Le sujet de ma thèse concerne des algorithmes de calcul d'isogénies des Courbes Elliptiques.

La théorie des Courbes Elliptiques est basée sur les domaines des Courbes Algébriques planes, de la théorie des Nombres Algébriques (structure de groupe,…) , de la théorie des Nombres Analytiques (fonction zêta de RIEMANN, fonctions arithmétiques), de la théorie des Nombres Géométriques (points singuliers, points ordinaires), de la Géométrie Algébrique (Variétés Abéliennes, Variétés Projectives).

Les Courbes Elliptiques ont intéressé de nombreux chercheurs :
CASSELS [1], MAZUR [10], SILVERMAN [13], TATE[14], ZITOUNI[17],etc..

Certaines Courbes Elliptiques ont été utilisées pour des applications en codage, en cryptographie. Elles ont été utilisées par WILLES pour démontrer le théorème de FERMAT.

Ma thèse est composée de 3 chapitres :

Dans le chapitre I j'ai abordé les propriétés Algébriques et Arithmétiques des équations de WEIERSTRASS, les invariants. J'ai construit une loi de groupe additif abélien sur l'ensemble E(K) des points K-rationnels des courbes au moyen de la règle géométrique de ″3 points colinéaires des Courbes Elliptiques″.
J'ai obtenu les formules des coordonnées du symétrique –P, de la somme P+R et de la somme 2P des points P et R de ces courbes.
Ce groupe de MORDELL-WEIL a une structure de groupe additif abélien de type fini.
J'ai utilisé les travaux de SILVERMAN pour préciser quelques propriétés de ces groupes.

Dans le chapitre II j'ai établi les propriétés de quelques homomorphismes des Courbes Elliptiques : Isomorphismes, Endomorphismes, Automorphismes.

Dans le chapitre III j'ai étudié quelques propriétés des isogénies des Courbes Elliptiques. J'ai utilisé quelques algorithmes de calcul d'isogénies :
Algorithme de B. MAZUR, Technique de VELU.