UNIVERSITE MENTOURI DE CONSTANTINE

DEPARTEMENT DE MATHEMATIQUE DE LA FACULTE DES SCIENCES

N°: D'ordre :……..
Série :…….

MEMOIRE

Présenté

Par Tayeb HAMAIZIA

POUR L'OBTENTION DU DIPLOME
DE MAGISTER EN MATHEMATIQUE
OPTION: TOPOLOGIE ALGEBRIQUE

SUJET :

GROUPE DE TORSION DE COURBE ELLIPTIQUE SUR UNE EXTENSION QUADRATIQUE DU CORPS ¥

SOUTENU LE : ……../……./…….

DEVANT LE JURY

- **PRESIDENT** : **M^r** RAHMANI Fouad Lazhar, Maitre de Conférence
  U. Mentouri de Constantine
- **RAPPORTEUR** : **M^r** ZITOUNI Mohamed, Professeur USTHB d'Alger.
- **EXAMINATEURS: M^r** BENKAFADAR Mohamed Naceredine, Professeur
  U. Mentouri Constantine
  M^elle BOUGHABA Soraya, Maitre de Conférence
  U. Mentouri Constantine

Remerciements

Tout d'abord je voudrais exprimer ma plus profonde reconnaissance à mon directeur de thèse, Mohamed ZITOUNI, pour son soutien, pour ses conseils chaleureux et pour toutes les mathématiques qu'il m'a apprises.

Ensuite je voudrais remercier les membres de mon jury d'avoir accepté d'évaluer mon travail, de s'y s'être intéresse, pour leur remarques, et encouragements.

Je remercie enfin toutes les personnes qui ont contribué d'une manière ou d'une autre à me permettre de faire cette thèse, et parmi eux ma famille.

TABLE DES MATIERES

CHAPITRE I : VARIETES ALGEBRIQUES ABELIENNES ……01

1. Variétés affines ……..01
2. Variétés projectives ……..04
3. Variétés abéliennes ……06
4. Courbes algébriques ……06

CHAPITRE II: ARITHMETIQUES DES COURBES ELLIPTIQUES……..09

1. Equation de Weierstrass ……09
2. Invariants des courbes irréductibles ……10
3. Discriminants…… ……..12
4. Résultants de 2 polynômes ……..14
5. Cubiques irréductibles singulières ……16
6. Courbes elliptiques ……...19
7. Classification des cubiques irréductibles avec $\Delta(E)$ et $c_4(E)$ ……..20

CHAPITRE III: GROUPE DE MORDELL-WEIL D'UNE COURBE ELLIPTIQUE ……...25

1. Structure de groupe abélien sur l'ensemble E (K) ……25
2. Coordonnées de –P et de P_1+P_2 ……...26
3. Point de E d'ordre fini ……..27
4. Finitude du groupe quotient E(K)/mE(K) ……...31
5. Hauteurs sur une courbe elliptique ……...32
6. Valuations d'un corps et réduction de courbes elliptiques ……...36

CHAPITRE IV: TORSION DE COURBE ELLIPTIQUE ……..39

1. Corps de nombres algébriques quadratiques……..39
2. Torsion du groupe de Mordell-Weil E(K) ……40
3. Isomorphismes de courbes elliptiques ……..43
4. Groupe de torsion sur un corps quadratique ……43
5. Algorithme de calcul……45

REFERENCE ……..47

INTRODUCTION

Ce mémoire traite des variétés algébriques, des cubiques de Weierstrass, des courbes elliptiques.

Le chapitre I, est une description des variétés et le lien avec les courbes elliptiques.

Dans le chapitre II, j'ai exposé quelques points de l'arithmétique des courbes elliptiques; j'ai omis les isogénies, les automorphismes, les tores complexes.

Dans le chapitre III, j'ai établi la loi de groupe de Mordell-Weil avec la règle géométrique de 3 points colinéaires de la courbe elliptique E et le point à l'infini O_E. J'ai calculé les formules des coordonnées du symétrique –P de la somme P_1+P_2 et du point 2P, j'ai introduit une fonction hauteur h : E (K)→ ♣ pour obtenu le théorème de Mordell-Weil. Le groupe E (K) est de type fini.

Dans le dernier chapitre j'ai décrit la structure d'un corps quadratique. Enfin j'ai traité les groupes de torsion T(E) (K) en utilisant plusieurs méthodes.

Deux exemples de calcul algorithmique du groupe T(E)(Q) de torsion terminent ce mémoire.

CHAPITRE I : VARIETES ALGEBRIQUES ABELIENNES ET COURBES ALGEBRIQUES

Les variétés algébriques sont du domaine de la géométrie algébrique.
Elles sont traitées dans des nombreux ouvrages comme [3], [4], [5], [7], [14-2][15], [19].

Pour les étudier, nous nous sommes inspirés principalement de l'ouvrage de Hartshorne.

Puisque nous n'étudions que des variétés algébriques, dans notre thèse nous omettrons l'adjectif " algébriques " dans les variétés affines, variétés projectives, variétés abéliennes, variétés de groupes, variétés normales, variétés non singulières, variété de Nagata, variété jacobienne, variété de Picard, etc…

1- VARIETES AFFINES

Les variétés sont construites sur des espaces affines avec la topologie de Zariski.

DEFINITION 1:

Un espace affine, sur un corps algébriquement clos K, est l'ensemble des n-uples $a = (a_1, a_2,\ldots, a_n)$ *d'éléments* a_i *du corps K.*

$$\mathbb{A}^n(K) = \{a = (a_1, a_2,\ldots, a_n) \text{ où } a_1, a_2,\ldots,a_n \text{ dans } K\}\ldots\ldots\ldots\ldots\ldots(1)$$

On utilise le langage géométrique pour désigner des éléments des espaces affines.

Le n-uple *a* est un point de l'espace affines $\mathbb{A}^n$ (K) de coordonnées $a_1,\ldots,a_n$.

DEFINITION 2:

Un corps algébriquement clos est un corps commutatif K tel que tout Polynôme f(x) de l'anneaux K[x], de degré d, admet d racines dans le corps.

Le polynôme $f(x) = x^2+1$ n'admet pas de racines réelles; donc il est irréductible dans l'anneau ♣[x]. Le corps ♣ n'est donc pas algébriquement clos.

Le polynôme $f(x) = x^2+1$ admet 2 racines complexes $\pm i$, il est donc décomposable dans l'anneau $\mathbb{C}[x]$ sous forme $f(x) =(x+i)(x-i)$ donc $\mathbb{C}$ algébriquement clos.

Un espace affine $\mathbb{A}^n(K)$ est muni de 2 lois semblables aux lois d'un espace vectoriel.

Une addition $\mathbb{A}^n(K) \times \mathbb{A}^n(K) \rightarrow \mathbb{A}^n(K)$

$$(a= (a_1\ldots, a_n), b= (b_1\ldots b_n)) \rightarrow a+ b= (a_1+b_1,\ldots,a_n+ b_n) \ldots\ldots\ldots\ldots(2)$$

Avec le point 0= (0,..,0) de coordonnées nulle,

Une multiplication externe: $K \times \mathbb{A}^n(K) \rightarrow \mathbb{A}^n(K)$

$$(l, a) \mapsto l.a = (la_1, la_2, \ldots, la_n) \ldots\ldots\ldots(3)$$

L'espace affine $\mathbb{A}^n(K)$ est associe à l'anneau de polynômes à n indéterminées

$$B_n = K[x_1, x_2, \ldots, x_n] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4)$$

L'espace affine $\mathbb{A}^n(K)$ possède un invariant, une dimension, comme l'espace vectoriel.

Il est de dimension n.

Tout polynôme $f(x) \in C[x]$ possède des zéros.

Tout polynôme $f(x) \in K[x_1, x_2, \ldots, x_n] = B_n$ possède des zéros.

DEFINITION 3 :

Un ensemble algébrique dans un espace affine $\mathbb{A}^n(K)$ est un ensemble X de zéros d'une famille de polynômes $f_i \hat{I} B_n$.

$$X = \{ P \hat{I} \mathbb{A}^n(K) ; f_1(P) = \ldots = f_d(P) = 0 \} \ldots\ldots\ldots\ldots\ldots(5)$$

PROPOSITION 1 :

Soient 2 familles de polynômes F_1et F_2 dans B et 2 ensembles algébriques X_1 et X_2.

1) *la réunion de 2 ensembles algébrique $X_1 È X_2$ est un ensemble algébrique.*
2) *L'intersection d'une famille d'ensembles algébriques est un ensemble algébrique.*
3) *L'ensemble vide et l'espace affine $\mathbb{A}^n(K)$ sont des ensembles algébriques.*
4) *L'inclusion $F_1 Ì F_2$ de polynômes implique l'inclusion des ensembles algébriques $X(F_1) É X(F_2)$.*

Preuve :

L'ensemble algébrique X ($f \subset B_n$) pour $f = 0x_1 + \ldots + 0x_n$ est l'espace affine $\mathbb{A}^n(K)$

L'ensemble algébrique X ($f \subset B_n$) pour $f = 1$ est l'ensemble vide.

Dans un anneau B, il y a des sous ensembles particuliers :

Les sous anneaux et les idéaux.

L'idéal engendré par un élément *f* est l'ensemble I=*f* B.

La proposition 1 relative aux ensembles algébriques permet de définir une topologie sur l'espace affine $\mathbb{A}^n$ (K) : la topologie de Zariski.

DEFINITION 4 :

Sur un espace affine $\mathcal{A}^n$ (K), la topologie de Zariski est déterminée par les ensembles algébriques comme des fermés et leurs complémentaires comme des ouverts.

Cette topologie satisfait les axiomes d'une topologie.

Elle n'est pas de Hausdorf.

L'ensemble vide et l'espace affine $\mathbb{A}^n$ (K) sont fermés et ouverts à la fois.

L'espace affine $\mathbb{A}^n$ (K) muni de la topologie de Zariski devient un espace topologique.

DEFINITION 5 :

Une variété affine est un sous ensemble Y d'un espace affine $\mathcal{A}^n$ (K) Irréductible et fermé.

Donc la réunion $Y_1 \cup Y_2$ de 2 variétés affines n'est pas une variété affine

EXEMPLES

1- un polynôme $f \in K[x, y]$ irréductible une variété affine dans l'espace $\mathbb{A}^2$ (K). c'est une courbe affine X (*f*).
2- dans un espace affine $\mathbb{A}^3$ (K), la variété affine est une surface.
3- Dans un espace $\mathbb{A}^n$ (K), pour n > 3, la variété affine est une hypersurfece.

Une variété affine Y (F), F = famille de polynômes $f_i \in$ B, admet des invariant qui sont la dimension et l'idéal.

DEFINITION 6 :

L'idéal d'une variété affine Y(F), F Î B=K[x_1,…,x_n], est l'ensemble des polynômes g Î B:

$$I(Y)= \{g \hat{I} K[x_1,\ldots,x_n], \ g(P) = 0 \text{ pour tout point P de Y}\}\ldots\ldots\ldots(6)$$

Une variété affine Y possèdes des sous ensembles particuliers.

DEFINITION 7 :

Soit une variété affine Y (F) Ì Y.

1) *Une sous variété de Y est une partie fermée de la variété.*
2) *Une variété quasi affine est une partie ouverte de la variété.*

2- VARIETES PROJECTIVES

Sur une variété affine $\mathbb{A}^{n+1}$ (K), de dimension n+1, considérons la relation binaire R déterminer par la condition :

$a = (a_1 \ldots, a_{n+1})$ R $b = (b_1 \ldots b_{n+1})$ si et seulement si $a = \lambda b$ pour $\lambda \neq 0$.

Cette relation est réflexive, symétrique et transitive, c'est donc une relation d'équivalence sur l'espace affine $\mathcal{A}^{n+1}(K)$

DEFINITION 8 :

L'espace projectif $P^n(K) = P^n$ est l'espace quotient de l'espace affine $\mathcal{A}^{n+1*}$ par la relation d'équivalence R :

$P^n(K) = \mathcal{A}^{n+1}(K)/R$ = *ensemble des classes modulo R*

La topologie de Zariski s'applique sur l'espace affine $\mathcal{A}^{n+1}(K)$ donc aussi sur l'espace projectif $P^n(K)$.

DEFINITION 9 :

Une variété projective est une partie de l'espace projectif $P^n(K)$,pour $n \geq 1$ Irréductible et fermé.

Un point P d'un espace projectif $P^n(K)$ admet (n+1) coordonnées

$P = (a_1 \ldots, a_{n+1}) \in P^n(K) = \mathcal{A}^{n+1}(K)/R$.

