N° d'ordre :

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

Université des Sciences et de la Technologie
Houari Boumediene

Faculté de Mathématiques

MEMOIRE
Présentée pour l'obtention du diplôme de MAGISTER
En : MATHEMATIQUES
Spécialité : **Algèbre et Théorie des Nombres**

Par M^me^ : OUAGAGUI Souhila

Sujet

LES ISOGENIES DE COURBES ELLIPTIQUES

Soutenue le : / / 2009, devant le jury composé de :

Mr Meziane AIDER	*Professeur à l'U.S.T.H.B*	*Président*
Mr Mohamed-ZITOUNI	*Professeur à l'U.S.T.H.B*	*Directeur de thèse*
Mr Rachid BEBBOUCHI	*Professeur à l'U.S.T.H.B*	*Examinateur*
Mr Mohand-Ouamar.HERNANE	*Maître de conférence l'U.S.T.H.B*	*Examinateur*
Mr Boualem BEN SEBAA	*Maître de conférence l'U.S.T.H.B*	*Examinateur*

SOMMAIRE

Introduction

Ma thèse porte sur les isogénies de Courbes Elliptiques .
J'ai décrit quelques propriétés des Variétés Affines, des Variétés Projectives et des Variétés Abéliennes.

Une Courbe Elliptique a une structure de Variété Abélienne de dimension un ; ces Variétés munies de la topologie de Zariski deviennent des espaces topologiques.

J'ai étudie les courbes algébriques planes qui sont liées aux Courbes Elliptiques ; ce sont des cubiques de Weierstrass. J'ai utilisé des changements linéaires de variables pour introduire plusieurs invariants de ces cubiques, J'ai utilisé la théorie du résultant de 2 polynôme $f, g \in \mathrm{IR}[x]$ pour obtenir une relation entre les discriminants $\mathrm{Dis}(f)$ d'un polynôme f et $\Delta(E)$ d'une cubique de Weierstrass.
Cela m'a permis de classifier ces cubiques de Weierstrass en 4 classes .

Ensuite, j'ai déterminé une loi de groupe abélien sur l'ensemble E(K) des points *K*-rationnels de E avec la règle géométrique de 3 points colinéaires d'une Courbe Elliptique .
J'ai obtenu les formules des coordonnées des points $-P$, $P_1 + P_2$ et $2P$.
J'ai ensuite établi les propriétés de quelques homomorphismes de Courbes Elliptiques :
Isomorphismes, Automorphismes, Endomorphismes et Isogénies.

CHAPITRE I
GEOMETRIE DES COURBES ELLIPTIQUES.

Les Courbes Elliptiques sont des Courbes algébriques planes particulières, c'est pourquoi nous commençons par une étude des courbes algébriques planes.

La théorie de ces courbes se trouve dans les ouvrages de Géométrie Algébrique (HARTSHORNE [5], SHAFAREVICH [16] , etc …) .

1-Courbes algébriques planes : équations et classifications.

Définition 1 :

Une courbe algébrique plane est l'ensemble des points P = (x,y) qui satisfont l'équation f(x,y) = 0 , où f(x,y) est un polynôme de degré n de l'anneau IR[x,y] .

Pour n =1 : les courbes algébriques sont des droites :

$$f(x,y) = (d_1x + d_2y) + d_3 ; \quad (1)$$

Pour n = 2 : les polynômes sont de la forme :

$$f(x,y) = (d_1x^2 + d_2xy + d_3y^2) + (d_4x + d_5y) + d_6 ; \quad (2)$$

Les courbes sont des cercles lorsque :

$$f(x,y) = (x-d_1)^2 + (y-d_2)^2 = r^2 ; \quad (3)$$

Des ellipses lorsque :

$$f(x,y) = \frac{x^2}{a^2} + \frac{y^2}{b^2} = 1 , a \neq b ; \quad (4)$$

Des hyperboles lorsque :

$$f(x,y) = \frac{x^2}{a^2} - \frac{y^2}{b^2} = 1 , a \neq b ; \quad (5)$$

Des paraboles lorsque :

$$f (x,y) = y^2 = 2ax ; \quad (6)$$

Pour n = 3 :les polynômes sont de la forme :

$f(x,y) = g_3 + g_2 + g_1 + g_0$, $g_i = g_i(x,y)$ = polynôme homogène de degré i , (7)

Les courbes algébriques associées sont des cubiques.

Dans la théorie des courbes algébriques, les courbes sont des quartiques pour n = 4, des quintiques pour n = 5, des sextiques pour n = 6, etc …

Un polynôme $f(x,y) \in IR[x,y]$ de degré n peut être factorisé ou non . Cela implique une classification des courbes algébriques en deux classes : la classe des courbes irréductibles et la classe des courbes réductibles.

Pour n =1 : les droites sont irréductibles.

Pour n = 2 : il y a les courbes irréductibles (cercles et coniques), et les courbes réductibles qui sont produit de deux droites.

Ces courbes algébriques de degré n = 2 sont des coniques : intersections d'un cône par un plan.

Pour n = 3 : il y a la classe des cubiques irréductibles et la classe des cubiques dégénérées en produit de trois droites ou dégénérées en produit d'une courbe quadratique par une droite .
Dans la classe des courbes algébriques, de degré n, irréductibles, il y a possibilité de points singuliers.

Cela implique une classification en deux classes :
Classe des courbes non singulières(pas de points singuliers) et classe des courbes singulières(admet un point singulier).
Le nombre s de points singuliers d'une courbe algébrique intervient dans l'invariant genre :

Définition 2 :
Le genre d'une courbe algébrique plane C de degré n , ayant s points singuliers , est l'entier naturel positif ou nul :

$$g(C) = (1/2)(n-1)(n-2) - s \; ; \qquad (8)$$

Exemples :
Les droites, les cercles, les coniques et les cubiques singulières ont un genre égal à g(C) = 0 .
Les cubiques non singulières ont un genre g(C) =1.

2-Equations de Weierstrass des cubiques irréductibles :
Une Courbe Elliptique est munie de plusieurs structures algébriques.
Nous choisissons la :
Définition 3 :
Une Courbe Elliptique E est une cubique plane, irréductible, non singulière, d'équation spécifique de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in \quad K [x , y] \; ; \qquad (1)$$

Où K est un corps commutatif global, local ou fini.
Les deux variables x et y sont des éléments d'une clôture algébrique K_{alg} du corps K.

Les propriétés de la Courbe Elliptique dépendent du corps de base K :
Lorsque K est le corps Q des nombres rationnels ou un corps de nombres algébriques nous étudions la Courbe Elliptique au moyen de la Théorie des Nombres (entiers algébriques, idéaux, équations diophantiennes, nombres premiers, fonctions arithmétiques, valuations, etc , …) .
Lorsque K est le corps C des nombres complexes , nous étudions la Courbe Elliptique au moyen de l'Analyse complexe (réseaux et tores complexes , fonctions elliptiques , formes modulaires , etc , …) et la Géométrie Algébrique (variétés abéliennes , diviseurs , schémas , cohomologie, etc , …)
Lorsque K est un corps fini IF_q, à $q = p^n$ éléments, p premier, nous étudions la Courbe Elliptique au moyen de la théorie des corps finis.
Lorsque K est un corps local, nous étudions la Courbe Elliptique au moyen de la théorie des corps locaux.
L'équation affine de Weierstrass se met sous la forme d'équation projective :

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4X Z^2 + a_6 Z^3 ; \quad \in IP^2 (K) \qquad (2)$$

L'équation (1) de Weierstrass peut être transformée au moyen de substitutions convenables. Nous éliminons les monômes en xy et en y avec le changement de variables linéaire :

$$(x , y) \longrightarrow [x , \frac{1}{2} (y - a_1x - a_3)] ; \qquad (3)$$

Nous obtenons pour un corps K de caract (K) ≠ 2, l'équation de Weierstrass :

$$E_1 : y^2 = 4x^3 + b_2x^2 + 2 b_4x + b_6 \quad \in \quad K [x , y] ; \qquad (4)$$

Les trois coefficients b_{2i} , sont des polynômes «homogènes» de degré 2i de l'anneau $Z[a_1, a_2 , a_3, a_4, a_6]$:

$$b_2 = a_1^2 + 4a_2 ; \ b_4 = a_1a_3 + 2a_4 ; \ b_6 = a_3^2 + 4a_6; \qquad (5)$$

L'élimination du coefficient 4 et du monôme en x^2 dans l'équation E_1 s'obtient avec le changement de variables linéaire :

$$(x , y) \longrightarrow [\frac{x - 3b_2}{36} , \frac{y}{108}] \qquad (6)$$

Pour caract (K) ≠ 2, 3, nous obtenons l'équation de Weierstrass :

$$E_2 : y^2 = x^3 – 27c_4x - 54c_6 \quad \in \quad K [x , y] ; \qquad (7)$$

Les deux coefficients c_{2i} sont des polynômes « homogènes » de l'anneau $Z[b_2 , b_4 , b_6]$

$$c_4 = b_2^2 - 24b_4 \quad ; \quad c_6 = -b_2^3 + 36 b_2b_4 - 216b_6 \ ; \qquad (8)$$

D'autres transformations permettent d'obtenir d'autres équations de Weierstrass :

(1) l'équation de Weierstrass :

$$E_3 : y^2 = x^3 + Ax + B ; \quad \in \quad K [x , y] ; \qquad (9)$$

(2) l'équation de Legendre :

$$E_4 : y^2 = x(x-1)(x-t) ; t \neq 0,1 \qquad (10)$$

(3) l'équation de Deuring :

$$E_5 : y^2 + txy + y = x^3 ; \text{ avec } t^3 \neq 3 ; \qquad (11)$$

(4) l'équation de Tate :

$$E_6 : y^2 + xy = x^3 + ax + b \; ; \; \in C[x, y] \; ; \qquad (12)$$

Les coefficients a et b admettent des développements en séries :

$$a = -5 \sum_{n\geq 1} n^3 q^n (1- q^n)^{-1} \; ;$$

$$b = -\frac{1}{12} \sum_{n\geq 1} q^n (7n^5 + 5n^3)(1- q^n)^{-1} \; ; \qquad (13)$$

avec $q = \exp(2i\pi z)$ et z dans le demi-plan supérieur $IH = \{z \in C , \text{Im } z > 0 \}$.

