Mohamed ZITOUNI

# GEOMETRIE ARITHMETIQUE ET ALGORITHMIQUE DES COURBES ELLIPTIQUES

*Office des Publications Universitaires*

**Professeur Mohamed ZITOUNI**
*Faculté de Mathématiques – USTHB*



# GEOMETRIE ARITHMETIQUE ET ALGORITHMIQUE DES COURBES ELLIPTIQUES

OFFICE DES PUBLICATIONS UNIVERSITAIRES
*1, Place centrale de Ben-Aknoun (Alger)*

**Chapitre I : VARIETES ALGEBRIQUES** 13
1- Introduction; 13
2- Variétés algébriques; 13
3- Espaces Affines; 13
4- Ensembles Algébriques;. 14
5- Topologie de Zariski; 15
6- Compacité et connexité; 16
7- Variétés Affines; 17
8- Variétés Projectives; 19
9- Variétés Abéliennes; 20
10- Variétés non singulières 21

**Chapitre II : DIVISEURS DE VARIETES** 25
1- Diviseurs d'une Variété; 25
2- Diviseurs dans le corps K(X) ; 26
3- Groupe de Picard; 27
4- Diviseurs des courbes algébriques; 28
5- Diviseurs d'un Schéma; 29
6- Diviseurs de l'invariant différentiel. 30

**Chapitre III : SCHEMAS** 33
1- Préfaisceaux de groupes ; 33
2- Faisceaux ; 33
3- Topologie spectrale 34
4- Schémas; 35
5- Faisceaux de modules; 36
6- Diviseurs de Cartier; 37
7- Cohomologie de groupes; 38
8- Groupes gradués différentiels; 39
9- Groupes de cohomologie 40
10- G- complexes; 42
11- Groupes de G dans A ; 43
12- Restriction et inflation. 45

**Chapitre IV : COURBES ALGEBRIQUES** 49
1- Terminologie ; 49
2- Diviseurs d'une courbe ; 49
3- Singularités ; 49
4- Structures et genres 52

**Chapitre V : EQUATIONS-INVARIANTS** 55
1- Structures algébriques; 55
2- Changements de variables ; 56
3- Invariants ; 57
4- Classification des cubiques 60

**Chapitre VI :GROUPES DE MORDELL – WEIL** 71
1- Structure de groupe abélien ; 71
2- Coordonnées du symétrique et de la somme; 72
3- Points d'ordre fini ; 74
4- Groupe de Galois et théorie de Kummer ; 75
5- Torsion sur le corps $\mathbb{Q}$ par Mazur ; 76
6- Nombres congruents ; 78
7- Finitude du groupe quotient E(K) / 2 E(K) ; 83
8- Formules de Cassels des points m P; 83
9- Formules de Lang des points m P ; 86
10- Corps des points de N - division . 87

**Chapitre VII : HOMOMORPHISMES** 91
1- Morphismes de Variétés ; 91
2- Isomorphismes ; 92
3- Relations d'isomorphismes; 93
4- Automorphismes; 96
5- Isogénies ; 99
6- Technique de Velu ; 102
7- Isogénies et application de Weil; 107
8- Endomorphismes ; 108

9- Courbes Elliptiques à Multiplication Complexe ; 110
10- Points d'ordre fini et racines de l'unité ; 113
11- Module de Tate . 115

**Chapitre VIII : RESEAUX COMPLEXES** 117
1- Réseaux ; 117
2- Fonctions Elliptiques ; 119
3- Réseaux L et Courbes Elliptiques associées E(L ) 123

**Chapitre IX:VALUATIONS - REDUCTIONS** 127
1- Valuations d'un corps ; 127
2- Valuations équivalentes ; 129
3- Completion d'un corps ; 129
4- Classification des valuations ; 130
5- Valuations non archimédiennes ; 131
6- Valuations additives; 132
7- Corps locaux; 132
8- Extension des valuations; 133
9- Réductions des courbes elliptiques; 133
10- Réductions d'équations de Weierstrass; 133
11- Classification des réductions ; 134
12- Réductions et sous groupes de E(K). 137