Les polynômes associes à une espace projectif $P^n(K)$ forment l'anneau des polynomes homogènes de degré $d \geq 0$:

$$B_n = [x_1, \ldots, x_{n+1}]$$

L'ensemble des Zéros d'un polynôme homogène $f \in B_n$ est un hyperplan

$$f = \lambda_1 x^1 + \lambda_2 x^2 + \ldots + \lambda_{n+1} x^{n+1} = 0$$

DEFINITION 10 :

Soit une variété projectif $X \subset P^n(K)$.

1- *une sous variété projective est une partie fermée d'une variété projective.*

2- *Une variété quasi projective est une partie ouverte d'une variété projective.*

EXEMPLES :

1) dans l'espace projectif P^2, l'ensemble des zéros du polynôme homogène de degré 3 $f(x, y, z) = x^3 + y^3 + z^3$ est une variété projective.

2) L'ensemble des zéros du polynôme $g(x, y, z) = y^2z + 2xyz - x^3 - 3x^2z + 5z^3$ est une variété projective.

Sa dimension est égale à : Dimension de P^2 – nombre de relations = 2-1=1.

Etablissons les formules de passage $P^n \rightarrow \mathbb{A}^n$

Pour n = 2, par exemple, un point P a pour coordonnées

$$P = (x, y, z) \in P^2.$$

L'application $P^2 \rightarrow \mathbb{A}^2$ est définie par sa valeur

$$(x, y, z) \rightarrow (x, y, 1)$$

Le polynôme projectif $f(x, y, z) = x^3 - 2xy^2 + 3yz^2 - 4z^3 \in P^2$ est

Transformé en polynôme affine.

$$f(x, y, z) = x^3 - 2xy^2 + 3y - 4 = g(x, y) \in \mathbb{A}^2$$

Le passage $\mathbb{A}^2 \rightarrow P^2$ s'obtient par 2 applications

Division par z : $(x, y) \rightarrow \left(\frac{x}{z}, \frac{y}{z}\right)$

Un polynôme $f(x, y) = 4x^3 + 3x^2y - 2xy + 5y^2 - 6$. Devient par division par z

La fraction rationnelle.

$$f\left(\frac{x}{z}, \frac{y}{z}\right) = 4\left(\frac{x}{z}\right)^3 + 3\left(\frac{x^2 y}{z^3}\right) - 2\left(\frac{x\ y}{z^2}\right) + \left(\frac{y^2}{z^2}\right) - 6$$

L'application $f\left(\frac{x}{z}, \frac{y}{z}\right) \rightarrow z^3 f(x, y) = g(x, y, z)$.

Transforme *f* en polynôme homogène.

$$G(x, y, z) = 4x^3 + 3x^2y - 2xyz + 5y^2z - 6z^3 \in P^2.$$

3- VARIETES ABELIENNES

Une variété peut être munie d'une structure de groupe.

DEFINITION 11.

Une variété de groupe est une variété Y munie d'une loi de groupe :

$$Y \acute{} Y \to Y;\ (a, b) \to a + b$$

Et d'une application interne $Y \to Y;\ a \to a^{-1}$

Lorsque cette loi de groupe est un groupe abélien, alors la variété est abélienne.

DEFINITION 12 :

Une variété abélienne est une variété projective avec une loi de groupe et une application inverse.

Cette variété abélienne est de dimension n ≥1.

Certaines variétés abéliennes de dimension 1 sont des courbes elliptiques. La structure de groupe abélien sera décrite dans le chapitre 3.

4 - COURBES ALGEBRIQUES PLANES.

Une courbe algébrique plane est l'ensemble des points $P = (x, y)$ qui satisfait une équation algébrique $f(x, y) \in R[x, y]$ dans le plan affine A^2, le polynôme f(x, y), de degré n, est somme de polynômes $f_d(x, y)$ de degré d……. (1)

Les polynômes homogènes $f_0(x, y)$ sont les constantes.

Les polynômes affines de degré n =1 sont de la forme

$$f(x, y) = r_1 x + r_2 y + r_3; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

f(x, y) = 0 est l'équation d'une droite.

Pour n = 2, $f(x, y) = = r_1 x^2 + r_2 x y + r_3 y^2 + r_4 x + r_5 y + r_6. = 0 \ldots\ldots\ldots\ldots\ldots(3)$

Est l'équation d'une cercle ou d'une conique lorsque le polynôme est irréductible.

Lorsqu'il est réductible, la courbe dégénère en un produit de 2 droites;

$$f(x, y) = (r_1 x + r_2 y + r_3)(r_4 x + r_5 y + r_6); \ldots\ldots\ldots\ldots\ldots\ldots(4)$$

Les courbes de degré n =3 sont des cubiques, elles sont classées en cubiques irréductibles d'équation

$f(x, y) = r_1 x^3 + r_2 x^2 y + r_3 x y^2 + r_4 y^3 + r_5 x^2 + r_6 x y + r_7 y^2 + r_8 x + r_9 y + r_{10} = 0; \ldots(5)$

Et en cubiques dégénérées sous les 2 formes.

a- f(x, y) = $r_1 x^2 + r_2 x y + r_3 y^2 + r_4 x + r_5 y + r_6$) ($r_7 x + r_8 y + r_9$)=0; ……(6)

Produit d'une conique par une droite.

b- f(x, y)= (r1 x + r_2 y + r_3) ($r_4 x + r_5 y + r_6$) ($r_7 x + r_8 y + r_9$)=0 ; …… (7)

Produit de trois droites.

Les courbes algébriques planes sont des quartiques pour n = 4, des quantiques pour n=5, des sextiques pour n = 6.

Nous intéressons aux cubiques irréductibles.

Elles sont classifiées par l'invariant genre arithmétique.

DEFINITION 13:

Le genre arithmétique d'une cubique irréductible E est l'entier g(E) non négatif égal à :

$$g(E) = \frac{1}{2}(n-1)(n-2)-s;\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(8)$$

Avec n degré de la cubique = 3.

Et s = nombre de points singuliers de la cubique E.

Dans la théorie des points d'une courbe plane, il y a des points simples, des points doubles, des points multiples d'ordre 3.

Un point simple P satisfait: $f(P) = 0$ et $f'(P) = 0$.

Un point singulier S satisfait: $f(S) = f'(S) = 0$.

Donc une cubique admet 0 ou un point singulier.

Il en résulte la classification des cubiques irréductibles en 2 classes:

La classe des cubiques irréductibles non singulières E; leur genre est égal à g(E) = 1.

La classe des cubiques singulières E; leur genre est égal à g(E) =0.

Cette classification implique une structure des courbes elliptiques.

DEFINITION 14:

Une courbe elliptique est une cubique E irréductible non singulière, d'équation de Weierstrass

$$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ \hat{I}\, K[x, y] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (9)$$

K est un corps commutatif global, local ou fini.

Les 5 coefficients a_1, a_2, a_3, a_4 et a_6 sont des éléments du corps K.

Les 2 variables x et y sont des racines de l'équation algébrique de Weierstrass, donc des éléments d'une clôture algébrique K_{alg} du corps K.

Les corps globaux sont des corps primitif ∞ des nombres rationnels et ses extensions algébriques. Ils sont de caractéristique 0.

Les corps locaux sont des corps infinis de caractéristique p>0.

Les corps finis sont des corps caractéristique p>0; il y a les corps finis F_p, p premier, et les corps finis F_q à $q = p^n$ éléments.

Cela implique l'influence du corps de base K sur les propriétés de la courbe elliptique E/K.

Signalons que l'équation de Weierstrass affine peut être transformée en équation projective dans le plan projectif P^2 (K).

EXEMPLE :

Equation de Weierstrass d'une cubique dans l'anneau F_3.

$$E: y^2 + 2 x y + y = x^3 + x + 2 \ \hat{I}\ F_3[x, y].$$

CHAPITRE II. ARITHMETIQUE DES COURBES ELLIPTIQUES.

Dans ce chapitre nous étudions des transformations d'équations de Weierstrass, des relations entre discriminants de cubique et de polynômes et une première classification des cubiques de weierstrass.

1- EQUATION DE WEIERSTRASS.

Par définition, une équation de Weierstrass d'une cubique plane irréductible, dans le plan affine, est un polynôme *f(x, y).*

$$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ \hat{I} K[x, y] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ (1)$$

Les monômes en *xy* et en *y* sont éliminés par le changement de variables:

$$x = X, \ y = \frac{1}{2} \ (Y - a_1 X - a_3), \text{ pour carac}(K) \neq 2; \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Avec le calcul nous obtenons l'équation de Weierstrass:

$$E_1: Y^2 = 4X^3 + b_2 X^2 + 2b_4 X + b_6 \ \hat{I} K[X, Y] \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2\text{-}1)$$

Les 3 coefficients b_{2i} sont des polynômes " homogènes de degré 2*i* "

Dans l'anneau ♦ $[a_1, a_2, a_3, a_4, a_6]$:

$$b_2 = a_1^2 + 4a_2 \ ; \ b_4 = a_1 a_3 + 2a_4 \ ; \ b_6 = a_3^2 + 4 a_6 \ ; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2\text{-}2)$$

Nous éliminons le monôme en x^2 et le coefficient 4 dans (2-1) avec le changement de variables;

$$X = (x - 3b_2)/36 \ ; \quad Y = y/108, \ \text{pour carac}(K) \neq 2,3 \ \ldots\ldots\ldots\ldots\ldots\ldots (3)$$

Nous obtenons l'équation de Weierstrass:

$$E_2: y^2 = x^3 - 27 c_4 x - 54 \ c_6 \ \hat{I} K [x, y] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3\text{-}1)$$

Les 2 invariants c_{2i} sont des polynômes " homogènes de degré *2i* "

Dans l'anneau ♦ $[b_2, b_4, b_6]$:

$$c_4 = b_2^2 - 24 b_4 \ ; \ c_6 = 36 b_2 b_4 - b_2^3 - 216 b_6 \ ; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3\text{-}2)$$

Dans la littérature mathématique, il existe d'autres modèles d'équations de Weierstrass de courbes elliptiques.

Le modèle de Legendre :

$C_1 : y^2 = x(x-1)(x-t)$ Î $K[x, y]$; *avec* t ¹ 0 *et* 1;……..(4)

Le modèle de Deuring

$C_2 : y^2+t\,xy+y = x^3$ Î $K[x, y]$, *avec* t^3 ¹ 3;……. (4-1)

Le modèle de tate:

$C_3 : y^2+xy=x^3 + ax+b$ Î $C[x, y]$;……(4-2)

Où les coefficients a et b sont des séries formelles en q = exp(2iπz)

$$a = -5 \sum_{n\geq 1} n^3 q^n \left(1-q^n\right)^{-1} \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4\text{-}3)$$

$$b = -\frac{1}{12} \sum_{n\geq 1} q^n \left(7n^5+5n^3\right)\left(1-q^n\right)^{-1} \ldots\ldots\ldots\ldots\ldots\ldots (4\text{-}4)$$

Les résultats sont pris dans [17-1]

Dans [18], nous avons relevé l'exemple de la courbe de Fermat :

$u^3 + v^3 = w^3$ Î $K[u, v]$, *carac* (K) ¹ $2,3$……. (5)

(5) est transformé par le changement de variables.

$$x=\frac{3w}{u+v}\ ,\ y=\frac{9}{2}\left(\frac{u-v}{u+v}\right)+\frac{1}{2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (5\text{-}1)$$

En l'équation de Weierstrass:

$C_4 : y^2 - y = x^3 - 7.$

Les coefficients b_{2i} et c_{2i} permet de définir des invariants des cubiques irréductibles.

2- INVARIANTS DES CUBIQUES IRREDUCTIBLES

Une courbe elliptique possède plusieurs invariants: un discriminants, un invariant modulaire, un invariant différentiel, un conducteur, un régulateur, une série de Dirichlet-Hasse.

DEFINITION 1:

Le discriminant d'une courbe elliptique E est un polynôme " homogène de degré 12 " de l'anneau ¨ [b_2, b_4, b_6, b_8]:

$\Delta(E) = 9b_2\,b_4\,b_6 - 8\,b_4^3 - 27\,b_6^2 - b_2^2 b_8$, *pour carac*$(K)$ ¹ 2,

Où l'on a posé $4b_8=b_2b_4 - b_4^2$;

EXEMPLES:

1) cubique d'équation de Weierstrass

$E_1 : y^2 = x^3 - 27\, c_4 x - 54\, c_6 \ \hat{I} K[x, y]$, *pour carac(K)* ¹ *2,3*

Alors $\Delta(E) = \dfrac{c_4^3 - c_6^2}{1728}$

2) équation de Legendre

$E_2 : y^2 = = x(x-1)\,(x - t) \ \hat{I} K[x, y]$; *avec* t ¹ *0 et 1;*

Alors $\Delta(E) = 16\, t^2\, (1-t)^2$.