3- Invariants d'une Courbe Elliptique :

Tout Courbe Elliptique E possède plusieurs invariants : un discriminant, un invariant modulaire, un invariant différentiel, un conducteur, un régulateur, un rang, une série de Dirichlet, etc …

a) Discriminant d'une Courbe Elliptique :

Définition 4 :

Le discriminant d'une Courbe Elliptique E est le polynôme homogène, de degré 12 , dans l'anneau $Z[b_2 , b_4 , b_6 , b_8]$ égal à :

$$\mathbf{\Delta (E) = 9b_2b_4b_6 - 8b_4^3 - 27\, b_6^2 - b_2^2\, b_8 \; ;} \qquad \mathbf{(1)}$$

sur un corps K de caractéristique $p \neq 2,3$

Le coefficient b_8 est déterminé par la relation :

$$\mathbf{4b_8 = b_2b_6 - b_4^2 \; ;}$$

La cubique (7) a un discriminant égal à :

$$\Delta(E) = \frac{1}{1728} (c_4^3 - c_6^2) \; ; \qquad (2)$$

La cubique (9) a un discriminant égal à :

$$\Delta(E) = -16(4A^3 + 27B^2) \qquad (3)$$

La cubique (10) a un discriminant égal à :

$$\Delta(E) = 16t^2 (1-t)^2 \; ; \qquad (4)$$

Exemple :
Soit la Courbe Elliptique d'équation de Weierstrass :

$$E : y^2 -7xy + 4y = x^3 -5x^2 + 8x -14 \quad ;$$

Les coefficients b_{2i} sont égaux à :

$$b_2 = 29 \; ; \; b_4 = -12 \; ; \; b_6 = -40 \; ; \; b_8 = -326 \; ;$$

Le discriminant est égal à :

$$\Delta(E) = 370070 = 2 \times 5 \times 23 \times 1609 \; ;$$

Le genre est égal à :

$$g(E) = 1 \; ;$$

b) Invariant modulaire d'une Courbe Elliptique :
Définition 5 :
L'invariant modulaire d'une Courbe Elliptique E est l'élément j(E) du corps K égal à :

$$\mathbf{j(E) = \frac{c_4^{\,3}}{\Delta(E)} \quad ;} \qquad \mathbf{(5)}$$

Exemples :
1) L'invariant modulaire de la cubique d'équation de Weierstrass :

$$E : y^2 + 6xy -12y = x^3 -10x^2 + 5x - 25 \quad ;$$

Nous obtenons avec le calcul :

$$b_2 = -4 \; ; \; b_4 = -62; \; b_6 = 44 \; ; \; b_8 = -105 \; ;$$

Le discriminant $\Delta(E) = 2^9 \times 5 \times 769$ et le coefficient $c_4 = 2^5 \times 47$.

L'invariant modulaire de la cubique E est égal à :

$$j(E) = \frac{2^6 \times 103823}{5 \times 769};$$

2) L'invariant modulaire de la cubique d'équation de Weierstrass :

$$E : y^2 = x^3 + 4x +3 \quad ;$$

Nous obtenons avec le calcul :

$$b_2 = 0 \; ; \; b_4 = 8 \; ; \; b_6 = 12 \; ; \; b_8 = -16 \; ;$$

Le discriminant $\Delta(E) = -2^4 \times 499$ et le coefficient $c_4 = -2^6 \times 3$.

L'invariant modulaire de la cubique E est égal à :

$$j(E) = \frac{2^{14} \times 3^3}{499} \; ;$$

$$j(E) = \frac{2^{14} \times 3^3}{499} ;$$

c) Invariant différentiel d'une Courbe Elliptique :

Définition 6 :

L'invariant différentiel d'une Courbe Elliptique est l'élément différentiel :

$$\omega(E) = \frac{dx}{F_y'} = \frac{-dy}{F_x'} \quad ; \qquad (6)$$

lié à la forme différentielle :

$$dF = F_x' \, dx + F_y' \, dy ;$$

où $F(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ est l'équation de Weierstrass de la cubique E .

F_y' est la dérivée partielle de F par rapport à y et

F_x' est la dérivée partielle de F par rapport à x.

Exemples :

1) L'invariant différentiel de la cubique d'équation de Weierstrass :

$$E : y^2 - 7xy + 4y = x^3 - 5x^2 + 8x - 14 ;$$

Le polynôme $F(x,y) = y^2 - 7xy + 4y - x^3 + 5x^2 - 8x + 14$; ses dérivées partielles du 1er ordre sont égales à :

$$F_x' = -7y - 3x^2 + 10x - 8 \text{ , et } F_y' = 2y - 7x + 4 ;$$

L'invariant différentiel de cette cubique E est égal à :

$$\omega(E) = \frac{dy}{7y + 3x^2 - 10x + 8} = \frac{dx}{2y - 7x + 4} ;$$

2) L'invariant différentiel de la cubique d'équation de Weierstrass :

$$E : y^2 + 6xy - 12y = x^3 - 10x^2 + 5x - 25 ;$$

Le polynôme $F(x , y) = y^2 + 6xy - 12y - x^3 + 10x^2 - 5x + 25$; ses dérivées partielles du 1er ordre égales à :

$F_x' = 6y - 3x^2 + 20x - 5$, et $F_y' = 2y + 6x - 12$;

L'invariant différentiel de cette cubique E est égal à :

$$\omega(E) = \frac{-dy}{6y - 3x^2 + 20x - 5\ ;} = \frac{dx}{2y + 6x - 12}\ ;$$

4-Variétés algébriques abéliennes :

Une Courbe Elliptique admet une structure de Variété abélienne de dimension un.

Nous indiquons quelques notions de Variétés algébriques en nous inspirant d'ouvrages de Géométrie Algébrique : [5] , [16] , [11] .

Nous décrivons successivement les espaces et les Variétés affines, les espaces et les Variétés projectives, les Variétés abéliennes, les Diviseurs.

Espaces affines, Variétés affines :

Considérons un corps K algébriquement clos et le K- espace vectoriel K^n des points $a = (a_1 , \dots , a_n)$ à n coordonnées $a_1 , \dots , a_n$ dans K .

Définition 7 :

Un n-espace affine sur un corps K est l'ensemble des n-uples $(a_1 , \dots , a_n)$ d'éléments de K :

$$\mathbb{A}^n(K) = \{a = (a_1 , \dots , a_n) ; a_1 , \dots , a_n \in K\} \qquad (1)$$

C'est un espace de dimension n.

Cet espace est muni d'une topologie spéciale : la topologie de Zariski qui repose sur les ensembles algébriques.

Définition 8 :

Un ensemble algébrique affine est l'ensemble des zéros d'une famille de polynômes $f_1, \dots , f_d$ de l'anneau $K[X_1 , \dots , X_n]$ associé au n - espace affines $\mathbb{A}^n(K)$.

Ce sont les ensembles algébriques de l'espace $\mathbb{A}^n(K)$ qui jouent le rôle de fermés .

Définition 9 :

La topologie de Zariski est formée par les ensembles algébriques comme des fermés et leurs complémentaires comme des ouverts.

Pour cette topologie, l'ensemble vide et l'espace $\mathbb{A}^n(K)$ sont les seules parties ouvertes et fermées à la fois .

Cette topologie n'est pas de Hausdorff.

Avec cette topologie, l'espace affine devient une Variété affine.

Définition 10 :

(1) Une Variété affine est une partie d'un espace affine, irréductible et fermée pour la topologie de Zariski.

(2) Une Variété quasi affine est une partie ouverte d'une Variété affine.

(3) Une sous Variété d'une Variété affine V est une partie Y de V irréductible et fermée.

Exemple :
L'ensemble V = { a = (a_1 , a_2 , a_3) Є $/A^3$(IR) ; f(a) = 0 ; f(x , y , z) = $x^2 y - xz^2$ } ;
muni de la topologie de Zariski est une Variété affine .

Pour obtenir une Variété projective, nous considérons une relation d'équivalence R dans l'espace affine $/A^{n+1}$(K) :
« Deux points a = (a_1 , a_2 , …, a_n , a_{n+1}) et b = (b_1 , b_2 , …, b_n , b_{n+1}) sont équivalents si et seulement si il existe un élément $\lambda \neq 0$ dans K tel que :

$$b = \lambda a = (\lambda a_1 , \lambda a_2 , \ldots, \lambda a_n , \lambda a_{n+1}) ;$$

Cette relation R satisfait les propriétés d'une relation d'équivalence : réflexivité, symétrie et transitivité.