**Chapitre X : HAUTEURS- RANGS** 141
1- Hauteur sur un groupe abélien; 141
2- Descente infinie; 141
3- Hauteur sur $\mathbb{Q}$, sur le plan projectif $\mathbb{P}^2$ 144
4- Hauteur de Weil et hauteur de Neron-Tate; 145
5- Hauteurs locales; 147
6- 2-descente 150
7- Rang r (E) 151
8- Rang analytique 155

**Chapitre XI : GROUPE MODULAIRE** 169
1- Introduction; 169
2- Transformations rationnelles du demi plan supérieur IH 170
3- Groupe modulaire = SL(2 ;ℤ); 171
4- Fonctions automorphes ; 177
5- Fonctions modulaires ; 178
6- Formes modulaires ; 179
7- Fonction Eta de Dedekind ; 182
8- Structures des espaces de formes modulaires; 183
9- Opérateurs de Hecke ; 184
10- Formes modulaires et séries de Dirichlet; 180
11- Courbes modulaires; 188
12- Symboles modulaires. 195

**Chapitre XII : TWISTS - GROUPES DE CHÂTELET-WEIL** 199
1- Twists ; 199
2- Espaces homogènes ; 202
3- Groupes de Châtelet - Weil ; 205
4- Groupes de Selmer et de Shafarevich-Tate ; 205

**Chapitre XIII:COURBES ELLIPTIQUES SUR CORPS FINIS** 215
1- Structures d'un corps fini ; 215
2- Endomorphisme de Frobeniüs ; 216
3- Groupe formel d'une courbe elliptique ; 218
4- Groupe de Mordell - Weil E(IF_{q}); 221
5- Groupes de torsion et endomorphismes ; 222
6- Courbes elliptiques supersingulières ; 224
7- Fonctions Zéta et séries L(E;s) de Dirichlet-Hasse; 228

**Chapitre XIV : THEORIE ALGORITHMIQUE** 231
1- Nombres de Mersenne ; 231
2- Nombres de Fermat ; 233
3- Logarithmes discrets ; 233
4- Algorithmes et Courbes Elliptiques ; 234

5- Méthode de Schoof ; 241
6- Méthode de Cremona ; 244
7- Méthode de 2- descente ; 247
8- Méthode Galbraith et collaborateurs ; 248
9- Algorithme de Miller ; 250
10- Calculs de S - points ; 252
11- Calculs sur l'équation triple de Fermat ; 258

**REFERENCES** 261

**EXERCICES** 270

**INDEX** 279

Le Professeur ZITOUNI Mohamed a soutenu une thèse de Doctorat de 3ème cycle (Mathématique Pures)-1969, et une thèse de Doctorat ès Science Mathématiques (Doctorat d'Etat) à l'Université de Besançon (France)-1973.
Il est Professeur de l'Enseignement Supérieur titulaire à compter du 10/09/1977.

Il enseigne les mathématiques (Algèbre, Analyse, Théorie des Nombres, Variétés Statistiques (Universités d'Alger Centre, de Boumerdes, U.S.T.H.B.)

Il enseigne en graduation et en post graduation.

Il a dirigé et faire soutenir plus de 40 Magistèrs en Mathématiques (Théorie des Nombres – Courbes Elliptiques)

Ses activités de recherche en mathématiques sont matérialisées dans des projets de recherche officiels des communications dans des Séminaires et des Colloques, des publications de la Faculté, une monographie (Théorie des Nombres ) et une autre « Statistiques pour 1ère année et résidents de pharmacie), un ouvrage « Algèbre-1ère année universitaire (OPU-1986) », un ouvrage « Problèmes d'examen corrigés (OPU-1992 »

Cet ouvrage s'adresse à tous ceux qui ont des connaissances en Algèbre Commutative et en Théorie des Nombres algébriques et qui sont intéressés par les Courbes Elliptiques. Le sujet central est la théorie des Courbes Elliptiques.

www.opu-dz.com

9 789961 010303

350 DA

Edition: 4691