3) cubique d'équation de Weierstrass :

$E_1 : y^2 = x^3 + ax - b \ \hat{I} K[x, y]$,

Alors $\Delta(E) = -\,16\,(4a^3 + 27b^2)$.

DEFINITION 2:

L'invariant modulaire du courbe elliptique E est

L'élément du corps K, carac(K) ¹ *2,3, égal à*

$$j(E) = \frac{c_4(E)^3}{\Delta(E)}$$

Dans les 3 exemples précédents, l'invariant modulaire est égal à

1- $j(E_1) = 1728\, c_4^3 / (c_4^3 - c_6^2)$;

2- $j(E_2) = 2^8 (t^2 - t + 1)^3 / (t^2 - t)^2$;

3- $j(E_3) = 1728 (4a)^3 / \Delta(E) = -\,1728 \times 4a^3 / (4a^3 + 27b^2)$.

DEFINITION 3:

L'invariant différentiel d'une courbe elliptique E d'équation de Weierstrass

E: $y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ \hat{I} K[x, y]$

Est l'élément différentiel:

$$w(E) = \frac{dx}{2y + a_1 x + a_3} = \frac{-\,dy}{3x^2 + 2a_2 + a_4 - a_1 y}$$

EXEMPLE:

Pour l'équation de Weierstrass E: $y^2 = x^3 + ax + b$, l'invariant différentiel est égal à:

$$w(E) = \frac{dx}{2y} = \frac{-\,dy}{3x^2 - a_1}$$

DEFINITION 4:

Le conducteur d'une courbe elliptique E de discriminant $\Delta(E)$

Est le produit:

$$N(E)=\prod p^{f_v}$$ *v= valuations inéquivalentes de corps K;*

p=diviseur premier de Δ(E).

f_v *= 0 lorsque E a une bonne réduction en v ;*

f_v *=1 lorsque E a une réduction multiplicative en v ;*

f_v *= 2+t lorsque E une réduction additive en v;*

t=0 pour p≥5; 0≤ t ≤3 pour p=3 et 0≤ t ≤6 pour p=2.

La théorie des réductions d'une courbe elliptique sera exposée dans la suite.

PROPOSITION 1

Le conducteur N(E) ne contient que certains facteurs de Δ(E).

Preuve.

Elle découle de la définition

Une conjecture de Weil prédit qu'il n'y a pas de courbe elliptique E/∞ de conducteur N(E/∞) < 11.

3- DISCRIMINANTS

Le discriminant constitue un invariant des polynômes $f(x)\in K[x]$, des courbes elliptiques, des corps de nombres algébriques.

Soit un polynôme *f(x)* de degré n factorise sous la forme

$$f(x) = d_0 (x-l_1) (x-l_2)\ldots(x-l_n)$$

$$= d_0x^n + d_1x^{n-1}+\ldots+d_n. \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

DEFINITION 5:

Le discriminant du polynôme (1) est égal à.

$$Dis\ (f) = d_0^{2n-2} \prod_{i\le j}\left(l_i - l_j\right)^2$$

EXEMPLES

1) $f(x) = ax^3 + bx^2 + cx + d;$

   Alors son discriminant est égal à:

   $dis(f) = 18abcd + b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2;$

2) $f(x)=ax^2+bx+c$

Alors son discriminant est égal à:

$dis\ (f) = b^2 - 4ac$

3) $f(x) = x^3 + Ax + B$

Alors son discriminant est égal à:

$dis\ (f) = -16(4\ A^3 + 27\ B^2)$

Ces exemples permettent de comparer les discriminants $\Delta(E)$ d'une courbe elliptique d'équation de Weierstrass:

$$E: y^2 = f(x)\ \hat{I}\ K[x];$$

Et *dis(f)* du polynôme *f(x)*.

PROPOSITION 2:

Soit une courbe elliptique E d'équation de Weierstrass:

$$E: y^2 = f(x)\ \hat{I}\ K[x, y],$$

1) *lorsque* $f(x) = 4x^3 + b_2 x^2 + 2b_4 x + b_6\ \hat{I}\ K[x, y]$, *alors les discriminants* $\Delta(E)$ *de E et dis(f) de f(x) satisfont la relation:*

$$dis\ (f) = 16\Delta(E);$$

2) *lorsque* $f(x) = x^3 + ax + b$, *alors*

$$\Delta(E) = 16\ dis(f)$$

Preuve :

Les discriminants $\Delta(E)$ et dis(f) sont calculés avec des formules établies précédemment.

La comparaison des résultats implique la proposition.

Il en résulte que le quotient $\Delta(E)$/dis(f) = c est une constante qui dépend de $f(x)$

La définition 5 du discriminant dis(f) implique la:

PROPOSITION 3:

Soit un polynôme $f(x)\ \hat{I}\ K[x]$ *de degré n. alors son discriminant dis(f) est nul si et seulement si f(x) admet 2 racines égales* $l_i = l_j$, $i \neq j$.

4- RESULTANT Res(f,g) DE 2 POLYNOMES.

Les résultats seront énoncés sans démonstration. Il se trouvent dans plusieurs ouvrages d'algèbre dont " Algébra "de Lang et " Introduction à l'Algèbre " de Kostrikine.

DEFINITION 5:

Soit 2 polynômes f(x) et g(x)

$f(x) = d_0x^n+d_1x^{n-1}+\ldots+d_n$ *, de degré n >0, et*

$g(x) = r_0x^t+r_1x^{t-1}+\ldots+r_t$ *, de degré t> 0*

Alors le résultant de ces 2 polynômes est le déterminant d'ordre n+t

$$Res\ (f,g) = \begin{vmatrix} d_0 & d_1 & \cdot & d_n & \cdot & \cdot & \cdot & \cdot \\ \cdot & d_0 & d_1 & \cdot & d_n & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & d_0 & d_1 & \cdot & \cdot & d_n \\ r_0 & r_1 & \cdot & r_t & \cdot & \cdot & \cdot & \cdot \\ \cdot & r_0 & r_1 & \cdot & r_t & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & r_0 & r_1 & \cdot & \cdot & r_t \end{vmatrix}$$

t lignes

n lignes

Dans ce déterminant, la diagonale principale est formée de t coefficients d_0 et n coefficients r_t.

Les termes manquants sont complétés par des zéros.

La théorie des déterminants de l'algèbre multilinéaire implique que ce déterminant est une fonction de ses vecteurs lignes

$$Res\ (f, g) = det\ (L_1,\ldots,L_t,L'_1, \ldots,L'_n)$$

PROPOSITION 4:

Soit les polynômes f(x) et g(x) ci-dessus et leur résultant Res(f, g)

Alors:

1) *Res(f, g) contient le produit* $d_0^t r_t^n$.
2) *Res(af, g) =* a^t *Res(f, g) et Res(f, bg) =* b^n *Res(f, g); a,b* $\hat{I}$ *K*

Le résultant res(f, g) est fonction symétrique de leurs racines.

PROPOSITION 5:

Soit 2 polynômes f(x) et g(x) dans un anneau K[x]

$f(x) = d_0 \prod_{1 \le i \le n} (x - l_i)$ *de degré n> 0 et*

$g(x) = r_0 \prod_{1 \le i \le n} (x - b_i)$ *de degré t> 0*

Alors leurs résultant est égal à :

1) $Res(f, g) = d_0^t r_0^n \prod_{1 \le i \le n} \prod_{1 \le j \le t} (l_i - b_j)$

2) $Res(f, g) = d_0^t \prod_{1 \le i \le n} g(l_i) = (-1)^{nt} r_0^n \prod_{1 \le j \le t} f(b_i) = d_0^t r_0^n \prod_{i, j} (l_i - b_j)$

COROLLAIRE

Le résultant Res(f, g) de 2 polynômes est nul si et seulement si les 2 polynômes ont une racine commune

Examinons le cas particulier d'un polynôme *f(x)* et son dérivé.

PROPOSITION 6:

Soit un polynôme $f(x) = d_0 \prod_{1 \le i \le n} (x - l_i)$ *de degré n> 0*

Alors le résultant de f(x) et de son dérivée f'(x) est égal à

$$Res(f, f') = d_0^{n-1} \prod_{1 \le i \le n} f'(l_i)$$

Ce résultant est lie au discriminant dis(f) par les formules:

$dis(f) = d_0^{2n-2} \prod_{i \ne j} (l_i - l_j)^2$ *et* $Res(f, f') = d_0 dis(f)$

EXEMPLE:

Courbe elliptique E d'équation de Weierstrass:

E: $y^2 = (x+3)(x-1)(x+4) = f(x) \in \mathbb{R}[x]$

Le polynôme *f(x)* admet 3 racines réelles λ_1=-3, λ_2=1, λ_3= -4;

Sa dérivée est égale à:

$f'(x) = 3x^2 + 12x + 5.$

Alors le résultant des polynômes *f(x)* et *f'(x)* et égal à:

Res $(f, f') = d_0^{n-1} \prod_{1 \le i \le n} f'(l_i) = 20(-4)(5) = -400$

La formule *Res (f, f') =d_0 dis(f)* et les résultats ci-dessus

Impliquent la valeur

dis(f) = Res (f, f') = - 400;

5- CUBIQUES IRREDUCTIBLES SINGULIERES

Considérons une cubique irréductible E d'équation de Weierstrass

$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \; \hat{I} K[x, y]$……. (1)

Le point à l'infini de la cubique est le point $O_E = (¥, ¥)$ ……..(2)

Dans le plan projectif P^2 (R), ce point a pour coordonnées.

$O_E = (0, 1, 0) = (x, y, z)$;……..(2-1)

C'est un représentant de la classe: $cl\{(0, 1, 0) = \{(0, t, 0), t \in R^*\}$ …….(2-2)

Donc le point à l'infini est déterminé par la <u>*direction de l'axe Oy*</u>.

PROPOSITION 6

Soit une cubique plane irréductible E d'équation (1) de discriminant $\Delta(E)$ et le point à l'infini O_E.

Alors :

1) *le point à l'infini est un point non singulier de E.*
2) *la cubique E est singulière si seulement si $\Delta(E)=0$.*

Preuve de " $O_E = (¥, ¥)$ est un point simple de la cubique"

Prenons, dans le plan projectif P^2(R) le point à l'infini $O_E = (0, 1, 0)$

et l'équation projective de E.

$F(X, Y, Z) = Y^2Z + a_1 XYZ + a_3 YZ^2 - X^3 + a_2X^2Z - a_4 XZ^2 - a_6Z^3 \in P^2(R)$;……..(1).

La valeur F (0, 1, 0) =0 implique que le produit à l'infini O_E est sur la courbe E. (2)

Considérons les 3 dérivées partielles de la fonction F (X, Y, Z);

Alors F_Z' (0, 1, 0) = 1 ≠ 0 ;……..(3)

Il en résulte que le point O_E n'est pas singulier sur la cubique E……(4)

Preuve de " cubique E singulier" implique "Δ (E) = 0"

Soit une cubique E d'équation de Weierstrass :

$E: y^2 = f(x)$ ……...(1)

L'hypothèse "E singulier" implique que le polynôme $f(x)$ admet une racine double

$\lambda_1 = \lambda_2$;……..…(2)

Par définition du discriminant de f, (2) implique

dis (f) = 0;…….(3)

La relation entre discriminant Δ (E) de E et dis(f) de f et (3) implique la valeur :

"Δ (E)=0;……...(4)

Nous ne ferons pas la preuve de la réciproque "Δ (E)=0" implique la cubique E est singulière"

La nature du point singulier est déterminée par l'invariant $c_4(E) = b_2^2 - 24\, b_4$

Il y a 2 types de points singuliers sur une cubique un nœud, point de E où la cubique admet 2 tangentes distinctes,

Un point de rebroussement, point de E où la cubique admet 2 tangentes confondues.

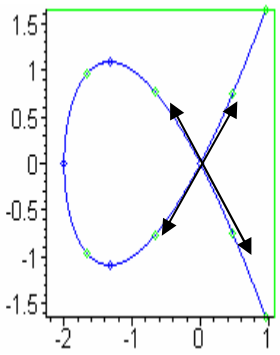


Figure d'une cubique avec un nœud S

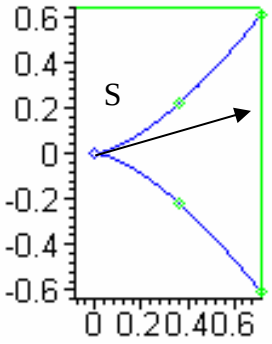


Figure d'une cubique avec un point de rebroussement S

PROPOSITION 7:

Soit une cubique E, irréductible et singulière et son invariant c_4

1) *la cubique admet un nœud si et seulement si $\Delta(E) = 0$ et $c_4 \neq 0$.*

2) *La cubique admet un point de rebroussement si et seulement si $c_4 = 0$ et $\Delta(E) = 0$*

Preuve de " la cubique E admet un nœud " implique " $\Delta(E) = 0$et $c_4 \neq 0$"

L'hypothèse "E admet u nœud " implique que la cubique est singulière par la proposition 6, $\Delta(E) = 0$ ……. (1)

Prenons une cubique E d'équation de Weierstrass.