Définition 11 :
Le n - espace projectif est l'ensemble des classes :

$$\mathbf{IP^n(K) = /A^{n+1}(K) - \{0\} / R ;} \qquad \mathbf{(2)}$$

Il en résulte que les notions d'ensembles algébriques et de topologie de Zariski valables sur l'espace affine $/A^{n+1}$(K), le sont aussi sur l'espace projectif IP^n(K).

Définition 12 :
(1) Une Variété projective est une partie de l'espace projectif IP^n(K) irréductible et fermée .
(2) Une Variété quasi projective est une partie ouverte d'une Variété projective.
(3) Une sous Variété projective est une partie irréductible et fermée d'une Variété projective.

Exemple :
La Variété projective IP^2(IR) est l'ensemble des classes :cl(r_1 , r_2 , r_3)

$$cl(0,1,0) = \{(0,1,0) , (0,2,0) ,(0,\sqrt{2},0) ,\ldots \}$$

$$cl(1,1,1) = \{(1,1,1) , (5,5,5) ,(-¾ ,-¾ ,-¾) , \ldots\}$$

Signalons que la réunion $Y_1 \cup Y_2$ de deux sous Variétés de la Variété projective IP^n(K) n'est pas une Variété ; la réunion $Y_1 \cup Y_2$ est réductible .

Il en résulte que les polynômes f(x_1, x_2 ,…, x_n , x_{n+1}) d'une Variété projective IP^n(K) sont homogènes de degré d = 0,1,2,…

Le passage des coordonnées affines aux coordonnées projectives s'obtient avec l'application :

$$/A^{n+1}(K) \longrightarrow IP^n(K)$$

$$(x_1,\ldots, x_{n+1}) \longrightarrow \left[\frac{x_1}{x_{n+1}} , \ldots, \frac{x_n}{x_{n+1}} \right] \qquad (tr1)$$

Suivie de l'application multiplication par x^d_{n+1} , où d = degré du polynôme f $\in K[x_1,\ldots, x_n]$.

$$\left[\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right] \longrightarrow x^d_{n+1}\left[\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right] \qquad \text{(tr2)}$$

Exemple de passage du plan affine $/A^2(K)$ au plan projectif $IP^2(K)$:
Soit le polynôme affine :

$$f(x,y) = x^3 - 3xy + 2y^2 - 4y - 7 \in /A^2(K) ;$$

La transformation (tr1) transforme le polynôme f en polynôme :

$$f\left[\frac{x}{z}, \frac{y}{z}\right] = \frac{x^3}{z^3} - \frac{3xy}{z^2} + 2\frac{y^2}{z^2} - 4\frac{y}{z} - 7 ; \in /A^2(K) .$$

Pour d = 3, la multiplication par z^3 transforme le polynôme $f\left[\frac{x}{z}, \frac{y}{z}\right]$ en polynôme homogène de degré 3 :

$$g(x,y,z) = x^3 - 3xyz + 2y^2z - 4yz^2 - 7z^3 ; \in IP^2(K) .$$

Le passage du polynôme homogène g(x,y,z) au polynôme affine s'obtient avec l'application :

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

Une Variété abélienne se construit avec une Variété de groupe abélien.

Définition 13 :
Une Variété abélienne est une Variété projective X muni de 2 applications :

$X \times X \longrightarrow X$, (a,b) $\longrightarrow$ a + b : loi de groupe abélien .

$X \times X \longrightarrow X$, a $\longrightarrow$ a^{-1} : application inverse.

Exemple :
Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 ; \in IP^2(K) .$$

La loi de groupe abélien sur le groupe de Mordell -Weil E(K) :

$f : E(K) \times E(K) \longrightarrow E(K)$ de valeur : $f(P_1, P_2) = P_1 + P_2$.

$$f(O_E) = O_E = \text{point à l'infini .}$$

et $E(K) \longrightarrow E(K)$, $P \longrightarrow -P$

La dimension de cette Variété abélienne est égale à :

$$\dim IP^2(K) - \text{nombre de relations} = 2-1 = 1 .$$

Donc une Courbe Elliptique a une structure de Variété abélienne de dimension un.

5-Diviseurs des courbes algébriques :

Cette notion de diviseurs d'une courbe est développée dans les ouvrages de Géométrie Algébrique.

HARTSHORNE [5] distingue les Diviseurs de Weil sur les courbes algébriques, les Variétés et les Diviseurs de Cartier sur les schémas.

SHAFAREVICH [16] traite les Diviseurs sur les Variétés, sur les schémas et sur les fonctions f Є K[X].

Nous suivons la description de HARTSHORNE [5].

Soit une courbe algébrique E, projective, non singulière dans $IP^2(K)$,de degré d et une famille {L}de lignes de $IP^2(K)$.

L'intersection L ∩C contient d points P_1 , …, P_d , simples ou multiples de multiplicités n_i .

Définition 14 :

Un Diviseur de Weil est un élément du groupe abélien libre Div(X) engendré par les Diviseurs premiers.

Définition 15 :

Un diviseur sur une courbe algébrique E est une somme formelle :

$$\mathbf{D = \sum_i n_i P_i \ , n_i \in Z , n_i \neq 0 \text{ pour } 1 \leq i \leq d .} \qquad \mathbf{(1)}$$

Les entiers $n_i > 0$ correspondent aux zéros de la courbe E , les entiers $n_i < 0$ correspondent aux pôles de E .

Cette somme formelle est liée à la notion de groupe libre.

D'après KOSTRIKINE [9] (chapitre VII) , un groupe libre est un groupe abélien F_d à d générateurs libres f_1 , … , f_d , avec la loi de composition :

$$\sum_i s_i f_i + \sum_i t_i f_i = \sum_i (s_i + t_i) f_i \ , \text{ pour } s_i , t_i \in \mathbb{Z} ;$$

Lorsque la ligne L varie, l'intersection L ∩E varie et les Diviseurs varient.

Nous obtenons une famille de Diviseurs Div(E) ; cet ensemble possède une structure de groupe abélien avec le Diviseur :

$$D = 0 = \sum_i 0.P_i \text{ , comme élément neutre .}$$

La loi : $D + \grave{D} = \sum_i n_i P_i + \sum_i \grave{n}_i P_i = \sum_i (n_i + \grave{n}_i) P_i$,

et le symétrique $-D = \sum_i (-n_i)P_i$. (2)

Exemple :
Diviseurs de la courbe E d'équation :

$$y^2 = f(x) = 4(x-2)^2(x-3)^3(x-4)^{-1}(x-5)^{-4} ;$$

Alors son Diviseur de Weil est égal à :

$D = 2P_1 + 3P_2 - P_3 - 4P_4$,

Avec les points :

$P_1 = (2,0)$ zéro d'ordre 2, $P_2 = (3,0)$ zéro d'ordre 3 , $P_3 = (4,0)$ pôle d'ordre 1 et

$P_4 = (5,0)$ pôle d'ordre 4.

Il y a des Diviseurs particuliers :

Définition 16 :
(1) Un Diviseur effectif est un Diviseur $D = \sum_i n_iP_i$ à coefficients $n_i \geq 0$.
(2) Un Diviseur principal est le Diviseur $(f) = \sum_i n_iP_i$ d'une fonction rationnelle non nulle $f \in K(E)$, les P_i sont les zéros et les pôles de f avec leurs ordres de multiplicités n_i .

Alors pour deux fonctions rationnelles f et g Є K(E) , les Diviseurs principaux associés sont

(f) , (g) et (f / g) = (f) – (g) .

Le groupe Div(X) des Diviseurs d'une courbe E contient un sous groupe particulier :

le sous groupe P(X) des Diviseurs principaux .

Définition 17 :
(1) deux Diviseurs D et Ď du groupe Div(X) sont linéairement équivalents si :
D - Ď est un Diviseur principal.

(2) Le groupe quotient Div(X)/P(X) est le groupe des classes des Diviseurs de X.

$$\mathbf{cl(X) = Div(X)/P(X)} \quad (3)$$

Le degré d'un Diviseur $D = \sum_i n_iP_i$ est l'entier rationnel :

$\deg D = \sum_i n_i$, pour des points P_i .

Le degré d'un Diviseur $D = \sum_i n_i X_i$, où les X_i sont des sous schémas de codimension un , est l'entier rationnel :

$$\deg D = \sum_i n_i \deg X_i .$$

Exemple : HARTSHORNE [5].
Soit une surface quadrique non singulière H d'équation : xy = zu , dans l'espace projectif $IP^3(K)$; alors son groupe de classes de Diviseurs est le groupe infini :

$$cl(H) \cong \mathbb{Z} \oplus \mathbb{Z}$$

Exemplar : SHAFAREVICH[16].
Groupe de classes de Diviseurs particuliers :

(1)$cl(/A^n(K)) \simeq \{0\}$;

(2)$cl(IP^n(K)) \simeq \mathbb{Z}$;

(3)$cl(IP^{n_1} x...x\ IP^{n_l}) \cong IZ^l$;

6-Discriminants – Résultants :
L'équation de Weierstrass d'une cubique irréductible :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in \quad K[x , y] ;$$

peut être singulière ou non singulière .
C'est avec le discriminant Δ(E) de la formule (1) (chap I-3) que nous pouvons le savoir.
Pour cela, nous considérons une équation cubique :

$$y^2 = f(x) \quad \in \quad K[x] ;$$

L'irréductibilité d'un polynôme $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in \mathbb{Q}[X]$ peut être déterminée au moyen du :

Critère d'irréductibilité (Eisenstein) :
Soit un polynôme $f(X) = a_0X^n + \ldots + a_n \in Q[X]$ de degré n et un nombre premier p .
Supposons que p satisfait les congruences :

a_0 non congru à 0 modulo p , $a_1 \equiv a_2 \equiv \ldots \equiv a_n \equiv 0 \bmod p$ et a_n non congru à 0 modulo p^2 .
Alors f(X) est irréductible sur Q.

