

TRAITÉ
DE MATHÉMATIQUES

KHELIFA ZIZI

GROUPES
ANNEAUX CORPS

LIVRE 03



OFFICE DES PUBLICATIONS UNIVERSITAIRES



Table des matières

1	Notions générales sur les groupes	7
1.1	Groupe - Exemples de groupes	7
1.2	Sous-groupe	19
1.2.1	Système de générateurs d'un groupe	20
1.2.2	Noyau et Image d'un homomorphisme	23
1.2.3	Générateurs du groupe symétrique - Le sous-groupe alterné A_n	23
1.2.4	Cycles - Décomposition en produit de cycles	25
1.2.5	Fonctions Mathematica concernant le groupe symétrique	31
1.3	Classe suivant un sous-groupe - Indice d'un sous-groupe - Théorème de Lagrange	31
1.4	Sous-groupe normal - Groupe quotient	36
1.4.1	Normalisateur, sous-groupe caractéristique	40
1.4.2	Simplicité du groupe alterné A_n , $n \geq 5$	42
1.4.3	Propriétés des sous-groupes normaux	43
1.4.4	Propriétés des groupes quotients	46
1.4.5	Sous-groupes d'un groupe quotient	47
1.5	Deuxième et troisième théorèmes d'isomorphismes	49
1.6	Groupes monogènes et groupes cycliques	51
1.6.1	Générateurs d'un groupe monogène	54
1.7	Produit de groupes - Produits directs et semi-directs de groupes	55
1.7.1	Groupe produit de groupes	55
1.7.2	Produit direct de sous-groupes	57
1.7.3	Produit semi-direct de groupes	62
2	Groupe libre- Groupe de Sylow- Groupe abélien de type fini- Groupe résoluble	71
2.1	Groupe libre - Présentation d'un groupe	71
2.2	Classification des groupes d'ordre inférieur à huit	77
2.3	Représentation de groupe - Groupe opérant sur un ensemble	82
2.4	Théorèmes de Sylow	88
2.5	Groupes abéliens de type fini	93
2.6	Groupe résoluble	98
2.7	Exercices sur les groupes	105
3	Congruences linéaires et quadratiques	129
3.1	Généralités sur les congruences	129
3.2	Congruence linéaire - Théorème chinois des restes	135
3.3	Utilisation des fractions continues	138

3.3.1	Une application du petit théorème de Fermat : Le code R.S.A	149
3.4	Congruences de degré supérieur ou égal à 2	150
3.5	Congruences quadratiques	159
3.6	Exercices sur les congruences	162
4	Notions générales sur les anneaux et les corps	169
4.1	Anneau - Idéal - Anneau int�grit� - Anneau principal	169
4.2	Domaine principal	173
4.3	Anneaux noeth�riens	175
4.4	Divisibilit� dans un domaine d'int�grit�	176
4.5	p.g.c.d et p.p.c.m dans un domaine d'int�grit�	178
4.6	Anneaux factoriels	186
4.7	Anneaux euclidiens	188
4.7.1	Nombres premiers dans l'anneau de Gauss $\mathbb{Z}[i]$	189
4.7.2	D�composition d'un entier en somme de deux carr�s d'entiers	190
4.7.3	D�composition d'un nombre entier en somme de quatre (resp. trois) carr�s	192
4.8	Corps premier - Caract�ristique d'un corps	195
4.8.1	Corps des fractions d'un domaine d'int�grit�	195
4.9	Exercices sur les anneaux et corps	198
5	Anneau des polyn�mes	215
5.1	Anneau des polyn�mes � une ind�termin�e	215
5.2	Anneau des polyn�mes � plusieurs ind�termin�es	220
5.2.1	Ordre lexicographique dans $A[X_1, X_2, \dots, X_m]$	223
5.3	Polyn�mes � m ind�termin�es sym�triques	226
5.4	Division euclidienne dans l'anneau des polyn�mes	233
5.4.1	Division suivant les puissances croissantes dans $K[X]$	236
5.5	Polyn�mes irr�ductibles	244
5.6	Polyn�me d�riv� - Formule de Taylor	250
5.6.1	Equations alg�briques - R�sultant	261
5.6.2	Discriminant d'un polyn�me	267
5.6.3	Transformation des �quations	271
5.7	Polyn�mes d'interpolation	273
5.8	Exercices sur les polyn�mes et les fractions rationnelles	279
6	Le corps des nombres complexes	297
6.1	Le corps des nombres complexes	297
6.2	Une autre d�finition du corps des nombres complexes	299
6.3	Le th�or�me de d'Alembert-Gauss	301
6.4	Racines rationnelles d'un polyn�me $P \in \mathbb{Z}[X]$	304
6.5	R�solution des �quations du 3-�me degr� par radicaux	306
6.6	R�solution des �quations du 4-�me degr�	310
6.7	Corps des fractions rationnelles	313
6.8	Exercices sur les racines des �quations dans \mathbb{C}	319