$E: y^2 = x^3 - 27\,c_4 x - 54\,c_6$,…… (2)

L'hypothèse "E admet un nœud " implique que la cubique E admet 2 tangentes distinctes en ce nœud …… (3)

Les pentes de ces tangentes sont égales à la dérivée y', calculée avec (2)

$$y' = \frac{3x^2 - 27\,c_4}{2y} = \frac{3}{2y} N(x) \text{ …….. (4)}$$

Le polynôme $N(x) = x^2 - 9c_4$ a pour discriminant

$dis\,(N(x)) = 36\,c_4$;……(5)

L'hypothèse de 2 tangentes implique.

$dis\,(N(x)) = 36c_4 \neq 0$, soit $c_4 \neq 0$;…….(6)

Preuve de " la cubique admet un point de rebroussement " implique "$c_4 = 0$"

Par hypothèse, la cubique E est singulière; donc son discriminant est nul

$\Delta(E) = 0$…… (1)

Gardons l'équation de Weierstrass:

$E: y^2 = x^3 - 27\,c_4 x - 54\,c_6$…..…(2)

Et la dérivée

$$y' = \frac{3}{2y} N(x)\text{ , } N(x) = x^2 - 9c_4 \text{ ; ……..(3)}$$

La cubique E admet 2 tangentes confondues au point de rebroussement;…(4)

Cela implique un discriminant nul:

$dis\,(N(x)) = 36c_4 = 0$, soit $c_4 = 0$;…….(5)

Nous ne ferons pas les preuves des réciproques.

6- COURBES ELLIPTIQUES

Le discriminant d'une courbe elliptique E n'est pas nul,

D'après la proposition 6.

Il y a 2 cas possibles : Δ (E)>0 ou Δ (E)< 0.

PROPOSITION 8:

Soit une courbe elliptique de discriminant $(x-e_1)\ (x-e_2)\ (x-e_3)$

1) *elle coupe l'axe Ox en 3 points simple si et seulement si Δ (E)>0;*
2) *elle coupe l'axe Ox en 1 seul point, simple, si et seulement si Δ (E)< 0.*

Preuve de " E coupe *Ox* en 3 points simple." Implique "Δ (E)> 0."

Prenons une équation de Weierstrass:

$E: y^2 = f(x) \in \mathrm{R}[x, y]$…… (1)

Considérons les 3 points d'intersection de E par l'axe Ox.

$P_i = (e_i, 0)$ *avec* $e_i \neq e_j$;……(2)

Il en résulte la forme du polynôme

$f(x) = (x-e_1)\ (x-e_2)\ (x-e_3)\ \hat{I}$ R[*x*, *y*]…..(3)

Par définition, le discriminant de *f* est égal à:

$dis\ (f) = (e_1-e_2)^2\ (e_2-e_3)^2\ (e_1-e_3)^2$…..*(4)*

Dans le corps R des nombres réels, les 3 facteurs dans (4) sont réels, leurs carrés sont positifs.

$dis(f) > 0$…….(5)

La relation entre discriminant Δ(E) de E et *dis (f)* de *f*

Implique le signe : $\Delta(E) > 0$……..(6)

Preuve de " E coupe *Ox* en 1 seul point simple" implique " Δ(E)< 0"

Soit une courbe elliptique E d'équation de Weierstrass:

$E: y^2 = f(x) \in \mathrm{R}[x, y]$;……..(1).

Les courbes elliptiques sont des cubiques non singulières…… (2)

Donc le polynôme f(x) admet 3 racines simples.

$f(x) = (x-e_1)\ (x-e_2)\ (x-e_3)\ \hat{I}$ R[*x*, *y*]…..(3)

L'hypothèse d'un seul point d'intersection implique une racine réelle e_i .et les 2 autres complexes conjuguées:

$e_i \in \mathrm{R}$, $e_2 = s + it\ \hat{I}\ C$ *et* $e_3 = s - it\ \hat{I}\ C$…..…..…...(4)

Calculons *dis(f(x))* avec la déinition

$dis\ (f) = (e_1-e_2)^2\ (e_2-e_3)^2\ (e_1-e_3)^2$…..*(5)*

Nous obtenons la valeur.

$dis\ (f) = -\ 4\ t^2\ ((e_1 - s)^2 + t^2))^2 < 0$;…….(6)

La relation entre les discriminant Δ (E) et *dis(f)* implique le signe.

Δ (E)< 0 ……. (7).

Nous ne ferons pas les preuves des réciproques.

7- CLASSIFICATION DES CUBIQUES IRREDUCTIBLES E AVEC Δ (E) ET c_4(E).

Les 3 propositions 6, 7, 8 ont fait apparaître 4 types de cubiques irréductibles. Rassemblons ces résultats dans la:

PROPOSITION 9:

Les cubiques irréductibles E sont classifiées par Δ (E) et c_4(E) en 4 classes:

1. *classe cl*I *des cubiques ayant un nœud, alors Δ (E)=0 et $c_4(E) \neq 0$.*
2. *classe cl*II *des cubiques ayant un point de rebroussement, alors Δ (E)=0 et $c_4(E)=0$.*
3. *classe cl*III *des courbes elliptiques coupant l'axe Ox en 3 points simples, alors Δ (E)> 0.*
4. *classe cl*IV *des courbes elliptiques coupant l'axe Ox en 1 seul point, simple, alors Δ (E)< 0.*

Indiquons un exemple de cubique de chaque classe.

EXEMPLE 1: *cubique E_1 qui admet un nœud.*

Soit la cubique E_1 d'équation de Weierstrass

$$\boldsymbol{E_1: y^2 = x^3 - 2x^2 + x} \in \mathrm{R}[x, y]$$

$b_2 = a_1^2+4a_2 = 0+4.(2)=-8$
$b_4 = a_1a_3+2a_4 =2$
$b_6 =a_3^2 +4a_6 = 0$ $\qquad\qquad$ $c_4= b_2^2-24b_4=64-48=16$
$b_8=b_2b_6-b_4^2/4= 0$

$\Delta(E) = 9\, b_2b_4b_6 - 27b_6^2 - 8b_4^3-b_2^2b_8. = 0$ et $c_4 = 16\neq 0$,

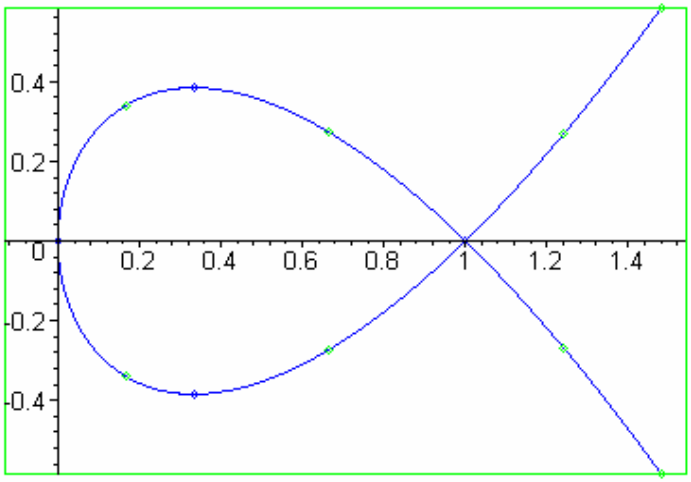
Cela implique que La cubique E_1admet un nœud.

Pour tracer la courbe, calculons les coordonnées de quelques points

x	- 1	0	1	2	3	1/2	3/4	1/4
y^2	-4 *pas de y réelles*	0	0	2	12	1/8	3/64	9/64

Ce tableau indique que la courbe n'a pas de points dans le demi-plan $x< 0$.

Le point *(1, 0)* est le nœud de la cubique.



EXEMPLE 2: *cubique E_2 qui admet un point de rebroussement*

Soit la cubique E_2 d'équation de Weierstrass:

$E_2 : y^2+2xy-2y = x^3 - x^2 +2x - 1 \in R[x, y]$

Calcul des invariants

$b_2 = a_1^2+4a_2 = 4-4=0$

$b_4 = a_1a_3+2a_4 =-4+4=0$

$b_6 = a_3^2 +4a_6 = 4-4=0$ $\qquad\qquad$ $c_4= b_2^2-24b_4=0$

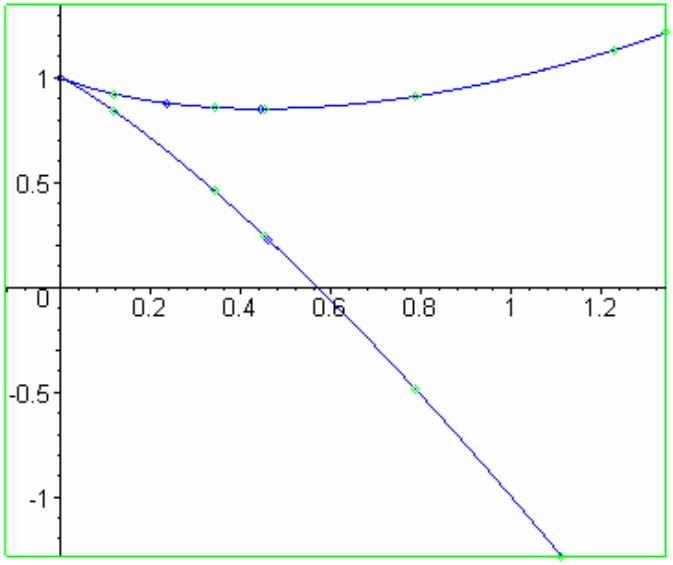
$b_8 = (b_2b_6-b_4^2)/4= 0$

$D(E) = 9\, b_2b_4b_6 - 27b_6^2 - 8b_4^3-b_2^2b_8.= 0$ et $c_4 = 0$ Cela implique que la cubique E_2 a un point de rebroussement.

Pour tracer la cubique E_2, calculons les coordonnées de quelques points.

x	*0*	-1	1	*0.4*	*3/4*
y	$y_1=y_2=1$	*Pas de y réel*	± 1	$0{,}6 \pm \sqrt{0.296}$	$\frac{1}{4} \pm \sqrt{\frac{23}{4}}$

Le tableau indique que la cubique admet un point de rebroussement au point (0, 1).



EXEMPLE 3: *courbe elliptique qui coupe l'axe Ox en un point.*

Soit la cubique E_3 d'équation de Weierstrass:

$$\mathbf{E_3 : y^2 = x^3 + 4x^2 - 2x + 1}$$

Calcul des invariants

$\Delta(E_3) = -9904$

$\Delta(E) < 0$ implique que cette courbe elliptique coupe *Ox* en un seul point.

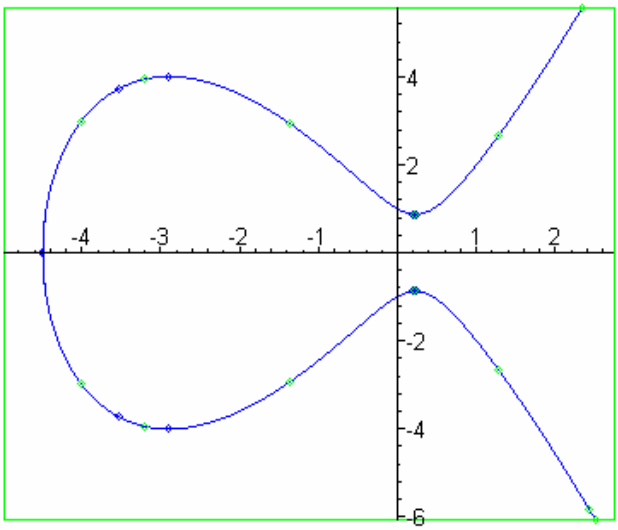
Tableau de coordonnées de quelques points de E_3

x	-4	-2	-1	0	1	2
y^2	9	13	6	1	4	21

D'après ce tableau la courbe E_3 coupe l'axe *Oy* en 2 points $(0, \pm 1)$.

Pour trouver le point d'intersection avec *Ox*, il faut résoudre l'équation:

$x^3+4x^2-2x+1=0$, avec le logiciel Maple j'ai obtenu la racine $x=1$.