Preuve : LANG [11-1] :Chapitre V § 7 , KOSTRIKIN [9] : Chapitre V § 3 .
□

Il y a un lien entre le discriminant Δ(E) d'une cubique de Weierstrass E et le discriminant dis(f(x)) d'un polynôme f(x) de la cubique de Weierstrass : $y^2 = f(x)$.
Commençons par le discriminant de f(x).

Définition 18 :
Le discriminant d'un polynôme :
$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n = a_0 (x - t_1)(x - t_2) \dots (x - t_n)$ de degré $n > 1$, est la

fonction symétrique «produit des carrés $(t_i - t_j)^2$ » égale à :

$$\mathbf{dis(f(x)) = a_0^{2n-2} \prod_{1 \le i < j \le n} (t_i - t_j)^2 .} \qquad \mathbf{(1)}$$

KOSTRIKIN [9] page 245 , LANG [11] page 139 .
Avec le calcul nous obtenons les discriminants dis(f) des polynômes cubiques :

(1) Pour $f(X) = X^3 + aX + b$: $dis(f) = - (4a^3 + 27b^2)$; (2)

(2)Pour $f(X) = d_0X^3 + d_1X^2 + d_2X + d_3$:

$$dis(f) = 18d_0d_1d_2d_3 + d_1^2d_2^2 - 4d_0d_2^3 - 4d_1^3d_3 - 27d_0^2d_3^2 ; \qquad (3)$$

(3) Pour $f(X) = 4X^3 + b_2X^2 + 2b_4X + b_6$: $dis(f) = 16(9b_2b_4b_6 - 8 b_4^3 - 27b_6^2 - b_2^2d_8)$; (4)

(4) Pour $f(X) = X^3 - 27c_4X - 54c_6$; $dis(f) = 4 \times 27^3(c_4^3 - c_6^2)$; (5)

En comparant les discriminants $\Delta(E)$ et dis(f), nous obtenons la :

Proposition 1 :
Soit une cubique plane E, irréductible, d'équation de Weierstrass :
$$\mathbf{E : y^2 = f(x).}$$
Les discriminants $\Delta(E)$ de E et dis(f) satisfont les relations :

(1)$dis(f) = 16\,\Delta(E)$ lorsque $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$;

(2) $\Delta(E) = 16\,dis(f)$ lorsque $f(x) = x^3 + AX + B$ et lorsque $f(x) = x^3 + a_2x^2 + a_4x + a_6$;

Preuve :
La formule (3) implique la relation (1).
La formule (2) implique la relation (2).
□

Les zéros de deux polynômes f(x) et g(x) d'un anneau K[x] sont liés par le résultant Res(f,g) de ces deux polynômes.

Définition 19 :
Soient deux polynômes $f(x) = u_0x^n + u_1x^{n-1} + \dots + u_n$, de degré $n > 1$ et

$g(x) = v_0x^p + v_1x^{p-1} + \dots + v_p$,de degré $p > 1$; le résultant de ces deux polynômes est égal

au déterminant d'ordre n+p :

$$\mathbf{Res(f,g)} = \begin{vmatrix} u_0 & u_1 & . & . & . & u_n & 0 & . & . & . \\ 0 & u_0 & u_1 & . & . & . & u_n & 0 & . & . \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & 0 & u_n & . \\ 0 & . & . & . & . & 0 & u_0 & . & . & u_n \\ v_0 & v_1 & . & . & . & v_p & 0 & . & . & 0 \\ 0 & v_0 & v_1 & . & . & . & v_p & . & . & 0 \\ . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & . & v_0 & v_1 & . & v_p \end{vmatrix}$$

formé de p lignes ($u_0, \ldots, u_n$) et n lignes ($v_0, \ldots, v_n$) , les termes manquants sont remplacés par des zéros.
La diagonale principale est formée de p termes u_0 et n termes v_p.

Les résultants possèdent de nombreuses propriétés que l'on peut trouver dans (LANG -1)[11] et (KOSTRIKIN)[9] .

Proposition 2 :
Le résultant Res(f,g) de deux polynômes est nul si et seulement si f et g ont un zéro commun.
□

Le résultant est une fonction des zéros des deux polynômes.

Proposition 3 :
Soit deux polynômes :

$$f(x) = u_0(x-\theta_1)(x-\theta_2)\ldots(x-\theta_n) \text{ de degré } n > 1 \text{ , et}$$

$$g(x) = v_0(x-\lambda_1)(x-\lambda_2)\ldots(x-\lambda_p) \text{ de degré } p > 1 \text{ .}$$

Alors leur résultant est égal à :

$$\mathbf{Res(f,g)} = u_0^p v_0^n \prod_{1\le i\le n} \prod_{j=1}^{p} (\theta_i - \lambda_j) \qquad \mathbf{(6)}$$

$$= u_0^p \prod_{1\le i\le n} g(\theta_i) = (-1)^{np} v_0^n \prod_{1\le j\le p} f(\lambda_j) .$$

□

Le discriminant dis(f) est lié au résultant Res(f , f ') de f(x) et sa dérivée f ' (x) par la :

Proposition 4 :
Soit un polynôme $f(x) = u_0(x - \theta_1)(x - \theta_2) \dots (x - \theta_n)$ de degré $n > 1$, sa dérivée $f'(x)$.
Alors le discriminant dis(f) et le résultant $Res(f , f')$ satisfont les relations :

$$Res(f , f') = (-1)^{n(n-1)/2} u_0 dis(f)$$
$$= u_0^{n-1} \prod_{1 \le i \le n} f'(\theta_i) \qquad (7)$$

□

Corollaire:
Soit les hypothèses de la proposition 4 .

Alors : $$Res(f , f') = u_0^{2n-1} \prod_{1 \le i \le n} \prod_{j \neq i} (\theta_i - \theta_j) \qquad (8)$$

□

7- Classification des cubiques irréductibles par leurs discriminants :
Soint une cubique plane E , algébrique , irréductible , d'équation de Weierstrass :

$$E : y^2 = f(x) \in K[x] ;$$

Le résultant $Res(f , f')$ est nul lorsque f(x) admet 2 racines égales ; (proposition 2) , il en résulte que la cubique E est singulière , son discriminant $\Delta(E)$ est nul ; (proposition 4).
Cela implique une classification des cubiques irréductibles par leurs discriminants :

Proposition 5 :
Soit une cubique algébrique plane E , irréductible , d'équation de Weierstrass :

$$E : y^2 = f(x) \in K[x] ;$$

de discriminant $\Delta(E)$:
1) **La cubique E est une Courbe Elliptique si et seulement si $\Delta(E) \neq 0$.**
2) **La cubique E est singulière si et seulment si $\Delta(E) = 0$.**

Preuve de "E est une Courbe Elliptique" implique "$\Delta(E) \neq 0$"
Prenons une équation de Weierstrass de la forme :

$$E : y^2 = f(x) \in K[x] ; \qquad (1)$$

Par définition, une Courbe Elliptique est une cubique non singulière, donc elle coupe l'axe Ox en trois points simples :

$$P_i = (e_i , 0) ; e_i \neq e_j ; i = 1,2 ,3 . \qquad (2)$$

(1) et (2) impliquent le polynôme f(x) :

$$f(x) = (x- e_1)(x- e_2)(x- e_3). \quad (3)$$

Le corollaire de la proposition 4 implique: le résultant $Res(f, f') \neq 0$; (4)

La proposition (4) implique le discriminant :

$$\Delta(E) \neq 0 ; \quad (5)$$

Preuve de"Δ(E) ≠ 0" implique"la cubique E est une Courbe Elliptique"

La relation $\Delta(E) = 16\, dis(f)$ et l'hypothèse $\Delta(E) \neq 0$ impliquent :

$$dis(f) \neq 0 ; \quad (6)$$

La relation (6) et la proposition 4 impliquent la valeur du résultant $Res(f, f') \neq 0$;

La proposition 2 implique que les polynômes f (x) et f' (x) n'ont pas de zéro commun.

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

Il en résulte que la cubique E est non singulière, donc elle est Elliptique.

Preuve de" la cubique E est singulière" implique "$\Delta(E) = 0$"

L'hypothèse "E est singulière" implique f (x) admet un zéro multiple, (7)

D'après la théorie des discriminants des polynômes :

dis(f) = 0 si et seulement si f a une racine multiple . (8)

(7) et (8) impliquent : dis (f) = 0 ; (9)

Les relations $\Delta(E) = 16\, dis(f)$ et (4) impliquent la valeur :

$$\Delta(E) = 0 ; \quad (10)$$

□

Une cubique irréductible E, singulière, admet 2 types de point singulier :
Un nœud, où la cubique admet deux tangentes distinctes.
Un point de rebroussement, où la cubique admet deux tangentes confondues.

Proposition 6 :

Soit une cubique de Weierstrass E, son discriminant $\Delta(E)$ et son invariant usuel $c_4(E) = c_4$.

