

MATHÉMATIQUES à l'Université

Cours et exercices corrigés

Collection dirigée par
Charles-Michel Marle
Philippe Pilibossian

Algèbre et théorie des nombres

Théorie de Galois & Codes
Géométrie & Arithmétique

niveau M1 et M2

Sabah Al Fakir



MATHÉMATIQUES À L'UNIVERSITÉ

Collection dirigée par Charles-Michel MARLE et Philippe PILIBOSSIAN

niveau M1-M2

M 529 / 1

ALGÈBRE ET THÉORIE DES NOMBRES

Théorie de Galois & Codes
Géométrie & Arithmétique

Sabah AL FAKIR

Professeur émérite

Université scientifique et technique de Lille



25088 1/10



Table des matières

	Notations	x
1	Compléments sur les groupes	1
1.1	Groupes d'opérateurs	1
1.2	Groupes symétriques	3
1.3	Groupes de Sylow	7
1.3.1	p -groupes	7
1.3.2	p -sous-groupes de Sylow	9
1.3.3	Sous-groupes d'un p -groupe	12
1.3.4	Reconstruction d'un groupe	13
1.4	Groupes résolubles	16
1.5	Groupes libres	20
1.5.1	Groupes définis par générateurs et relations	23
1.5.2	Quelques exemples	23
1.6	Note historique sur les groupes	24
1.7	Exercices	25
2	Compléments d'Algèbre commutative	29
2.1	Degré de transcendance	29
2.1.1	s -dimension	30
2.1.2	Conjecture de Schanuel	32
2.2	Théorie de l'élimination	33
2.2.1	Résultant	33
2.2.2	Calcul pratique du résultant	35
2.2.3	Théorème de Bézout affine	38
2.3	Théorème des zéros de Hilbert	40
2.4	Exercices	42
3	Théorie de Galois	43
3.1	Correspondances de Galois	43
3.2	Extensions galoisiennes	44
3.3	Extensions normales	46
3.4	Cas des corps finis	49
3.5	Groupe de Galois d'une équation algébrique	49
3.6	Extensions cyclotomiques	50
3.6.1	Généralités	50
3.6.2	Calcul des polynômes cyclotomiques	52
3.6.3	Polynômes cyclotomiques sur \mathbb{Q}	52
3.6.4	Polynômes cyclotomiques sur \mathbb{F}_q	54
3.7	Equations binômes	56

3.8	Equations résolubles par radicaux	57
3.8.1	Introduction	57
3.8.2	Un point d'histoire.	57
3.8.3	Clôture normale	58
3.8.4	Théorème de Galois	59
3.9	Trace et Norme	61
3.9.1	Théorème 90 de Hilbert	64
3.10	Equation du troisième degré	66
3.11	Equation du quatrième degré	68
3.12	Applications à la constructibilité	70
3.13	Calcul du groupe de Galois	71
3.13.1	Méthode de Van Der Waerden	71
3.13.2	Calcul du groupe de Galois avec Maple	73
3.14	Théorème fondamental de l'Algèbre	74
3.15	Note historique	76
3.16	Exercices	80
4	Corps de Nombres	83
4.1	Un point d'histoire	83
4.2	Discriminant	84
4.3	Corps de nombres	85
4.3.1	Plongements	85
4.3.2	Module $O_{\mathbb{K}}$	86
4.3.3	Corps cubiques purs	89
4.3.4	Corps cyclotomiques	89
4.3.5	Unités	90
4.3.6	Problème de la factorialité	92
4.4	Anneaux de Dedekind	92
4.4.1	$O_{\mathbb{K}}$ est un anneau de Dedekind	93
4.4.2	Groupe des idéaux fractionnaires	94
4.4.3	Ramification	98
4.5	Nombres de classes	101
4.5.1	Résultats complémentaires	104
4.6	Compléments sur les anneaux de Dedekind	105
4.7	Exercices	106
5	Théorème de Dirichlet	109
5.1	Caractères d'un groupe	109
5.1.1	Caractères modulaires.	111
5.1.2	Séries de Dirichlet	112
5.2	Théorème de Dirichlet	114
5.2.1	Cas $b = 4$	116
5.3	Exercices	118
6	Codage correcteur d'erreurs	119
6.1	Généralités	119
6.1.1	Introduction	119
6.1.2	Détection des erreurs	119
6.1.3	Distance de Hamming	120