EXEMPLE 4: *courbe elliptique de la classe cl* III

Soit la courbe elliptique E_4 d'équation de Weierstrass:

$$E_4: y2= x^3+3x^2 -6x-8=0 \ \hat{I}\ R[x, y].$$

Calcul du discriminant: $\Delta(E_4) > 0$.

Cela implique que la courbe E_4 coupe l'axe *Ox* en 3 points simples.

Leurs abscisses sont racines de l'équation $f(x)=x^3+3x^2 -6x-8=0$ …(1)

Pour trouver les racines entières il faut appliquer le

Théorème : *soit l'équation diophantienne* $f(x) = x^n + d_1x^{n-1}+\ldots+d_n \ \hat{I}\ ¨[x]$

Toute racine de cette équation sont des diviseurs du terme constant.

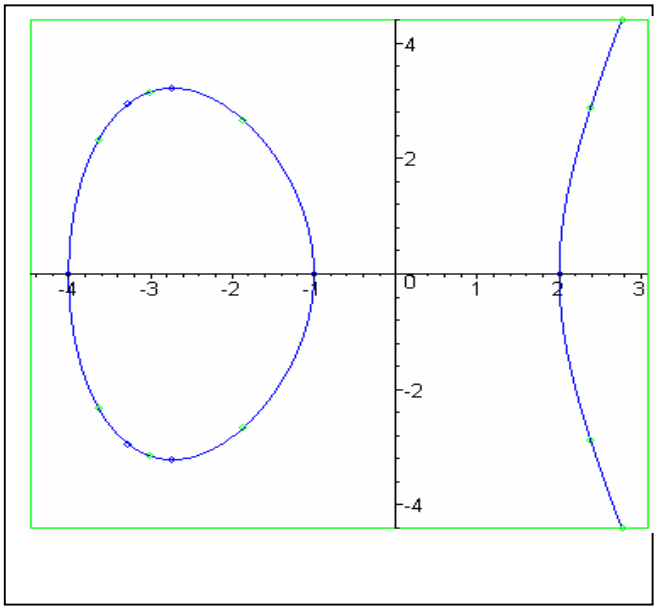
Dans l'équation diophantienne (1), le terme constant est égal à -8.

Les diviseurs de -8 sont $d = \pm1, \pm2, \pm4$ et ±8.

Le calcul des valeurs *f(d)* implique les résultats.

$f(-1) = f(2) = f(-4) = 0$. Il en résulte les 3 points d'intersection de E_4 et l'axe *Ox*.

$P_1= (-4, 0)$, $P_2 = (-1, 0)$, $P_3 = (2, 0)$



CHAPITRE III: GROUPE DE MORDELL-WEIL D'UNE COURBE ELLIPTIQUE

D'après Lang, dans [12-2], Poincaré a conjecturé que le groupe de points rationnels d'une courbe elliptique est de type fini.

En 1922, Mordell a prouvé cette conjecture dans « Diophantine Equations » Academic Press.

En 1930, dans la publication « sur un théorème de Mordell- bull. Sci. Math 54 (1930) ,182-191 », Weil a étendu ce résultat aux variétés abéliennes.

Nous commençons par la construction d'un groupe abélien sur l'ensemble E (K) des points K-rationnels d'une courbe elliptique E/K.

1- STRUCTURE DE GROUPE ABELIEN SUR L'ENSEMBLE E (K)

Soit une courbe elliptique et l'ensemble E (K).

$$E(K) = \{P = (x, y), E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ \hat{I} K[x, y]\}\ldots (1)$$

PROPOSITION1:

L'homomorphisme $u: E(K)\acute{}E(K) \to E(K)$

$$(P, R) \to P+R$$

Est une loi de groupe abélien d'élément neutre le point à l'infini O_E*, avec la règle géométrique de 3 points colinéaires de la courbe elliptique.*

$$P_1+P_2+P_3=O_E, \qquad P_i = (x_i, y_i)$$

Vérifions les axiomes d'un groupe abélien.

Axiome de l'élément neutre :

Pour tout point $P \hat{I} E(K)$, $P+O_E$ est sur E et sur la parallèle à Oy passant par le point P. le point O_E est déterminé par la direction de l'axe Oy.

Donc $P + O_E = O_E + P = P$

Axiome de symétrique d'un point $P \hat{I} E(K)$

Soit un point $P \hat{I} E(K)$, la parallèle à l'axe Oy passant par P recoupe la courbe E en un point P'

La règle des 3 points colinéaires de E implique la relation

$$P+P'+O_E=O_E \text{ ……. (2)}$$

D'après la proposition 6- chap 2, le point à l'infini est sur la courbe E.

(2) implique le symétrique de P.

$$P'= -P \quad \text{…… (3)}$$

Axiome de commutativité.

La sécante P_1P_2 coïncide avec la sécante P_2P_1……..… (4)

Cela implique $(P_1+P_2) +P_3 = (P_2+P_1) +P_3$…….. (5)

Axiome d'associativité:

Soit 3 points non colinéaires P, R et S sur E (K)

Je n'ai pas trouvé de propriété géométrique des sécantes d'une courbe pour prouver l'égalité d'associativité.

C'est par le calcul des coordonnées des points

(P+R)=M, M+S=M', R+S=T, P+(R+S) =T'

Que l'on arrive à obtenir l'égalité d'associativité.

$$(P+R)+S = P+(R+S)$$

L'image de l'élément neutre (O_E, O_E) est égale à

$$u(O_E, O_E)= O_E+O_E=O_E$$

L'image de la somme $(P_1, R_1) + (P_2, R_2)$ est égale à

$$u\,((P_1, R_1) + (P_2, R_2)) = (P_1 + P_2\,, R_1+ R_2)$$
$$= (P_1, R_1) + (P_2, R_2)$$
$$= u\,(P_1, R_1) + u\,(P_2, R_2)$$

2- COORDONNEES DU SYMETRIQUE –P D'UN POINT P ET DE LA SOMME P_1+P_2

Soit une courbe elliptique E d'équation de Weierstrass

$E: y^2 + a_1\,x\,y + a_3\,y = x^3 + a_2x^2 + a_4\,x + a_6\ \hat{I}\,K[x, y]$…..… (1)

Soit un point $P\,(x_p, y_p)$ sur la courbe E ……..(2)

Par la proposition 1, le symétrique –P de P est à l'intersection de la courbe E par la parallèle à l'axe *Oy* passant par P.

Avec les calculs nous obtenons les coordonnées du symétrique –P

$$-P = (x_{-p}, y_{-p})= (x_p, -y_p-a_1x_p - a_3) \text{……} \quad (3)$$

Soient 2 points $P_i = (x_i\,,\ y_i)$ sur E, $P_1 \neq \pm P_2$.....(4)

La sécante P_1P_2 recoupe E au point P_3……(5)

La relation $P_1+P_2+P_3=O_E$ implique

$$P_1+P_2= -P_3 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

Avec l'équation de la sécante P_1P_2 et les formules du symétrique –P

Nous obtenons les coordonnées de la somme P_1+P_2

$P_1+P_2= M= (x_M, y_M),$ $\quad t = \dfrac{y_1 - y_2}{x_1 - x_2}$

$$x_M = t^2 + a_1 t - a_2 - x_1 - x_2$$

$$y_M = -t^3 - 2a_1t^2 + (a_2 - a_1^2 + 2x_1 + x_2)t + a_1a_2 - a_3 + a_1(x_1+x_2) - y_1 \ldots\ldots\ldots\ldots(7)$$

Rassemblons ces résultats dans la

PROPOSITION 2

Soit une courbe elliptique E d'équation de Weierstrass.

$$E: y^2 + a_1 x y + a_3 y = x^3 + a_2x^2 + a_4 x + a_6 \ \hat{I} K[x, y]$$

1) *Les coordonnées du symétrique –P d'un point P de E sont égales à :*

$$-P = (x_{-p}, y_{-p}) = (x_p, -y_p - a_1x_p - a_3)$$

2) *Les coordonnées de la somme P1+P2 de 2 points sont égales à :*

$$P_i = (x_i, y_i),\ P_1 \neq \pm P_2,\ P_1+P_2= M= (x_M, y_M) \quad t = \frac{y_1 - y_2}{x_1 - x_2}$$

$$x_M = t^2 + a_1 t - a_2 - x_1 - x_2$$

$$y_M = -t^3 - 2a_1t^2 + (a_2 - a_1^2 + 2x_1 + x_2)t + a_1a_2 - a_3 + a_1(x_1+x_2) - y_1$$

3- POINTS DE E D'ORDRE FINI.

Dans un groupe abélien E (K) il y a des points d'ordre fini, éventuellement des points d'ordre infini, des sous groupes cycliques, des sous groupes abéliens.

DEFINITION 1

Un point P du groupe E(K) est d'ordre fini m lorsqu'il satisfait la relation mP = O_E.

Pour tout entier m fini, les points P d'ordre m forment un sous groupe *E(K)[m]*.

DEFINITION 2

Le sous groupe de m-torsion du groupe E (K) est l'ensemble E (K)[m] des points d'ordre m.

La réunion des sous groupes de m- torsion est le groupe de torsion T(E (K)) du groupe E (K)

DEFINITION 3

Le groupe de torsion d'une courbe elliptique E est l'ensemble

$T(E(K)) = T(E) = \{P \hat{I} E(K);\ mP = O_E,\ m \hat{I} \ ¨\}$

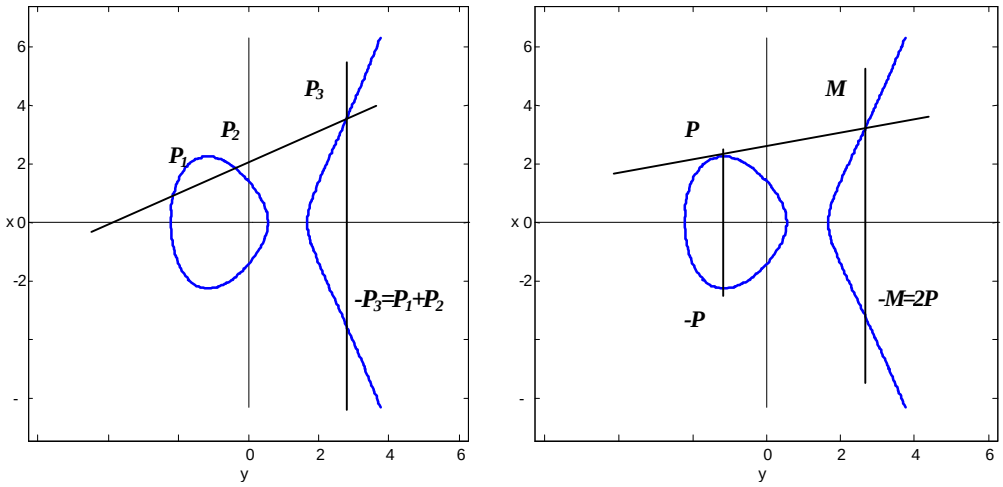
C'est aussi la réunion des sous groupe de m-torsion

$$T(E) = \bigcup_{m \in Z} E(K)[m]$$

Etablissons les coordonnées du point 2P.

La tangente à la courbe elliptique E en un point P coupe la courbe en un point M, le symétrique –M de ce point M est le point –M =2P.

Cette construction géométrique permet de calculer les coordonnées du point 2P.



PROPOSITION 3

Soit une courbe elliptique E /K d'équation de Weierstrass.

$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ \hat{I} K[x, y]$

Les coordonnées du point 2P pour tout point P de E sont égales à.

$P = (x_P , y_P)$; $2P = (x_{2P}, y_{2P})$; $y' = \dfrac{\left(3x^2 + 2a_2 x + a_4 - a_1 y\right)}{\left(2y + a_1 x + a_3\right)}$

$x_{2P} = y'^2_P + a_1 y'_P - 2x_P - a_2$

$y_{2P} = -y'^3_P - 2a_1 y'^2_P (a_2 - a_1^2 + 3x_P) y'_P + a_1 a_2 - a_3 + 2a_1 x_P - y_P$

Les 2 propositions impliquent que les points P_1+P_2 et $2P$ ont des coordonnées fractions rationnelle du corps K[x, y].

En particulier

$$x_{2p} = \frac{\Phi_2}{\Psi_2^2},\ y_{2p} = \frac{w_2}{\Psi_2^3}$$

Les polynômes numérateur et dénominateur ont des degrés croissants avec m.

Pour obtenu des formules maniables, il faut diminuer le nombre de coefficients a_i de l'équation de Weierstrass.