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

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

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

Soit une cubique E qui admet un nœud, donc cette cubique E est singulière. D'après la proposition 5 son discriminant est nul :

$$\Delta(E) = 0 ; \qquad (1)$$

L'hypothèse d'un nœud S sur la cubique E implique que la cubique admet deux tangentes distinctes en S. (2)

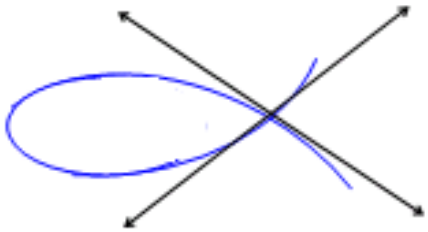

Figure1 :un nœud.

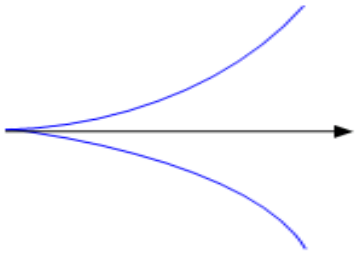

Figure2 : un point de rebroussement.

La pente d'une tangente est égale à la dérivée y' de y .

Prenons une équation de Weierstrass :

$$E : y^2 = x^3 - 27c_4x - 54c_6 \quad \in \quad K [x , y] ; \qquad (3)$$

La dérivée de y est égale à :

$$y' = \frac{3x^2 - 27c_4}{2y} = \frac{3(x^2 - 9c_4)}{2y} = \frac{3N(x)}{2y} ; \qquad (4)$$

Les tangentes au nœud S sont distinctes, cela implique que le polynôme $N(x) = x^2 - 9c_4$ admet deux zéro simples.

Donc $c_4 \neq 0$ sur un corps K de carac(K) $\neq 3$. (5)

Preuve de" la cubique E admet un point de rebroussement " implique" $\Delta(E) = 0$ et $c_4 = 0$ ".

Soit une cubique E qui admet un point de rebroussement, cela implique que la cubique est singulière, donc$\Delta(E) = 0$.

L'hypothèse d'un point de rebroussement S sur E implique 2 tangentes confondues à la cubique en S.

Cela implique que N(x) admet un zéro double, il en résulte que $c_4 = 0$.

□

Les Courbes Elliptiques sont classifiées en deux classes par leurs discriminants :
Classe des Courbes Elliptiques qui coupent l'axe Ox en trois points simples.
Classe des Courbes Elliptiques qui coupent l'axe Ox en un seul point, qui est simple.

Proposition 7 :
Soit une Courbe Elliptique E et son discriminant $\Delta(E)$.
1) E coupe l'axe Ox en trois points simples si et seulement si $\Delta(E) > 0$.
2) **E coupe l'axe Ox en un seul point, qui est simple, si et seulement si $\Delta(E) < 0$.**

Preuve de "E coupe l'axe Ox en trois points simples" implique "$\Delta(E) > 0$".
Nous choisissons une équation de Weierstrass :

$$E : y^2 = (x-e_1)(x-e_2)(x-e_3) = f(x) \in IR[x] , e_i \neq e_j . \quad (1)$$

Par définition, le discriminant de f(x) est égal à :

$$dis(f) = (e_1- e_2)^2 (e_1- e_3)^2(e_2 - e_3)^2 ; \quad (2)$$

Les trois zéros e_1,e_2 ,e_2 sont des nombres réels , les carrés $(e_i-e_j)^2$ sont positifs . (3)
Il en résulte :

$$dis(f) > 0 ; \quad (4)$$

la formule (4) et la relation entre les discriminants de f et de E impliquent :

$$\Delta(E) > 0 ; \quad (5)$$

Preuve de"$\Delta(E) > 0$" implique" la Courbe Elliptique E coupe l'axe Ox en trois points simples."

Soit une Courbe Elliptique d'équation de Weierstrass :

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 = f(x) \in IR[x] . \quad (6)$$

La relation $dis(f(x)) = 16\Delta(E)$ et l'hypothèse $\Delta(E) > 0$ impliquent :

$$dis(f(x)) > 0 ; \quad (7)$$

(6) et (7) impliquent que le polynôme f(x) admet trois racines simples : e_1, e_2, e_2 .

Il en résulte trois points d'intersection $P_i = (e_i ,0)$ de la Courbe E avec l'axe Ox .

Preuve de "E coupe l'axe Ox en un seul point simple" implique "$\Delta(E) < 0$."
Considérons une Courbe Elliptique qui coupe l'axe Ox en un seul point simple P = (e ,0) .
Cela implique l'équation de Weierstrass :

$$y^2 = (x - e)g(x) = f(x) \in IR[x] . \quad (8)$$

Les deux racines e_1 et e_2 du polynôme g(x) sont conjuguées complexes.

$e_1 = r + is$, $e_2 = r - is$, r et s réels . (9)

Le discriminant du polynôme f(x) est égal à :

$$dis(f) = ((e-e_1)(e-e_2)(e_1-e_2))^2 ; \quad (10)$$

Avec le calcul nous obtenons la valeur :

$$dis(f) = -4s^2((e-r)^2 + s^2) ; \quad (11)$$

Les carrés des nombres réels sont positifs, il en résulte :

$$dis(f) < 0 ; \quad (12)$$

La relation entre dis(f) et $\Delta(E)$ implique :

$$\Delta(E) < 0 ; \quad (13)$$

Preuve de "$\Delta(E) < 0$ " implique " la Courbe Elliptique E coupe l'axe Ox en un seul point simple."
Un polynôme cubique admet trois racines e_i , simples ou multiples :

$$E : y^2 = 4(x-e_1)(x-e_2)(x-e_3) = f(x) \in IR[x] ; \quad (14)$$

La relation entre dis(f(x)) et $\Delta(E)$ et l'hypothèse $\Delta(E) < 0$ impliquent : $dis(f(x)) < 0$. (15)

Par définition dis(f) est lié aux racines e_i par :

$$dis(f) = 4^4(e_1- e_2)^2 (e_1- e_3)^2(e_2 - e_3)^2 \in IR ; \quad (16)$$

les relations (14) et (15) impliquent un carré négatif .

cela implique $e_1 = e$ réel , $e_2 = r + it$ et $e_3 = r - it$;

Alors $dis(f) = (e - r - it)^2 (e - r + it)^2 (2it)^2$

$= -4t^2[(e - r)^2 + t^2]^2 < 0$;

Il en résulte un point d'intersection $P_1 = (e_1,0)$ de la Courbe E avec l'axe Ox .
□

Les résultats précédents sont rassemblés dans la :

Proposition 8 : **(classification des cubiques de Weierstrass).**
Soit une cubique E de Weierstrass, son discriminant $\Delta(E)$, son invariant usuel c_4 et son équation :

$$\mathbf{E : y^2 = f(x) \in IR[x] ;}$$

L'ensemble de ces cubiques se répartit en quatre classes selon les valeurs $\Delta(E)$ et c_4 :
1) La classe des cubiques singulières qui ont un nœud, lorsque $\Delta(E) = 0$ et $c_4 \neq 0$.
2) La classe des cubiques singulières qui ont un point de rebroussement, lorsque $\Delta(E) = 0$ et $c_4 = 0$.
3) La classe des Courbes Elliptiques E qui coupent l'axe Ox en trois points simples, lorsque $\Delta(E) > 0$.
4) La classe des Courbes Elliptiques E qui coupent l'axe Ox en un seul point, qui est simple, lorsque $\Delta(E) < 0$.
□

Exemple 1 : cubique singulière ayant un nœud :
Soit la cubique E_1 d'équation de Weierstrass :

$$E_1 : y^2 = x^3 - 5x^2 + 3x + 9 ; \qquad (1)$$

Nous obtenons avec le calcul les invariants de E_1:

$$b_2 = -20 , b_4 = 6 , b_6 = 36 , b_8 = -189 , c_4(E_1) = 256 \neq 0 , \Delta(E_1) = 0 . \qquad (2)$$

$\Delta(E_1) = 0$ implique que la cubique E_1est singulière .

Cette cubique E_1 a un point singulier.

Le coefficient $c_4 \neq 0$ implique que ce point est un nœud.

Les coordonnées de ce nœud sont les solutions du système de trois équations algébriques :

$$f(x,y) = y^2 - x^3 + 5x^2 - 3x - 9 = 0 ;$$

$$\frac{df}{dx}(x,y) = -3x^2 + 10x - 3 = 0 ; \qquad (3)$$

$$\frac{df}{dy}(x,y) = 2y = 0 ;$$

Nous obtenons la solution (3,0).

Pour trouver les abscisses entières, nous utilisons le :

Théorème :
Soit une équation diophantienne :

$$\mathbf{f(x) = x^n + r_1 x^{n-1} + \ldots + r_n = 0 ; f(x) \in IZ[x] ;}$$

Toute solution de f(x) est un diviseur du coefficient r_n .

Ici $r_n = 9$, le test des diviseurs de 9 implique $f(-1) = 0 = f(3)$.

Donc $f(x)$ admet 2 racines : $x_1 = -1$ et $x_2 = 3$.

Il en résulte la factorisation de :

$$y^2 = x^3 - 5x^2 + 3x + 9 = (x-3)(x-3)(x+1) ;$$

$$= (x-3)^2(x+1) ; \qquad (4)$$

La relation (4) implique la condition $x \geq -1$.

Tableau des coordonnées de quelques points de la cubique E_1 :

x	-1	$-\frac{1}{2}$	**0**	**1**	**2**	**3**	**4**	**5**
y	**0**	$\pm\frac{7\sqrt{2}}{4}$	± 3	$\pm 2\sqrt{2}$	$\pm\sqrt{3}$	**0**	$\pm\sqrt{5}$	$\pm 2\sqrt{6}$

La cubique E_1 coupe l'axe Ox en un seul point simple (-1,0) et un point double (3,0) qui est le nœud.

