Algèbre et calcul formel



La côte de l'ouvrage : 2-512-170

Table des matières

Introduction	3
I Algorithmique	11
1 Cours	13
1.1 Représentation des réels	13
1.2 Algorithmes	19
1.3 Complexité	21
1.4 Calcul rapide de puissance	24
1.5 Exercices	26
1.6 Corrigés	31
2 Courbes de Bézier	49
2.1 Texte	49
2.2 TP	53
2.3 Corrigé	54
3 Multiplication de grands objets	57
3.1 Texte	57
3.2 TP	61
3.3 Corrigé	61
4 FFT et applications	63
4.1 Texte	63
4.2 TP	67
4.3 Corrigé	68

II	Actions de groupes	71
5	Cours	73
5.1	Définitions et exemples	73
5.2	Aspects combinatoires des actions de groupes	75
5.3	Applications aux groupes symétriques	77
5.4	Exercices	80
5.5	Corrigés	81
6	Permutations et jeu de taquin	87
6.1	Texte	87
6.2	TP	93
6.3	Corrigé	94
7	Matrices à coefficients entiers de Gauss	97
7.1	Texte	97
7.2	TP	103
7.3	Corrigé	103
8	Énumération de molécules	107
8.1	Texte	107
8.2	TP	112
8.3	Corrigé	113
III	Polynômes	115
9	Cours	117
9.1	Construction et propriétés arithmétiques	118
9.2	Algorithme de Berlekamp	133
9.3	Polynômes à plusieurs indéterminées	141
9.4	Exercices	148
9.5	Corrigés	151
10	La factorisation dans $\mathbb{Z}[X]$	165
10.1	Texte	165
10.2	TP	168
10.3	Corrigé	169
11	Racines réelles d'un polynôme réel	171
11.1	Texte	171
11.2	TP	175

<i>TABLE DES MATIÈRES</i>	7
11.3 Corrigé	175
12 La décomposition de Dunford	179
12.1 Texte	179
12.2 TP	183
12.3 Corrigé	183
13 Explosion des coefficients	187
13.1 Texte	187
13.2 TP	191
13.3 Corrigé	192
IV Élimination	197
14 Cours	199
14.1 Résultants à une indéterminée	199
14.2 Élimination	205
14.3 Exercices	208
14.4 Corrigés	211
15 Paramétrisation d'une courbe	219
15.1 Texte	219
15.2 TP	222
15.3 Corrigé	223
16 Enveloppes de courbes	225
16.1 Texte	225
16.2 TP	228
16.3 Corrigé	229
17 Un théorème de Poncelet	233
17.1 Texte	233
17.2 TP	238
17.3 Corrigé	239
18 Génétique et résultants	243
18.1 Texte	243
18.2 TP	247
18.3 Corrigé	247

19 Géométrie du cyclohexane	251
19.1 Texte	251
19.2 TP	255
19.3 Corrigé	256
20 Construction de surfaces algébriques	259
20.1 Texte	259
20.2 TP	264
20.3 Corrigé	265
V Cryptographie, codes correcteurs	269
21 Cours	271
21.1 Cryptographie à clé publique	272
21.2 Le système RSA	275
21.3 Théorie des codes	280
21.4 Exercices	290
21.5 Corrigés	299
22 Compression d'information	321
22.1 Texte	321
22.2 TP	327
22.3 Corrigé	327
23 Une extension de Diffie-Hellman	329
23.1 Texte	329
23.2 TP	332
23.3 Corrigé	333
24 Factorisation et friabilité	335
24.1 Texte	335
24.2 TP	341
24.3 Corrigé	342
25 Logarithme discret	343
25.1 Texte	343
25.2 TP	347
25.3 Corrigé	348

26 Le problème du sac à dos	349
26.1 Texte	349
26.2 TP	354
26.3 Corrigé	354
VI Systèmes linéaires	357
27 Cours	359
27.1 Conditionnement	359
27.2 Méthodes de résolution directes	369
27.3 Méthodes de résolution itératives	376
27.4 Complément sur les matrices hermitiennes	379
27.5 Exercices	385
27.6 Corrigés	389
28 Étude d'un système proies-prédateurs	409
28.1 Texte	409
28.2 TP	414
28.3 Corrigé	415
29 Suites linéaires récurrentes	417
29.1 Texte	417
29.2 TP	421
29.3 Corrigé	422
30 Régularisation d'une grille	423
30.1 Texte	423
30.2 TP	429
30.3 Corrigé	431
31 Annexe : Introduction à Maxima	433
31.1 Généralités	433
31.2 Exercices	434
31.3 Corrigés	443
Bibliographie	452
Index	455