C'est Cassels dans [2] qui à trouvé des formules intéressantes pour les points mP sur les courbes elliptiques E d'équation de Weierstrass

$$E: y^2 = x^3 + Ax + B \ \hat{I}\ Q[x, y] \text{ avec } 4A^3+27B^2 \neq 0 \ \ldots\ldots. (1)$$

PROPOSITION 4

Soit une courbe elliptique d'équation (1). Alors les coordonnées du point 2P sont égales à :

$$2P = \left(\frac{\Phi_2}{\Psi_2^2},\ \frac{w_2}{\Psi_2^3} \right),\ \text{avec } Y_2 = 2y,\ F_2 = x^4 - 2Ax^2 - 8Bx + A^2;$$

Et $w_2 = x^6 - 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2.$

Preuve

Nous utilisons les formules de la proposition 3.

PROPOSITION 5

Soit une courbe elliptique E d'équation de Weierstrass:

$E: y^2 = x^3 + Ax + B \ \hat{I}\ \infty[x, y] \text{ avec } 4A^3+27B^2 \neq 0$

Alors pour tout entier $m \geq 2$, *les coordonnées du point mP du groupe E (Q) sont de la forme:*

$$mP = \left(\frac{\Phi_m}{\Psi_m^2},\ \frac{w_m}{\Psi_m^3} \right)$$

Y_m, F_m *et* w_m *sont des polynômes de l'anneau* $\ddot{}[x, y, A, B]$ *qui satisfont les relations.*

$Y_{-1} = -1\ ;\ Y_0 = 0,\ Y_1 = 1,\ Y_2 = 2y,\ Y_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

$Y_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2$

$Y_{2m} = 2Y_m(Y_{m+2}Y_{m-1} - Y^2_{m-2}Y^2_{m+1})$

$Y_{2m+1} = Y_{m+2}Y^3_m - Y_{m-1}Y^3_{m+1}$

Les polynômes F_m *et* w_m *satisfont*

$F_m = xY^2_m - Y_{m-1}Y_{m+1}$

$4y\ w_m = Y_{m+2}Y_{m-1} - Y_{m-2}Y^2_{m+1}$

Ainsi F_m est un polynôme en x, A, B de degré m^2

Preuve

Pour m=-1, -(x, y)=(x, -y); alors x= $\frac{x}{(-1)^2}$ et y= $\frac{y}{(-1)^3}$

Il en résulte $Y_{-1} = -1$.

Pour m=0, 0(x, y)=(∞, ∞) ; alors ∞= $\frac{x}{0^2}$ et ∞ = $\frac{y}{0^3}$

Il en résulte $Y_0 = 0$.

Pour m=1, 1(x, y)=(x, y) ; alors x= $\frac{x}{1^2}$ et y = $\frac{y}{1^3}$

Il en résulte $Y_1 = 1$.

Pour m = 2 les formules des coordonnées du point 2P

Impliquent $Y_2 = 2$.

Pour m>2, on utilise une récurrence sur l'entier m.

« Lorsque K=C, ce sont les formules familières qui découlent de la théorie de la fonction P

(z, L) de Weierstrass », d'après Fricke (Elliptisckey Funktionen –Leipzig (1922a)/ et weber

(Lehrbuch der algebra- braunschrverg (1908a)/

Avec le calcul nous avons obtenu le polynômeΦ_3 qui est unitaire de degré 9

Et le polynôme ω_3 qui est de degré 12.

Les points P du groupe E (K), d'ordre m ont des applications:

L'application de Kummer et la suite de Kummer d'une courbe elliptique.

DEFINITION 4

L'application du Kummer d'une courbe elliptique E est la fonction

$l_E : E(K) \times Gal(K_{gal}/K) \to E(K)[m]$

De valeur $l_E(P, s) = s(R) - R$ *, avec* $mR = P$

Cette application est bilinéaire.

PROPOSITION 6

Soit une courbe elliptique E, son groupe de mordell-weil E (K_{alg}) son sous groupe de m-torsion E (K) [m].

Alors la suite de groupes abéliens.

$$0 \to E(K)[m] \to E(K_{alg}) \xrightarrow{t_m} E(K_{alg}) \to 0$$

Où t_m est la multiplication par m et K_{alg} une clôture algébrique de K,

Est une suite de Gal (K_{gal}/K)- modules, exacte et courte

Gal (K_{gal}/K) désigne le groupe de Galois.

Avec les groupes H^1 de cohomologie, nous obtenons la suite de Kummer.

DEFINITION 5

La suite de Kummer d'une courbe elliptique E est la suite de groupes abéliens .

$$0 \to E(K)/m\,E(K) \to H^1(G, E(K)[m]) \to H^1(G, E(K_{alg})[m]) \to 0$$

Où G est le groupe de Galois de l'extension K_{alg} du corps K

4- FINITUDE DU GROUPE QUOTIENT E (K)/m E(K)

Ce groupe figure dans la suite de Kummer ci dessus

PROPOSITION 7

Le groupe quotient E (K)/m E (K) d'une courbe elliptique E est fini

Pour les entier $m \geq 2$.

Preuve.

Soit l'application bilinéaire de Kummer

$$l_E : E(K) \times Gal(K_{gal}/K) \to E(K)[m]$$

de valeur $l_E(P,s) = s(R) - R$, avec $mR = P$

Cette application possède un noyau à gauche égal au groupe m E (K), et un noyau à droite égal à un groupe de Galois d'une extension K_{alg}/L, avec L= K (m^{-1}E (K)), sont G_L ce groupe de Galois.

L'application λ_E induit une application bilinéaire.

$$l_E : E(K)/mE(K) \times G_L \to E(K)[m]$$

Cette application est bijective.

La finitude du groupe de m-torsion de E implique la finitude du groupe quotient E (K)/mE(K) pour m≥2.

5- HAUTEURS SUR UNE COURBE ELLIPTIQUE.

Pour monter que le groupe de Mordell-Weil E(K) d'une courbe elliptique E est fini, on utilise des fonction spéciales et l'algorithme de descente infinie.

DEFINITION 6:

Une hauteur sur un groupe abélien A est une fonction réelle

h: A® §

Qui satisfait les 3 axiomes :

***(haut1)** à tout point P_1 de A on peut associer une constante C_1 (A, P_1)=C_1*

Telle que h (P+P_1)£ 2h (P) +C_1,

Pour tout point P de A.

***(haut2)** il y a un entier m³2 et une constante C_2(A,m)=C_2 telle que*

h(mP) ³m^2h(P)-C_2,

Pour tout point P de A

***(haut3)** pour toute constante C_3, l'ensemble des points P de hauteur bornée est fini*

{P ÎA; h (P) £ C_3}

Le groupe abélien A peut être un espace projectif, le groupe E (K) de Mordell-Weil d'une courbe elliptique.

L'image h (P) peut prendre plusieurs valeurs; il en résulte qu'il y a plusieurs fonctions hauteurs.

PROPOSITION 8:

Soit un groupe abélien A et un entier m ³ 2 tel que le groupe quotient A/mA soit fini. Alors le groupe A est de type fini

Preuve

Considérons un système de représentants des classes A/Ma.

$T_1, T_2, T_3, \ldots, T_r$…….……(1)

Construisons une suite infinie de points P_i de A avec l'algorithme

De descente infinie.

$P=mP_1+T_1$; $P_{i,1}= mP_2+T_{i,2}$;…, $P_{n-1}= mP_n+T_{i,n}$ ……..…..(2)

Où les points $T_{i,j}$ sont pris parmi les représentants de l'ensemble (1).

Introduisons une hauteur h sur le groupe A :

h: A® § ……..…..…(3)

Dans la suite (2), prenons une combinaison.

$mP_k = P_{k-1} – T_{k,i}$ ……..…..(4)

Appliquons à (4) l'axiome (haut2) à gauche et l'axiome (haut1) à droite:

Nous obtenons l'inégalité :

$m^2 h(P_k) - C_2 \leq 2 h(P_{k-1}) + C_1$ ……………………………………..(5)

il en résulte l'inégalité .

$m^2 h(P_k) \leq 2 h(P_{k-1}) + C'$; $C' = C_1 + C_2$……………………………....(6)

En faisant la somme des inégalités (6) pour k=1, 2, 3, …, n

Nous obtenons l'inégalité

$h(P_n) \leq \frac{2}{m^2} h(P) + (m^{-2} + m^{-4} + \ldots + m^{-2n}) C_4$, $C_4 = c(C_1, C_2)$ ………..(7)

Pour m ≥ 2, (7) implique l'inégalité:

$h(P_n) \leq u(n) h(P) + \frac{1}{m^2} (1-m^{-2})^{-1}$ avec $\lim_{n \to \infty} u(n) = 0$ ……………..….(8)

Donc à la limite h (P_n) est borné par une certaine constante B

$h(P_n) \leq B$ ………………. (9)

L'axiome (haut3) implique l'ensemble de ces points P_n est fini; ………….. (10)

Les relations (1) et (10) impliquent que le groupe A est engendré

par les poins T_i et P_j………………………………………(11)

Il en résulte que tout point P du groupe A est une ♦- combinaison linéaire.

$P = c_1T_1 + \ldots + c_rT_r + d_1P_1 + \ldots + d_sP_s$; ………………………….……(12)

Donc le groupe abélien est de type fini.

Appliquons cette proposition au groupe de Mordell-Weil

PROPOSITION 9:

Le groupe de Mordell-Weil E (K) d'une courbe elliptique E/K

Est de type fini.

C'est le théorème de Mordell-Weil d'une courbe elliptique.

La proposition 8 est le théorème de descente des courbes elliptiques.

La structure du groupe de Mordell-Weil E (K) d'une courbe elliptique est semblable à celle du groupe U(L) des unités d'un corps de nombre algébrique L.

THEOREME DES UNITES DE DEDEKIND.

Soit un corps de nombres algébriques L, de degré n = s +2t,
qui a s conjugués réels s (L) et 2t conjugués complexes $\overline{t(L)} = t(L)$.
Alors, les unités du corps L forment un groupe abélien U (L)
multiplicatif de type fini .

$$U(L) \simeq D(L) \times \mu^{r}$$

Où D(L) est le groupe des racines de 1 contenues dans L?
$r = s+t- 1$ *et* μ^{r} *= r copie du groupe* μ .

DEFINITION 7 :

L'entier r = s + t – 1 est le rang du groupe des unités de L.

DEFINITION 8 :

1) *une unités d'un corps de nombres algébriques L est un entier u de L de norme* $N_{L/Q} = \pm 1$.
2) *Un système complet d'unités indépendantes du groupe U(L) est un système d'unités* $u_1,\ldots,u_n$ *tels que la relation* $u_1^{e_1}u_2^{e_2}\ldots.u_n^{e_n}=1$ *implique* $e_1,\ldots,e_n=0$.
3) *Un système d'unités fondamentales de L est un système de r unités* $u_1,\ldots, u_r$ *qui engendrent le groupe des unités, alors toute unité u de L est de la forme*

$u = u_1^{a_1}u_2^{a_2}\ldots.u_r^{a_r}$, $a_1,\ldots,a_r$ *dans* μ

Il n'y a pas d'unités dans la courbe elliptique E, il y en a dans le corps de base K de E (K).

PROPOSITION 10 :

Le groupe de Mordell-Weil E (K) d'une courbe elliptique E
Est isomorphe au produit direct de groupes.

$$E(K) \simeq T(E) \times \mu^{r},$$

Où T(E) = groupe de torsion de E,
r = entier ≥ 0
μ^{r} *= r copies du groupe abélien* μ

Le groupe T(E) est fini, le groupe $\blacklozenge^{r}$ est infini, le groupe quotient E (K)/T(E) est donc la partie infinie de la courbe elliptique E.

DEFINITION 9 :

L'entier r = r(E) est le rang de la courbe elliptique E, c'est le nombre de points de E (K) qui sont indépendants et qui engendrent la partie infinie de E.