Figure 3 (courbe tracée avec le logiciel Scientific Note book 5.0)

Exemple 2 : cubique singulière ayant un point de rebroussement.
Soit la cubique E_2 d'équation de Weierstrass :

$$E_2 : y^2 + 2xy = x^3 + 2x^2 + 3x + 1 ; \qquad (1)$$

Nous obtenons avec le calcul les invariants de E_2 :

$$b_2 = 12 , b_4 = 6 , b_6 = 4 , b_8 = 3 , c_4(E_2) = 0 , \Delta(E_2) = 0 . \quad (2)$$

$\Delta(E_2) = 0$ implique que la cubique plane E_2 n'est pas une Courbe Elliptique .

Cette cubique E_2 a un point singulière.

Le coefficient $c_4 = 0$ implique que ce point singulier est un point de rebroussement.

Les coordonnées de ce point de rebroussement sont les solutions du système de trois équations algébriques :

$$f(x,y) = y^2 + 2xy - x^3 - 2x^2 - 3x - 1 = 0 ;$$

$$\frac{df}{dx}(x,y) = 2y - 3x^2 - 4x - 3 = 0 ; \quad (3)$$

$$\frac{df}{dy}(x,y) = 2y + 2x = 0 ;$$

Nous obtenons la solution (-1,1).

Tableau des coordonnées de quelques points de la courbe E_2 :

x	-2	-1	$-\frac{1}{2}$	0	$\frac{1}{2}$	1
y	Pas de racines y réelles.	1 racine double.	$\frac{1}{2} \pm \frac{\sqrt{2}}{4}$	± 1	$-\frac{1}{2} \pm \frac{3\sqrt{6}}{4}$	$-1 \pm 2\sqrt{2}$

La cubique E_2 coupe l'axe Oy en deux points d'ordonnées $y_1 = -1$ et $y_2 = 1$.

Figure 4 (courbe tracée avec le logiciel Scientific Note book 5.0)

Exemple 3 : Courbe Elliptique qui coupe l'axe Ox en trois points simples.
Soit la cubique E_3 d'équation de Weierstrass :

$$E_3 : y^2 + xy - 5y = x^3 + 5x^2 + 2x - 8 ; \quad (1)$$

Nous obtenons avec le calcul les invariants de E_3 :

$$b_2 = 21 , b_4 = -1 , b_6 = -7 , b_8 = -37 , \Delta(E_3) = 16325 > 0 . \quad (2)$$

$\Delta(E_3) > 0$ implique que la cubique E_3 est une Courbe Elliptique qui coupe l'axe Ox en trois points simples . .
Avec logiciel Scientific Note book 5.0 je trouve les abscisses x_1 , x_2 et x_3 de ces points :

$$x_1 = -4 , x_2 = -2 \text{ et } x_3 = 1 ; \quad (3)$$

Tableau des coordonnées de quelques points de la courbe E_3 :

x	**-5**	**-4**	**-3**	**-2**	**0**	**1**	**3**	**6**
y	$5 \pm \sqrt{7}$	**0 et 9**	$4 \pm 2\sqrt{5}$	**0 et 7**	**Pas de racines réelles.**	**0 et 4**	$1 \pm \sqrt{71}$	$-\frac{1}{2} \pm \frac{\sqrt{1601}}{2}$

La Courbe Elliptique E_3 coupe l'axe Ox en trois points simples :

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

Figure 5 (courbe tracée avec le logiciel Scientific Note book 5.0)

Exemple 4 : Courbe Elliptique qui coupe l'axe Ox en un seul point simple.
Soit la cubique E_4 d'équation de Weierstrass :

$$E_4 : y^2 + 6y = x^3 + 4x^2 + 3x + 12 ; \quad (1)$$

Nous obtenons avec le calcul les invariants de E_4 :

$$b_2 = 16 , b_4 = 6 , b_6 = 84 , b_8 = 327 , \Delta(E_4) = -203376 < 0 . \quad (2)$$

Donc la cubique E_4 est une Courbe Elliptique, qui coupe l'axe Ox en un seul point simple.
Avec logiciel Scientific Note book j'obtiens l'abscisse x_4 de ce point :

$$x_4 = -4 . \quad (3)$$

Tableau des coordonnées de quelques points de la courbe E_4 :

x	-5	-4	-3	-2	0	2	5	8
y	**Pas de racines réelles.**	**0 et -6**	$-3 \pm \sqrt{21}$	$-3 \pm \sqrt{23}$	$-3 \pm \sqrt{21}$	$-3 \pm \sqrt{51}$	$-3 \pm 3\sqrt{29}$	$-3 \pm \sqrt{813}$

Ce tableau implique 3 points d'abscisses x = -3, -1 et 0 sur la même droite y $= -3 \pm \sqrt{21}$ parallèle à Ox.
La Courbe Elliptique E_4 coupe l'axe Ox en un seul point (-4,0) simple.

Figure 6 (courbe tracée avec le logiciel Scientific Note book 5.0)

CHAPITRE II
GROUPE DE MORDELL-WEIL DES COURBES ELLIPTIQUES.

Une loi de groupe sur une Courbe Elliptique peut être déterminée par la théorie des diviseurs sur une Variété abélienne.

Cette loi peut être aussi déterminée par une propriété géométrique « de trois points colinéaires d'une Courbe Elliptique » ; c'est cette loi que nous choisissons d'exposer et d'utiliser.

1 – Structure de groupe abélien sur l'ensemble E(K) des points K- rationnels d'une Courbe Elliptique E :

Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in \quad K [x , y] ; \qquad (1)$$

Pour obtenir une structure de groupe abélien, nous considérons :

1) L'ensemble E(K) des points K- rationnels de la Courbe Elliptique E .
2) Le point à l'infini O_E qui joue le rôle d'élément neutre ;

$O_E = (\infty,\infty)$ dans le plan affine $/A^2(K)$, et (0,1,0) dans le plan projectif $IP^2(K)$.

Ce point est unique.
Il est déterminé par la direction de l'axe Oy dans le plan projectif $IP^2(IR)$.

3) une loi de composition interne :

$$h : E(K) \times E(K) \longrightarrow E(K)$$

$$\text{de valeur : } \quad h(P_1 ,P_2) = P_1 + P_2 \qquad (2)$$

« Trois points colinéaires de la courbe E ont une somme nulle. »

$$P_1 + P_2 + P_3 = O_E \ . \qquad (3)$$

La somme $M = P_1 + P_2$ est obtenue par une construction géométrique :
M est le symétrique par rapport à l'axe Ox du troisième point d'intersection P_3 de E par la sécante P_1P_2.
Cette construction est représentée dans la figure 1 :

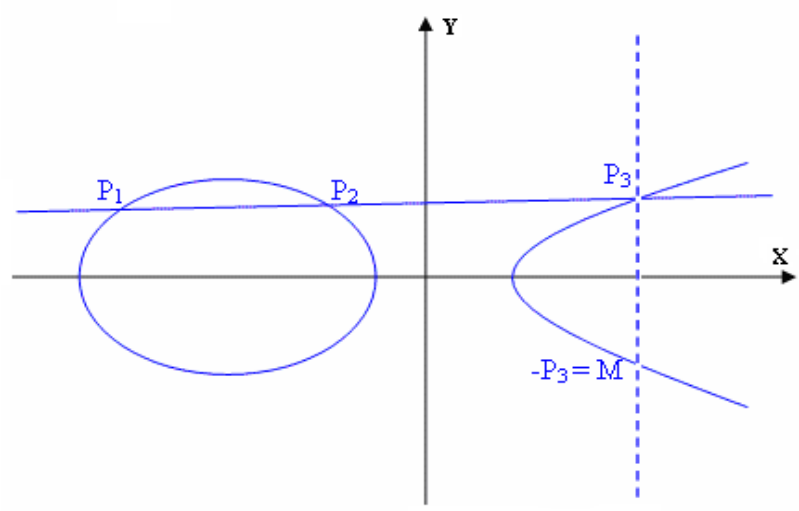

Figure 1.

Vérifions les 4 axiomes d'un groupe abélien :

Axiome de l'élément neutre O_E :
Le point O_E à l'infini joue le rôle d'élément neutre ; il est déterminé par la direction de l'axe Oy .
Pour tout point P de E(K) , la sécante PO_E est parallèle à l'axe Oy .
La règle des 3 points colinéaires implique

$$P + O_E = P = O_E + P \ . \qquad (4)$$

L'axiome de l'élément neutre est vérifié .

Axiome du symétrique :
Soit un point P de l'ensemble E(K) ;
la parallèle à l'axe Oy passant par le point P coupe la courbe E en trois points P , P` , O_E ;
il en résulte la relation :

$$P + P` + O_E = O_E \ ; \qquad (5)$$

Il en résulte le symétrique de P :

$$P` = -P \ ; \qquad (6)$$

Cette construction du symétrique d'un point P de la courbe E est représentée dans la figure 2 :

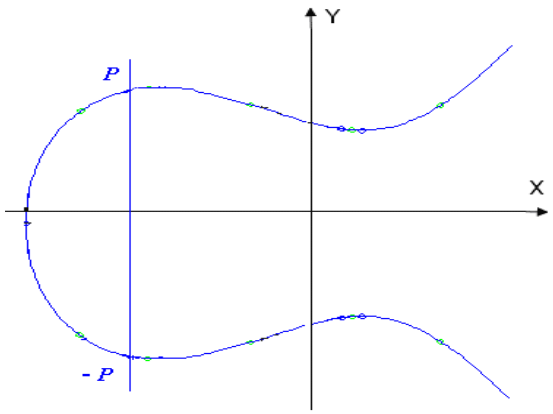

Figure 2.

