

Odile Fleury
Loïc Foissy
Alain Ninet

Agrégation
de
Mathématiques
Option C

Algèbre et calcul formel

2^e édition



ellipses

Table des matières

I	Cours et exercices corrigés	11
1	Algorithmes et complexité	13
1.1	Représentation en machine	13
1.2	Algorithmes, complexité	18
1.3	Algorithmes classiques	22
1.4	Bilan : complexités classiques à connaître	37
1.5	Exercices	38
1.6	Corrigés	40
2	Le théorème chinois et des applications	47
2.1	Cas simple	48
2.2	Cas général	50
2.3	Quelques applications	52
2.3.1	Fonction d'Euler	52
2.3.2	En algèbre linéaire	54
2.4	Exercices	56
2.5	Corrigés	58
3	Actions de groupes	65
3.1	Définitions et exemples	65
3.2	Orbites et stabilisateurs	67
3.3	Applications aux groupes symétriques	71
3.4	Exercices	74
3.5	Corrigés	75
4	Représentations des groupes finis	83
4.1	Définitions et premières propriétés	84
4.1.1	Représentation d'un groupe	84
4.1.2	Opérations sur les représentations	85

4.1.3	Morphismes de représentations	87
4.2	Représentations irréductibles	88
4.2.1	Définition	88
4.2.2	Semi-simplicité des représentations	89
4.3	Caractères d'un groupe abélien fini	92
4.3.1	Représentations d'un groupe abélien fini	92
4.3.2	Groupe dual	93
4.3.3	Théorème de Kronecker	95
4.4	Caractères d'une représentation	98
4.4.1	Définition	98
4.4.2	Lemme de Schur et applications	102
4.4.3	Orthonormalité des caractères irréductibles	103
4.4.4	Représentation régulière	106
4.4.5	Noyaux des représentations	109
4.5	Exemples de tables de caractères	111
4.5.1	Les groupes cycliques	111
4.5.2	Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	112
4.5.3	Le groupe symétrique \mathfrak{S}_3	113
4.6	Représentations réelles en petite dimension	114
4.6.1	Résultats préliminaires	115
4.6.2	Cas de la dimension 2	116
4.6.3	Cas de la dimension 3	117
4.7	Exercices	126
4.8	Corrigés	127
5	Polynômes	137
5.1	Construction et propriétés arithmétiques	138
5.2	Polynômes à plusieurs indéterminées	156
5.3	Polynômes symétriques	163
5.3.1	Indépendance algébrique	165
5.3.2	Poids et homogénéité	167
5.3.3	Ordre lexicographique	168
5.3.4	Théorème fondamental	169
5.4	Exercices	172
5.5	Corrigés	176
6	Corps finis	191
6.1	Premières propriétés des corps finis	192
6.2	Existence et unicité d'un corps fini, construction	200
6.3	Sous-corps et extensions d'un corps fini	204
6.4	Carrés dans un corps fini	206

6.5	Algorithme de Berlekamp	212
6.6	Exercices	219
6.7	Corrigés	223
7	Élimination	241
7.1	Résultants à une indéterminée	242
7.2	Élimination	248
7.3	Exercices	252
7.4	Corrigés	254
8	Cryptographie, codes correcteurs	269
8.1	Cryptographie à clé publique	270
8.2	Théorie des codes	279
8.3	Exercices	290
8.4	Corrigé	297
II	Textes de modélisation	311
9	Introduction aux textes	313
10	Étude de populations	315
10.1	Texte	315
10.2	Commentaires	319
10.3	TP	320
10.4	Corrigé	320
11	Position d'un objet	323
11.1	Texte	323
11.2	Commentaires	327
11.3	TP	328
11.4	Corrigé	329
12	Multiplication de grands objets	333
12.1	Texte	333
12.2	Commentaires	337
12.3	TP	337
12.4	Corrigé	338
13	Permutations et jeu de taquin	343
13.1	Texte	343
13.2	Commentaires	349

13.3 TP	350
13.4 Corrigé	350
14 Énumération de molécules	355
14.1 Texte	355
14.2 Commentaires	360
14.3 TP	361
14.4 Corrigé	361
15 Construction d'un icosaèdre	365
15.1 Texte	365
15.2 Commentaires	369
15.3 TP	369
15.4 Corrigé	369
16 Représentations d'un groupe de matrices	379
16.1 Texte	379
16.2 Commentaires	384
16.3 TP	384
16.4 Corrigé	385
17 La factorisation dans $\mathbb{Z}[X]$	391
17.1 Texte	391
17.2 Commentaires	395
17.3 TP	395
17.4 Corrigé	395
18 Racines réelles d'un polynôme réel	401
18.1 Texte	401
18.2 Commentaires	404
18.3 TP	404
18.4 Corrigé	404
19 La décomposition de Dunford	409
19.1 Texte	409
19.2 Commentaires	413
19.3 TP	414
19.4 Corrigé	414
20 Paramétrisation d'une courbe	419
20.1 Texte	419
20.2 Commentaires	423

20.3 TP	423
20.4 Corrigé	424
21 Enveloppes de courbes	431
21.1 Texte	431
21.2 Commentaires	435
21.3 TP	435
21.4 Corrigé	436
22 Un théorème de Poncelet	445
22.1 Texte	445
22.2 Commentaires	451
22.3 TP	451
22.4 Corrigé	452
23 Logarithme discret	459
23.1 Texte	459
23.2 Commentaires	463
23.3 TP	463
23.4 Corrigé	464
24 Un problème de sac-à-dos	469
24.1 Texte	469
24.2 Commentaires	474
24.3 TP	475
24.4 Corrigé	476
25 Codes cycliques auto-orthogonaux	479
25.1 Texte	479
25.2 Commentaires	483
25.3 TP	483
25.4 Corrigé	484
III Annexe	487
26 Introduction à SageMath	489
26.1 Exercices	490
26.2 Corrigés	497
Bibliographie	506
Index	508