Ces points ont une hauteur minimale

Citons quelques hauteurs, [17-1]

DEFINITION 10:

1- la hauteur logarithmique hauteur de Weil sur E est la fonction

$$h_x : E(\infty) \to \S \ ; P=(x, y) \to h_x(P)$$

de valeur $h_x(P) = \log(\max(|p|,|q|))$ *si* $P \neq O_E$, $x=p/q \in Q$ *et* $h_x(O_E)=0$

2- la hauteur canonique de Néron-Tate est la fonction

$$\hat{h} : E(K_{alg}) \to \S$$

de valeur $\hat{h}(P) = \frac{1}{\deg f} \lim_{N \to \infty} 4^{-N} h_f\left(2^N P\right)$

Où $f \in E(K)$ *est une fonction paire non constante,*

$h_f(P)=h(fP)$, *h= hauteur logarithmique.*

Cette hauteur canonique $\hat{h}$ possède plusieurs propriétés qui sont énoncées dans le

THEOREME ***(Néron-Tate)***

Soit une courbe elliptique E/K et la hauteur canonique $\hat{h}$ *sur E*

1) *Pour tout points Pet R de E (K), la hauteur* $\hat{h}$ *satisfait la loi de parallélogramme.*

$$\hat{h}(P+R) + \hat{h}(P-R)=2\hat{h}(P)+2\hat{h}(R)$$

2) *Pour point* $P \in E(K_{alg})$ *et tout entier* $m \in \mathbb{Z}$,

$$\hat{h}(mP)=m^2 \hat{h}(P).$$

3) $\hat{h}(P)=0$ *si et seulement si P est un point de torsion*

Et $\hat{h}(P)> 0$ *sinon;*

4) $\hat{h}$ *est une forme quadratique sur* $E(K_{alg})$ *:*

la fonction $\langle , \rangle : E(K_{alg}) \times E(K_{alg}) \to \S$ *est bilinéaire :*

$$\langle P, R \rangle = \hat{h}(P+R) + \hat{h}(P-R) - \hat{h}(P) - \hat{h}(R)$$

Cette forme quadratique $\langle , \rangle$ sur E permet d'introduire un invariant de la courbe elliptique E : le régulateur

DEFINITION 11 :

Le régulateur d'une courbe elliptique E/K est égal au déterminant

$$R(E, K) = det (\langle P_i, P_j \rangle) , 1£ i, j£ r$$

Où r =r(E) = rang de E, P_1,…...P_r = système générateur des points indépendants qui engendrent E/T(E).

$\langle , \rangle$ *= forme quadratique bilinéaire de Néron-Tate.*

6- VALUATIONS D'UN CORPS ET REDUCTION D'UNE COURBE ELLIPTIQUE

La théorie des valuations d'un corps est traitée dans les ouvrages de théorie des nombres comme [20].

DEFINITION 12 :

Une valuation d'un corps K est une fonction à valeurs réelles :

$$V : K® \S$$

Qui satisfait les 3 axiomes :

(Val$_1$) *V(x) ³ 0 pour tout élément x de K et V (x) = 0*

Si et seulement si x= 0

(Val$_2$) *V (xy) = V(x) V(y) pour tout éléments x et y de K*

(Val$_3$) *V(x)£ 1 implique V (1+x) £ c pour une constante c ³ 1.*

L'axiome ***(Val$_2$)*** implique que la valuation V est un homomorphisme du groupe multiplicatif K* dans le groupe $\S^+$.

L'axiome ***(Val$_3$)*** peut être remplace par l'inégalité triangulaire

$$V (x+y) £ V(x) +V(y)$$

La valuation V est archimédienne lorsque c = 2 dans ***(Val$_3$);*** elle est non archimédienne lorsque c = 1.

Exemples de valuations de corps

1. la valeur absolue usuelle sur le corps ♣

   $V(x) = |x| = \max \{x, -x\}$.

   Elle est archimédienne.
2. la valuation p-adique sur le corps Q.

   Pour tout nombre premier p, $V_p(p) = 1/p$ et $V_p(q) = 1$ pour tout nombre premier $q \neq p$.

   Elle non archimédienne
3. la valuation triviale : V: K→♣.

Elle prend les 2 valeurs : $V(0) = 0$ et $V(x) = 1$ pour tout élément x du corps K*.

C'est avec les valuations du corps de base K d'une courbe elliptique qu'on obtient les réductions d'une courbe elliptique.

DEFINITION 13:

La réduction d'une courbe elliptique E/K modulo une valuation V de K

Est l'application :

$$E(K) \to \tilde{E}(K)$$

$$P \to \overline{P}$$

Où la courbe réduite $\tilde{E}$ modulo V est obtenue avec

L'application $K \to k, x \to V(x)$.

La courbe réduite $\tilde{E}$ modulo V possède des invariants réduites

DEFINITION 14:

1) *la courbe elliptique E/K a une bonne réduction $\tilde{E}$ modulo V si la courbe réduite $\tilde{E}/k$ est non singulière.*
2) *La courbe elliptique a une mauvaise réduction si la courbe réduite est singulière*
   La réduction est multiplicative si $\tilde{E}$ a un nœud.
   La réduction est additive si $\tilde{E}$ à un point de rebroussement.

EXEMPLE 1.

Courbe elliptique d'équation de Weierstrass:

$E_1 : y^2 - 4xy - 2y = x^3 + 4x^2 + 3x + 6 \in \infty [x, y]$

Calcul du discriminant: $\Delta(E_1) = -4 \times 13183$

Réduisons la courbe E/Q modulo la valuation p-adique V_5

La courbe réduite $\tilde{E}$ a pour équation:

$\tilde{E}_1 : y^2 + xy + 3y = 4x^2 + 3x + 1 \in \mathbb{F}_5 [x, y]$.

Calcul du discriminant: $\Delta(\tilde{E}_1) = 2 \neq 0 \bmod 5$.

Donc la courbe E a une bonne réduction modulo 5.

EXEMPLE 2

Courbe elliptique d'équation de Weierstrass

$E_2 : y^2 + 4xy + 6y = x^3 - 4x^2 - 14x - 9 \in \mathbb{Q}[x, y]$

Calcul du discriminant: $\Delta(E_2) = 2^6 3^3$

Réduisons la courbe modulo 3:

$\tilde{E}_2 : y^2 + xy = x^3 + 2x^2 + x \in \mathbb{F}_3[x, y]$.

Calcul du discriminant de la courbe $\tilde{E}_2$ réduite :

$\Delta(\tilde{E}_2) = 0 \bmod 3$

Donc la courbe réduite $\tilde{E}_2$ est singulière; elle a une mauvaise réduction en p=3.

Calcul de l'invariant $c_4(\tilde{E}_2)$

$c_4(\tilde{E}_2) = 0 \bmod 3$.

Donc la courbe elliptique E_2 a une réduction additive en p=3.

CHAPITRE IV: TORSION DE COURBE ELLIPTIQUE

Dans le chapitre III, paragraphe 3, nous avons définir les points de groupe de Mordell-Weil E(K) d'ordre fini, les sous groupes de m-torsion E(K)[m] et le groupe de torsion T(E).

Dans ce chapitre nous allons décrire les corps de nombres quadratique, la théorie des isomorphismes, la construction des groupes de torsion T (E) (∞).

1- CORPS DE NOMBRES ALGEBRIQUES QUADRATIQUES.

Un corps quadratique est une extension du corps ∞ des nombres rationnels par un nombre irrationnel quadratique.

$K=¥(\sqrt{d}),\ d$ Î ¨, sans facteur carré ………….(1)

Tout élément de K est de la forme

$x = a+ b\sqrt{d}$;…………………………………..(2)

Un entier du corps K est un élément qui satisfait une équation

$x^2+A\,x+B = 0;\quad A, B$ Î ¥ ……………………...(3)

Les entiers du corps K sont de la forme

$$\begin{cases} e=\frac{1}{2}\left(1+\sqrt{d}\right) \text{ lorsque } d\ °1 \bmod 4 \\ \text{Et} \\ e=\sqrt{d} \qquad \text{lorsque } d\equiv 2, 3 \bmod 4 \end{cases} \quad \text{……………….. (4)}$$

Les entiers de K forment un anneau A(K) qui a une structure de ♦-module:

A_K=♦+♦$_e$ ………………………………………(5)

Le discriminant du corps K est égal au discriminant d'une base d'entiers:

$$\begin{cases} D(K)=d \text{ lorsque } d\ °1 \bmod 4 \\ Et \\ D(K)=4d \text{ lorsque } d°2, 3 \bmod 4 \end{cases} \quad \text{……………….. (6)}$$

Les nombres premier p∈Z engendrent des idéaux pA_K qui se décomposent dans l'anneau A_K suivant 3 types, p impair

pA_K=PP' : p est décomposé, les idéaux P, P' sont premier de norme commune NP=NP '= p ……………………………………………………..………(7-1)

pA_K=P^2: p est ramifie; alors il divise le discriminant D(K); l'idéal P est premier de norme NP= p ………………………………………………..………(7-2)

pA_K=P : p est inerte; alors l'idéal P est premier de norme NP= p^2.

Le nombre premier p=2 engendre un idéal $2A_K$ qui se décompose

$2A_K$ = PP ', les idéaux P≠P' sont premier de norme commune

NP=NP '= 2 lorsque D (K) ≡1 mod 8;

$2A_K$ = P, l'idéal P est premier lorsque D (K) ≡5 mod 8;

Lorsque 2 divise le discriminant D(K), il st ramifier .

D'après le théorème de dédekind sur le rang du groupe U (K) des unités,

il y a 2 cas possible:

a) lorsque K est quadratique réel, s=2, t=0 et r =1, il y a donc une unité fondamentale.

Plusieurs auteurs ont déterminé des tables d'unités fondamentales comme Borevich et chafarevich dans " théorie des nombres",Gauthver –Villars- Paris.(1966).

Il y a des logiciels de calcul de ces unités

Dans le groupe U (k) des unités, seuls ±1 est des racines de 1.

b) lorsque k imaginaire, s=0, t=2 et r=0,

Le groupe U (k) est réduit aux racines de 1

U (k) = {±1, ±*i*} pour d = - 4, i^4= (-*i*) ^{4}=1

U (k) = {±1, ±*j*, ±j^2} pour d = -6, j^3= (j^2) ^{3}=1

Et U (k) = { ±1 } pour les autres d < 0.

2- TORSION DU GROUPE DE MORDELL-WEIL E (K)

a- Kubert a étudie des bornes pour l'ordre du groupe de torsion T(E)(K) d'une extension finie du corps ∞ dans " Universal bounds on the torsion of elliptic curves" –proc. London math. Soc. 33 (1976) 193-237.

Il utilise des n-cycles et des courbes modulaires X_0(n), X_1(n).

b- Manin a prouvé le résultat :

THEOREME 1:

Soit une courbe elliptique E sur un corps de nombres K et un nombre premier p

Alors il y a une constante N=N (K, p) telle que la composante p- primaire du groupe E (K) à un ordre qui divise p^N.

Preuve dans: " the p-torsion of elliptic curves is uniformly boundet ", izv.Akad Nauk. SSSR. 33 (1969) AMS transl, 433-438

Ce théorème implique la

CONJECTURE

Le groupe de torsion T(E) (K) est d'ordre borné par N

c- La structure de groupe de torsion T(E) (∞) de courbes elliptiques E/∞ a été Conjecturée par Ogg.
Mazur a prouvé cette conjecture dans [13-2]

THEOREME 2 (Mazur)

Le groupe de torsion T(E)(¥) d'une courbe elliptique E/ ¥ est un groupe abélien fini isomorphe à l'un des 15 groupes:

¨/m ¨ pour 1£ m £ 10 ou m=12

¨/2 ¨ ´ ¨/2d ¨ 1£ d £ 4

Preuve (d'après Mazur)

La structure du groupe de torsion T(E) (∞) est apparue au cours de la recherche des nombres premiers N telles qu'il existe des courbes elliptiques qui admettent des

N-isogénies ∞-rationnelles.

Alors, la représentation de groupes:

$$r_N : Gal\ (K_{alg}/K) \to GL\ (2, \ ¨/n\ ¨)$$

Est surjective.
Ces points de torsion du groupe T(E)(∞) ont des propriétés déterminées dans

" rationals points on modular curves", Lectures Notes in Math. 601.

Supposons que le groupe E(∞) ne possède pas des points d'ordre N=11 et N≥17

Cela implique que la courbe elliptique E a une bonne réduction potentielle en p =3. Par la théorie de Néron sur la spécialisation d'un point, la fibre de Néron du groupe E (F_3) possède un point d'ordre N≤4; ce résultat est en contradiction avec l'hypothèse N>7. Il en résulte le théorème de Mazur

Ce théorème montre que le groupe de torsion T(E)(∞) est d'ordre ≤ 16.

THEOREME 3 (Corollary 4-6 de Mazur)

Soit un corps quadratique imaginaire K=¥(√−d), d>0.

Alors il y a un ensemble fini B de nombres premiers tels que, si N est un nombre premier hors de B, qui est inerte dans K, il n'y a pas sur le groupe E (K) de points de torsion d'ordre N.

d- indiquons la méthode utilisée par Fung , Stroher, williams et Zimmer pour déterminer des groupes de torsion T(E)(K) sur un corps cubique pur K=∞(∛(a b²) ,

a et *b* entiers positifs sans facteurs carrés, la courbe elliptique E ayant un invariant modulaire *j*(E) entier.