Axiome de commutativité :
Les sécantes P_1P_2 et P_2P_1 sont confondues ; il en résulte la relation :

$$P_1 + P_2 + P_3 = P_2 + P_1 + P_3 = O_E \ ; \qquad (7)$$

Cela implique la relation :

$$P_1 + P_2 = P_2 + P_1 = - P_3 \ ; \qquad (8)$$

Axiome d'associativité :
Soient3 points P , Q , R non colinéaires de la Courbe Elliptique E .
Pour vérifier l'axiome d'associativité, il n'y a pas de construction géométrique utilisable.

Il faut comparer les points :

$$(P + Q) + R \text{ et } P + (Q + R)$$

Il faut donc calculer les coordonnées des sommes :

$$P + Q = A \ , \ A + R = B \ , \ Q + R = C \text{ et } P + C = D \ ;$$

Avec le calcul nous obtenons l'égalité B = D et l'associativité de la loi :

$$(P + Q) + R \ = \ P + (Q + R) \ ;$$

Nous avons démontré la :

Proposition 1 :
L'ensemble E(K) des points rationnels d'une Courbe Elliptique E , muni de la loi de composition déterminée par la règle géométrique de trois points colinéaires de la courbe E , est un groupe abélien , additif , d'élément neutre le point à l'infini $O_E = (\infty,\infty)$.
□

Définition 1 :
Le groupe abélien E(K) est le groupe de Mordell–Weil de la Courbe Elliptique E .

2- Formules du symétrique –P , de la somme $P_1 + P_2$ et de la somme P + P = 2P dans le groupe E(K) :

Proposition 2 :
Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad \in \quad K [x , y] ;$$

1) le symétrique d'un point $P = (x_P , y_P)$ de E est le point $-P = (x_P, - y_P - a_1x_P - a_3)$;

2) la somme $P_1 + P_2 = M$ de deux points $P_1 \neq \pm P_2$ de la courbe E , est le point M de coordonnées :

$$X_M = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2 ;$$

$$Y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_2 - a_1^2 + 2x_1 + x_2) + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1 ;$$

avec la pente $\lambda = \dfrac{y_1 - y_2}{x_1 - x_2}$;

Preuve :

1) Soit un point $P = (x_P , y_P)$ sur une Courbe Elliptique E .
Nous considérons la parallèle à l'axe Oy passant par P.
Cette sécante a pour équation :

$$x = x_P ; \qquad (1)$$

La parallèle coupe la courbe E en deux points P et –P d'ordonnées qui sont les solutions de l'équation en y, qui est quadratique .

$$y^2 + a_1x_Py + a_3y = x_P^3 + a_2 x_P^2 + a_4 x_P + a_6 \quad ; \qquad (2)$$

La somme des racines d'un polynôme est une fonction symétrique élémentaire.

$$y(-P) + y_P = - a_1x_p - a_3 ; \qquad (3)$$

Il en résulte les coordonnées du symétrique –P du point $P = (x_P , y_P)$:

$$-P = (x_P, - y_P - a_1x_P - a_3) ; \qquad (4)$$

2) La règle géométrique de trois points colinéaires implique la relation :

$$P_1 + P_2 + P_3 = O_E \ ; \qquad (5)$$

Cette relation implique la somme :

$$P_1 + P_2 = - P_3 \ ; \qquad (6)$$

L'équation de la sécante P_1P_2 est :

$$y = \lambda(x-x_1) + y_1 ; \qquad (7)$$

avec la pente $\lambda = \dfrac{y_1 - y_2}{x_1 - x_2}$; (8)

La sécante P_1P_2 coupe la Courbe Elliptique E en trois points simples P_1 , P_2 et P_3 d'abscisses x_1, x_2 et x_3 .
Ces trois abscisses sont les racines de l'équation algébrique en x de degré 3 obtenue avec (7)

$$[\lambda(x-x_1) + y_1]^2 + [\lambda(x-x_1) + y_1][\, a_1x + a_3\,] = x^3 + a_2x^2 + a_4x + a_6 \quad ; \quad (9)$$

La fonction symétrique «somme des racines d'un polynôme » implique la relation :

$$x_1 + x_2 + x_3 = -(\, a_2 - \lambda^2 - a_1\lambda) ; \qquad (10)$$

(10) implique : $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$ et $y = \lambda(x_3 - x_1) + y_1$; (11)

Donc : $y_3 = \lambda^3 + a_1\lambda^2 - (\, x_1 + x_2 + a_2\,)\lambda + \alpha$; (12)

Avec les formules du symétrique du point P_3 , nous obtenons le point :

$$-P_3 = P_1 + P_2 = M ; \qquad (13)$$

de coordonnées : $x_M = \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2$;

$$y_M = -\lambda^3 - 2a_1\lambda^2 + \lambda(a_2 - a_1^2 + 2x_1 + x_2) + a_1a_2 - a_3 + a_1(x_1 + x_2) - y_1 ; \qquad (14)$$

avec la pente $\lambda = \dfrac{y_1 - y_2}{x_1 - x_2}$

□

Proposition 3 :
Soit une Courbe Elliptique E d'équation de Weierstrass :

$$\mathbf{E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \;\; Є \;\; K\,[\, x\,,\, y\,]\,;}$$

Soit un point $P = (x_P, y_P)$ de E .
Alors les coordonnées du point $P + P = 2P = (x_{2P}, y_{2P})$ sont égales à :

$$\mathbf{x_{2P} = y_P'^2 + a_1y_P' - a_2 - 2x_P} \qquad \mathbf{et} \qquad \mathbf{y'_P = \frac{}{2y_P + a_1x_P + a_3}} \;\; ;$$

$$\mathbf{y_{2P} = -\,y_P'^3 - 2a_1y_P'^2 + y_P'(a_2 - a_1^2 + 3x_P) + a_1a_2 - a_3 + 2a_1x_P - y_P} \;\; ;$$

Preuve :
Soit un point $P = (x_P , y_P)$ de la Courbe Elliptique E.
La tangente à cette Courbe Elliptique au point P a pour équation :

$$y = y_P' (x - x_P) + y_P \; ; \qquad (15)$$

où y_P' est la pente de la tangente à la Courbe Elliptique E au point $P = (x_P , y_P)$:

$$y_P' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y}{2y_P + a_1x_P + a_3} \; ;$$

Cette tangente coupe la courbe E en un point double $P = (x_P , y_P)$ et en un point simple $M = (x_M , y_M)$.

La règle géométrique de trois points colinéaires des Courbes Elliptiques implique la relation :

$$2P + M = O_E \text{ et } 2P = - M \; ; \qquad (16)$$

Les abscisses de ces trois points sont les racines de l'équation cubique en x :

$$[y_P + y_P' (x - x_P)]^2 + a_1x [y_P' (x - x_P) + y_P] = x^3 + a_2x^2 + a_4x + a_6 \; ; \qquad (17)$$

La fonction symétrique élémentaire somme des racines de l'équation (17) implique la relation :

$$2x_P + x_M = y_P'^{\,2} + a_1 y_P' - a_2 \; ; \qquad (18)$$

La relation (18) implique l'abscisse du point M :

$$x_M = y_P'^{\,2} + a_1y_P' - a_2 - 2x_P \; ; \qquad (19)$$

(16) , (19) et la formule du symétrique d'un point impliquent les coordonnées du point 2P :

$$x_{2P} = y_P'^{\,2} + a_1 y_P' - a_2 - 2x_P \text{ et } \quad y_P' = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y}{2y_P + a_1x_P + a_3} \; ;$$

$$y_{2P} = - y_P'^{\,3} - 2a_1 y_P'^{\,2} + y_P' (a_2 - a_1^2 + 3x_P) + a_1a_2 - a_3 + 2a_1x_P - y_P \; ; \qquad (20)$$

□

Exemple 1 :

Soit la Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 - xy + y = x^3 + 2x^2 - x - 2 \quad \in Q [x , y] ;$$

Le groupe de Mordell-Weil E(Q) contient les deux points M = (-2,-3) et R = (-1,-2) .
Calcul des coordonnées des points M + R , -M , -R , 2M , 2R :
Nous obtenons les résultats suivants :

M + R = (1,0) , -M = (-2,0) , -R = (-1,0) , 2M = (2,4) , 2R = (2,-3) .

Figure 3(courbe tracée avec le logiciel Scientific Note book 5.0)

Avec les propositions 2 et 3 , nous pouvons calculer les coordonnées de tout point mP , m > 2 .
Ainsi 3P = 2P + P , 4P = 2(2P) , 5P = 4P + P , etc …

Les coordonnées de ces points sont des fractions rationnelles du corps $K(x , y , a_1 , \dots , a_6)$.