6.1.4	Stratégie de décodage	121
6.1.5	Problème central du codage	123
6.1.6	Constructions de codes	124
6.2	Théorème de Shannon	125
6.2.1	Entropie d'une variable aléatoire	126
6.3	Codes linéaires	128
6.3.1	Code dual	130
6.3.2	Décodage par syndrome	131
6.3.3	Décodage par majorité logique	132
6.3.4	Codes de Hadamard	133
6.3.5	Codes de Reed-Muller	135
6.3.6	Codes de Hamming	136
6.3.7	Codes MDS	137
6.4	Codes cycliques	137
6.5	Zéros d'un code cyclique	141
6.6	Codes BCH	143
6.7	Codes de Reed-Solomon	143
6.7.1	Premier procédé d'encodage	144
6.7.2	Décodage	145
6.7.3	Correction des erreurs dans les codes BCH	146
6.8	Exercices	147
7	Groupes et Géométries	149
7.1	Groupes linéaires	149
7.1.1	Homothéties et centre	150
7.1.2	Homologies	151
7.1.3	Générateurs de $GL(V)$ et $SL(V)$	154
7.1.4	Groupes dérivés	155
7.1.5	Simplicité de $PSL(V)$	156
7.2	Formes quadratiques	157
7.2.1	Bases orthogonales	160
7.2.2	Groupe f -orthogonal	162
7.2.3	Théorème de Cartan-Dieudonné	164
7.2.4	Résultats sans démonstration	166
7.3	Espaces homogènes et affines.	167
7.3.1	Barycentres	168
7.3.2	Sous-espaces affines	169
7.3.3	Parallélisme	170
7.3.4	Géométrie dans un espace affine de dimension 2	170
7.3.5	Repères affines	172
7.3.6	Coordonnées barycentriques	173
7.3.7	Applications affines	174
7.4	Groupe affine	176
7.4.1	Dilatations	176
7.4.2	Homologies	178
7.4.3	Générateurs du groupe affine	180
7.4.4	Cas de la dimension 2	181
7.4.5	Théorème fondamental de la géométrie affine.	182
7.5	Géométrie projective intrinsèque	183

7.5.1	Projections coniques	
7.5.2	Espaces quasi-projectifs	
7.5.3	Dualité naïve dans un plan	
7.5.4	Quelques configurations	
7.6	L'espace projectif $\mathbb{P}(V)$	
7.6.1	Homographies	
7.6.2	Repères projectifs	
7.7	Birapport	
7.8	Liaison affine-projectif	
7.8.1	Complétion projective d'un espace affine	
7.8.2	Envoi d'un hyperplan à l'infini	
7.8.3	Homologies projectives	
7.9	Exercices	
8	Courbes algébriques planes	
8.1	Anneaux sur les variétés affines	
8.2	Corps de fonctions d'une variable	
8.3	Anneaux de valuation discrètes	
8.3.1	Localisation	
8.3.2	Caractérisations d'un anneau de Dedekind	
8.3.3	Anneaux de valuations d'un corps de fonctions	
8.4	Anneau local en un point d'une courbe algébrique	
8.5	Algèbre affine	
8.6	Complétion projective des courbes affines	
8.7	Multiplicité d'intersection	
8.8	Points d'inflexion	
8.9	Exercices	
9	Nombres congruents & Courbes elliptiques	
9.1	Nombres congruents	
9.1.1	Histoire des nombres congruents	
9.2	Courbes elliptiques	
9.2.1	Equations de Weierstrass	
9.2.2	Loi d'addition de Newton-Poincaré	
9.2.3	Retour aux corps de nombres	
9.2.4	Théorème de Mordell-Weil faible	
9.2.5	Hauteurs	
9.2.6	Théorème de Mordell-Weil	
9.2.7	Courbes elliptiques sur \mathbb{C}	
9.3	Courbes E_n	
9.4	Fonctions Zêta et L	
9.4.1	Théorème de Tunnel	
9.5	Courbes elliptiques, primalité et factorisation	
9.6	Exercices	
9.7	Références pour ce chapitre	

10 Solutions des exercices	263
10.1 Chapitre 1	263
10.2 Chapitre 2	268
10.3 Chapitre 3	268
10.4 Chapitre 4	274
10.5 Chapitre 5	277
10.6 Chapitre 6	279
10.7 Chapitre 7	280
10.8 Chapitre 8	284
10.9 Chapitre 9	287
Bibliographie	289
Index	291

La collection *Mathématiques à l'Université* se propose de mettre à la disposition des étudiants de troisième, quatrième et cinquième années d'études supérieures en 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.

Cet ouvrage est la suite de *Algèbre et théorie des nombres. Cryptographie, Primalité* paru dans la même collection. Il est cependant largement indépendant de ce tome, grâce à des rappels fréquents.

Il commence par un traitement classique de la théorie de Galois avec ses deux volets : théorie des groupes et celle des extensions de corps. Certaines questions se trouvent ici particulièrement approfondies, notamment le calcul du groupe de Galois d'une équation algébrique, le caractère algébriquement clos du corps des nombres complexes, les bases intégrales des anneaux d'entiers des corps de nombres, le théorème de Dirichlet sur les nombres premiers dans une progression arithmétique...

Il se poursuit par une étude introductive à la théorie moderne des codes correcteurs d'erreurs : théorème de Shannon, problème central du codage, codes linéaires et codes cycliques. La notion de classe cyclotomique dans un corps fini trouve ici des applications intéressantes.

Le dernier tiers est consacré à la géométrie et à ses liens avec l'arithmétique. Après une étude des groupes classiques et des géométries affines et projectives, on passe aux courbes algébriques planes, aux courbes elliptiques et aux nombres congruents. On fait le point sur ces nombres dont la détermination reste un problème majeur de la géométrie arithmétique et encore largement ouvert.

Ce livre a été conçu à l'origine pour les étudiants du second cycle et pour les candidats à l'agrégation. Les deux derniers chapitres s'adressent plutôt aux étudiants des masters (niveau 2) et aux enseignants.