En utilisant plusieurs propriétés (isomorphismes de courbes elliptiques, unités fondamentales du corps k, valuations de k, réduction de la courbe E, entiers

x= *a*+*b* ∛(a b²) +*d* ∛(a b²) , décompositions des idéaux du corps k , ces auteurs obtiennent le résultat .

THEOREME 4

Soit une courbe elliptique E sur un corps cubique pur K, avec un invariant modulaire j(E) de valuation v (j(E)) ≥0 pour chaque valuation v de k qui divise 2 ou 3.

Alors, à isomorphisme prés, les groupes de torsion T(E)(k) sont isomorphes à l'un des 8 groupes abéliens:

¨/2¨, ¨/2¨Å¨/2¨, ¨/4¨, ¨/3¨, ¨/2¨Å¨/3¨, ¨/2¨Å¨/6¨, ¨/12¨, Z/5¨

Preuve dans "torsion groups of elliptic curves with intégral j-invariant over pure cubic fields ", jour. of number theory 36 (1990), 12-45.

Ce théorème implique que le groupe de torsion T(E)(K) est d'ordre fini ≤ 12. Pour K=∞(∛(a b²)).

3- ISOMORPHISMES DE COURBES ELLIPTIQUES

Soit une courbe elliptique E d'équation de Weierstrass

$E: y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$;.....(1)

Le morphisme E (K) $\rightarrow$E'(K) de groupes abéliens de valeurs $x = u^2X+r$,

$y=u^3Y+su^2X+t$ avec $u \neq 0, r, s, t \in K$.....(2)

Est un isomorphisme de courbes elliptiques qui transforme la courbe elliptique E en la courbe isomorphe

E': $Y^2 + a'_1 X Y + a'_3 Y = X^3 + a'_2 X^2 + a'_4 X + a'_6 \in K[X, Y]$; ..... (3)

Avec le calcul nous obtenons les relations entre les invariants des 2 courbes elliptiques.

En particulier, $u^{12}=D(E')=D(E)$, et $j(E) = j(E)$.

Il en résulte que les courbes elliptiques isomorphes ont des invariants modulaires égaux.

Dans la méthode Fung, citée précédemment, les auteurs ont utilisée l'isomorphisme de courbes elliptiques pour transformer la courbe E en la courbe E'.

$E': Y^2=X^3+AX+B \in K[X, Y]$

La théorie de cet isomorphisme peut être consulté dans l'ouvrage [17-1]

4- GROUPES DE TORSION SUR UN CORPS QUADRATIQUE.

Nous décrivons deux méthodes d'étude de ces groupes T(E) (K), pour $K=¥(\sqrt{d})$.

a) méthode de Kenku dans " certain torsion points on elliptic curves défined over quadratic Fields"- jour. London Math. Soc (2) 19 (1976); 233-240.

Manin a prouvé que pour chaque nombre premier p, il existe un entier non négatif n = n (k, p) tel que le groupe de p-torsion E(K)[p] est d'ordre $\leq p^n$

Le théorème de Mordell- Weil qui prouve que le groupe abélien E(K) est de type fini implique que le groupe de torsion T(E)(¥) est fini.

Soit le demi plan supérieur H = {z∈C; z=x+iy; y>0} et les sous groupe de la congruence modulaire de niveau N:

$$\Gamma_1(N) = \{A \in SL(2, \blacklozenge).\ A \equiv \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \bmod N\}$$

$$\Gamma_0(N) = \{A \in SL(2, \blacklozenge).\ A \equiv \begin{pmatrix} x & x \\ 0 & x \end{pmatrix} \bmod N\}$$

SL (2, ♦) désigne le groupe spécial linéaire; il est formé des 2×2 matrices $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de déterminant 1 et de coefficients entiers.

Une matrice A opère sur le demi-plan H par homographie

$$Az = \frac{az+b}{cz+d}$$

Les 2 sous groupes de congruences modulaires $\Gamma_1(N)$, $\Gamma_0(N)$ permettent de construire des surfaces de Riemann. Ces surfaces modulaires $X_1(N)$, $X_0(N)$.

La théorie de ces courbes modulaires se trouve dans [17-2]

Kenku étudie la courbe modulaire $X_1(32)$ et les points paraboliques pour le sous groupe de congruence modulaires $\Gamma_1(32)$, notions disponibles dans [16]

Il démontre le

THEOREME 5

Il n'y a pas de courbe elliptique E sur K, K=¥ ($\sqrt{d}$) qui a un point d'ordre 32 sur le corps quadratique K.

b) Méthode de kamieny dans " torsion points on elliptic curves over all quadratic fields"- Duke Mathématical journal (march 1986)- 157-162.

Kamieny commence par décrire quelques courbes modulaires $X_0(p)$ pour p premier et leur variété abélienne Jacobienne J(p) pour p= 17, 19, 23, 29 et 31

THEOREME 6

Les courbes modulaires $X_1(17)$, $X_1(19)$, $X_1(23)$, $X^{(7)}(29)$, $X^{(5)}(31)$ ne sont pas des courbes hyperelliptiques.

Une courbe modulaire elliptique est de genre égal à 1.

Une courbe modulaire hyperelliptique est de genre g≥2.

$X^{(n)}(p)$ désigne l'unique recouvrement de $X_0(p)$ de degré n.

Kamieny prouve le

THEOREME 7

Soit p = 17, 19, 23, 29 ou 31 et un corps quadratique K.

Alors il n'existe pas de courbe elliptique E sur K contenant des points k-rationnels

D'ordre p

Kamieny a étudie les points de torsion de courbes elliptiques sur ¥ ($\sqrt{d}$) dans

"Points of order p on elliptic curves over ¥ ($\sqrt{d}$) - Math. Annals 261(1982)413-424"

c) Il y a une méthode de points d'ordre m d'une courbe elliptique E/K basée sur la réduction de E.

PROPOSITION

Soit une courbe elliptique E/K et la réduction mod p.

Si la courbe réduite $\tilde{E}(F_p)$ est non singulière alors l'application :

$$E(K)[m] \to \tilde{E}(F_p)$$

Est injective.

Preuve :[17-2], proposition VI-3-1.

5- ALGORITHMES DE CALCUL

EXEMPLE 1

Soit la courbe elliptique E d'équation de Weierstrass.

$$E: y^2 + y = x^3 - x + 1 \hat{I} ¥[x, y] \ldots\ldots\ldots\ldots (1)$$

Calcul des invariants : $\Delta(E) = -643$, premier cela implique que la réduction modulo 2 est bonne.

La résolution de l'équation (1) dans F_2

Pour $x = 0$, $y^2 + y \equiv 1 \bmod 2$, pas de solution,

Pour $x = 1$, $y^2 + y \equiv 1 \bmod 2$, pas de solution,

Cela implique $\tilde{E}(F_2) = \{O_E\}$

L'injection $E(¥)[m] \to \tilde{E}(F_2)$ implique

$$E(¥)[m] = \{O_E\}.$$

Donc E (¥) n'a pas de points de m-torsion.

EXEMPLE 2

Courbe elliptique E d'équation de weierstrass.

$$E: y^2 = x^3 - x \quad \hat{I}\ ¥[x, y] \quad \ldots\ldots\ldots\ldots \quad (1)$$

Calcul des invariants: $\Delta(E) = -64$.

Le point $(0, 0) \in E(¥)$ est d'ordre 2.

Réduction mod3: l'équation (1) réduite admet 4 solution :

$(0, 0)$, $(2, \pm 1)$ et O_E.

Réduction mod5: l'équation (1) réduite admet 8 solution :

$(0, 0)$, $(3, \pm 3)$, $(5, \pm 2)$, $(1, \pm 3)$ et O_E.

L'injection $E(¥)[m] \to \tilde{E}(F_p)$ implique les isomorphismes

$\tilde{E}(F_3) \pi \blacklozenge/4\blacklozenge$ et $\tilde{E}(F_5) \pi (\blacklozenge/2\blacklozenge)^2$

Il en résulte le groupe de torsion $E(¥)[m] = \{(0, 0), O_E\}$.

Ces exemples terminent mon mémoire.

Résumé:

Cette étude concernant le groupe de torsion de courbe elliptique sur une extension quadratique du corps ¥.On commence par un aperçu sur les variétés abéliennes. Puis on expose des généralités arithmétiques et géométriques sur les courbes elliptiques. Ensuite nous établissons la structure de groupe abélien de Mordell-Weil, on s'intéresse aux points d'ordre fini, les sous groupe de m- torsion E (K)[m] et le groupe de torsion T(E). On donne également deux méthodes d'étude de ces groupes T(E) (K), pour $K=¥(\sqrt{d})$ *Méthode de Kamieny [8] et méthode de Kenku* [9].

ملخص:

في هذه المذكرة الدراسة تخص زمر فتل المنحنيات الاهليليجية المعرفة على امتـــداد تربيعـــي للحقل∞ ، بدئنا بلمحة على المنوعات الآبيلية ، ثم عرضـــنا عموميـــات حـــسابية و هندســـية علـــى المنحنيات الاهليليجية، وبعدها أنشئنا بنية زمرة تبديلية لMordell-Weil واهتممنا بالنقط ذات الرتب المنتهية ، الزمر الجزئية لـــ m –فتل$E\ (K)[m]$ وزمر الفتلT(E). وأعطينا طريقتين لدراســـة هـــذه الزمر T(E) (K), من اجل $K=\infty(\sqrt{d})$ طريقة [8] *Kamieny* و طريقة.[9] *Kenku*

Abstract

This paper is a survey concerning the torsion groups of elliptic curves over quadratic Fields. One starts with a preview on the Abelian varieties. Then one exposes arithmetic and geometric generalities on the elliptic curves. Then we establish the structure of Abelian group of Mordell-Weil, one is interested in the points of finite order, the subgroup of m - torsion E (K)[m] and the group of torsion T(E). One also gives two methods of survey of these T(E groups) (K), for $K = ¥(\sqrt{d})$ *Method of Kamieny [8] and method of Kenku [9].*

REFERENCES

[1] BIRCH –B-T and KUYK: Modular functions of one variable IV- lecture notes in Math.476- springer (1975);

[2] J.CASSELS: diophantine equations with special reference to elliptic curves- jour London Math- soc 4(1966/193-291);

[3] LOX and LITTELE and O'SEA: using algebraic geometry graduate texts in Mathematics n° 185;

[4] R-HARTSHORNE: Algebraic Geometry-Graduate texts in math53-springer (1982);

[5] HARRIS: Algebraic Geometry – A first course – GTM 185;

[6] HUSEMOLLER: elliptic curves- GMT 133;

[7] ITAKA: Algebraic Geometry GMT 76;

[8] S.KAMIENY: torsion points on elliptic curves over all quadratic fields- duke math. Jour -53 (march 1986/157-162);

[9] M-A- KENKU: certain torsion points on elliptic curves defined over quadratic fields Jour. London Math. Soc 19(1979/233-240);

[10] N-KOBLITZ: introduction to elliptic curves and modular forms- GTM 97 (1984);

[11] D-KUBERT: universal bounds on the torsion of elliptic curves proc. Lond. Math. Soc .33 (1976/ 193-237);

[12] S-LANG: 1) abélian varieties- interscience pub. New york (1959)
2) Elliptic curves Diophantine analysis -springer-(1978);

[13] B-MAZUR: 1) Rational points of modular curves –LNM 349(1976)
2) Rational isogenies of prime degree-inv. Math.44 (1978)-129-162;

[14] J.P.SERRE: 1) Propriétés galoisiennes des points d'ordre fini des courbes elliptique – Inv. math 15 (1972) 259-331.
2) Géométrie algébrique et géométrie analytique –annal. Inst fourier-6 (1956)/1.42);

[15] I-R- SHAFAREVICH: Basic Algebraic geometry – Springer (1977)

[16] C. SHIMURA: Introduction to the Arithmetic Théory of Automorphic Functions- Princeton Univ. Press (1971).

[17] J. H. SILVERMAN: 1) The Arithmetic of Elliptic Curves. GTM 106 (1986)

2) Lower Bound for Canonical Height on Elliptic Curves. Duke Math. Jour. 48(1981)633-648.

[18] J- TATE: The Arithmetic of Elliptic Curves- Inv. Math 23(1974)179-206

[19] A- Weil: Courbes Algébriques et Variétés Abéliennes- Hermann (1971).

[20] E-WEISS: Algebraic Number Theory- McGraw- Hill Book Company. Inc. New York (1974).

[21] ZARISKI e SAMUEL: Commutative Algebra Vol I et Vol II GTM 28 et 29.

[22] ZITOUNI: Géométrie, Arithmétique, Algorithmique Des Courbes Elliptique- O.P.U -Alger (2005).