7	Extensions de corps	331
7.1	Extension d'un corps	331
7.1.1	Extension simple	338
7.1.2	Construction d'extensions simples	339
7.1.3	Extension de degré fini	343
7.1.4	Le corps \bar{K} des éléments algébriques sur K	346
7.2	Clôture algébrique	348
7.3	Corps quadratiques	351
7.4	Loi de réciprocité quadratique	356
7.4.1	Reste de degré n modulo p , Reste quadratique	356
7.4.2	Symbole de Legendre	358
7.5	Exercices sur les extensions de corps	364
8	Éléments de la théorie de Galois	369
8.1	Corps des racines d'un polynôme irréductible	369
8.2	Extensions normales, Groupe de Galois	375
8.3	Le théorème fondamental de Galois	386
8.4	Equation résoluble par les radicaux	401
8.4.1	Etude de l'équation de degré un nombre premier à coefficients dans \mathbb{Q}	405
8.5	Exercices sur la théorie de Galois	409
9	Les équations de Fermat $x^n + y^n = z^n$ pour $2 \leq n \leq 4$	415
9.1	Etude de l'équation $x^2 + y^2 = z^2$	415
9.2	Etude de l'équation $x^4 + y^4 = z^4$	417
9.3	Etude de l'équation $x^3 + y^3 = z^3$	418
9.4	Construction de polygones réguliers - Nombres de Fermat	423
9.4.1	Points constructibles	425
9.5	Polygones réguliers constructibles et non constructibles	429
9.6	Exercices sur l'équation de Fermat	436
10	Corps finis - Application aux codes correcteurs d'erreurs	441
10.1	Théorème de Wedderburn - Polynômes cyclotomiques	441
10.1.1	Les corps finis à 4, 9, 25, 8, 16, 32 éléments	447
10.1.2	Sous-corps d'un corps fini - Classes de cyclotomie	450
10.2	Introduction aux codes détecteurs et correcteurs d'erreurs	454
10.2.1	Codage de l'information	454
10.2.2	Mots de code - Encodage	455
10.2.3	Code linéaire : matrice de contrôle et matrice génératrice	456
10.2.4	Codes de Hamming	459
10.2.5	La matrice génératrice	463
10.2.6	Matrice génératrice d'un code linéaire systématique	470
10.2.7	Code orthogonal d'un code linéaire	472
10.3	Décodage et Correction des erreurs	472
10.3.1	Distance de Hamming	472
10.3.2	Décodage par le tableau standard	475
10.3.3	Décodage par la méthode du syndrome	477
10.3.4	Le code de Hamming	478
10.3.5	Les codes cycliques	480

10.3.6	Les codes BCH	486
10.3.7	Les codes de Reed-Muller	487
10.4	Exercices sur les codes détecteurs et correcteurs d'erreurs	490