3-Formules de Cassels des coordonnées des points mP , m > 2 :

Cassels a obtenu les formules des coordonnées de points mP en prenant une Courbe Elliptique d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B \in \mathbb{Z}[x , y , A , B] ; \text{ avec } 4A^3 + 27B^2 \neq 0 .$$

Soit un point P du groupe E(Q) de Mordell-Weil de E .
Posons :

$$mP = \begin{cases} P + P + \ldots + P ; & m \text{ fois } P \quad \text{si } m > 0 . \\ (-P) + (-P) + \ldots + (-P) ; & (-m) \text{ fois } (-P) \quad \text{si } m < 0 . \\ O_E ; & \text{si } m = 0 . \end{cases} \qquad (1)$$

Selon Cassels les points mP ont pour coordonnées :

$$x(mP) = \frac{\Phi_m(P)}{\Psi_m^2(P)} ; \quad \text{et} \quad y(mP) = \frac{\omega_m(P)}{\Psi_m^3(P)} ; \qquad (2)$$

Les polynômes Ψ_m sont égaux à :

$$\Psi_{-1} = -1 , \Psi_0 = 0 ; \Psi_1 = 1 , \Psi_2 = 2y ;$$
$$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 ; \qquad (3)$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2) ;$$

Les polynômes Ψ_m , sont déterminés par des relations de récurrence :

$$\Psi_{2m+1} = \Psi_{m+2} \Psi_m^3 - \Psi_{m-1} \Psi_{m+1}^3 \quad ; \ m \geq 2$$
$$2y \Psi_{2m} = \Psi_m (\Psi_{m+2} \Psi_{m-1}^2 - \Psi_{m-2} \Psi_{m+1}^2) \quad ; m \geq 3 \qquad (4)$$

Les polynômes Φ_m et ω_m sont déterminés par les formules :

$$\Phi_m = x \Psi_m^2 - \Psi_{m+1} \Psi_{m-1} ; \quad m \geq 2$$
$$4y\omega_m = \Psi_{m+2} \Psi_{m-1}^2 - \Psi_{m-2} \Psi_{m+1}^2 ; m > 2 \qquad (5)$$

Proposition 4 :
Soit un point P = (x,y) du groupe de Mordell-Weil E(Q) d'une Courbe Elliptique E d'équation de Weierstrass :

$$y^2 = x^3 + Ax + B \in Q[x , y] \text{ ; avec } 4A^3 + 27B^2 \neq 0 \text{ et } A , B \in Z .$$

Alors un point mP = (x_m , y_m) a des coordonnées égales à :

$$x(mP) = \frac{\Phi_m(P)}{(\Psi_m(P))^2} \text{ ; et } y(mP) = \frac{\omega_m(P)}{(\Psi_m(P))^3} \text{ ;}$$

Les numérateurs et les dénominateurs Φ_m ,Ψ_m et ω_m sont des polynômes de l'anneau $\mathbb{Z}[A ,B,x,y]$.
Les polynômes Φ_m ,Ψ_m et ω_m satisfont les relations :

$\Psi_{-1} = -1 , \Psi_0 = 0 , \Psi_1 = 1 , \Psi_2 = 2y$;

$\Psi_3 = 3x^4 + 6Ax^2 + 12Bx – A^2$;

$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 – 4ABx – A^3 - 8B^2)$;

$\Psi_{2m+1} = \Psi_{m+2} \Psi_m^3 - \Psi_{m-1} \Psi_{m+1}^3$; $m \geq 2$

$2y \Psi_{2m} = \Psi_m (\Psi_{m+2} \Psi_{m-1}^2 - \Psi_{m-2} \Psi_{m+1}^2)$; $m \geq 3$

$\Phi_m = x \Psi_m^2 - \Psi_{m+1} \Psi_{m-1}$; $m \geq 2$

$4y\omega_m = \Psi_{m+2} \Psi_{m-1}^2 - \Psi_{m-2} \Psi_{m+1}^2$; $m > 2$

Preuve :
C'est le lemme 7-2 dans « Diophantine Equations with Special References to Elliptic Curves » de Cassels [3].

pour m = 0 , $0P = O_E = (\infty,\infty) = [\frac{\Phi_0}{\Psi_0^2} , \frac{\omega_0}{\Psi_0^3}]$; cela implique $\Psi_0 = 0$, $\Phi_0 = \omega_0 = 1$.

Pour m = -1 , -P est le symétrique du point P ; il en résulte $\Psi_{-1} = -1$.
Les formules se démontrent par récurrence sur l'entier naturel m .
□

En appliquant ces formules pour m = 2 , nous obtenons les polynômes :

$\Psi_2 = 2y$; $\Phi_2 = x^4 - 2Ax^2 – 8Bx + A^2$; (6)

$\omega_2 = x^6 + 5Ax^4 + 20Bx^3 - 5A^2 x^2 - 4ABx - A^3 - 8B^2$;

Les coordonnées du point 2P sont donc égales à :

$$x_{2P} = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{(2y)^2} \; ;$$

$$y_{2P} = \frac{x^6 + 5Ax^4 + 20Bx^3 - 5A^2 x^2 - 4ABx - A^3 - 8B^2}{(2y)^3} \; ; \qquad (7)$$

Pour m = 3 , nous obtenons les polynômes :

$\Phi_3 = x^9 - 12Ax^7 - 96Bx^6 + 30A^2x^5 - 24ABx^4 + 12(3A^3 + 4B^2)x^3 + 48A^2Bx^2 +$

$3A(3A^3 + 32B^2)x + 8B(A^3 + 8B^2)$; (8)

C'est un polynôme de l'anneau Z[x,A,B] de degré 9 en x .

$\omega_3 = y[x^{12} + 22Ax^{10} + 220Bx^9 - 165A^2x^8 - 528ABx^7 - 4(23A^3 + 444B^2)x^6 + 264A^2Bx^5 -$

$5A(37A^3 + 576B^2)x^4 - 80B(4B^2 + A^3)x^3 - 6A^2(15A^3 + 104B^2)x^2 - 28AB(3A^3 + 32B^2)x -$

$3A^6 - 96A^3B^2 - 512B^4]$; (9)

donc $\frac{\omega_3}{y}$ est un polynôme de l'anneau $\mathbb{Z}$ [x,A ,B] de degré 12 en x .

Avec le calcul , nous obtenons le carré du polynôme Ψ_3 :

$\Psi_3^2 = 9x^8 + 36Ax^6 + 72Bx^5 + 30A^2x^4 + 144ABx^3 + 12(12B^2 - A^3)x^2 - 24A^2Bx + A^4$; (10)

Ψ_3^2 est un polynôme de l'anneau [x,A ,B] de degré 8 en x , nous en déduisons le polynôme :

$\Psi_3^3 = 27x^{12} + 162Ax^{10} + 324Bx^9 + 297A^2x^8 + 1296ABx^7 + 108(A^3 + 12B^2)x^6 + 1080A^2Bx^5 +$

$9A(288B^2 - 11A^3)x^4 + 432B(4B^2 - A^3)x^3 + 18A^2(A^3 + 24B^2)x^2 - 12A^4Bx - A^6$; (11)

Ψ_3^3 est un polynôme de l'anneau Z[x,A ,B] de degré 12 en x .

Les formules (2) , (8) , (9) , (10) et (11) impliquent les coordonnées du point 3P :

$$x_{3p} = \frac{\Phi_3}{\Psi_3^2} \quad , \quad y_{3p} = \frac{\omega_3}{\Psi_3^3} \; ; \qquad (12)$$

4-Sous groupes de m-torsion , groupe de torsion d'une Courbe Elliptique :
Le groupe E(K) de Mordell -Weil d'une Courbe Elliptique E , qui est additif , admet des sous groupes cycliques et des sous groupes abéliens .

Définition 2 :
1) Le sous groupe de m- torsion d'une Courbe Elliptique E, pour tout entier m > 1 , est l'ensemble des points P Є E(K) d'ordre m :

$$E(K)[m] = \{ P \in E(K) ; mP = O_E \}$$

Ces sous groupes sont cycliques ou abéliens d'ordre m.
2) Le groupe de torsion de la Courbe Elliptique, est l'ensemble des points P d'ordre fini. C'est la réunion infinie des sous groupes de m torsion de E :

$$T(E) = \bigcup_m E(K)[m]$$ **; pour chaque point P Є E(K) il existe m Є Z tel que** $mP = O_E$

Ce groupe de torsion T(E) est cyclique ou abélien, selon les invariants de la Courbe Elliptique. La détermination du groupe de torsion T(E) a été réalisée pour les Courbes Elliptiques sur le corps Q des nombres rationnels. La structure de ce groupe a été conjecturée par Ogg. Cette conjecture a été démontrée par Mazur [12].

Proposition 5 :
Les groupes de torsion des Courbes Elliptiques , sur le corps Q des nombres rationnels , sont isomorphe à l'un des 15 groupes additifs abéliens finis :

(1) $\mathbb{Z}/m\mathbb{Z}$ **pour m = 1,2,3,…,10 et m = 12 .**

(2) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2d\mathbb{Z}$ **pour d = 1,2,3,4 .**

Preuve :
Mazur a obtenu la preuve en utilisant les travaux de Ogg sur les équations diophantiennes, les propriétés des points rationnels sur les courbes modulaires et les travaux de Kubert sur les bornes de torsion de Courbes Elliptiques.
□

Citons quelques résultats publiés sur les groupes T(E)(K) de torsion .
(1)Kenku a montré qu'il n'y a pas de Courbe Elliptique E , sur un corps quadratique , qui contient un point d'ordre 32 , il a utilisé les courbes modulaires $X_1(16)$ et $X_1(32)$.
«Certain torsion points on Elliptic Curves defined over quadratic Fields » ; J .Lond . Math .19 (1979)-233-240.
(2) Kamienny a montré qu'il n'y a pas de Courbe Elliptique, sur un corps quadratique, qui contient un point d'ordre premier p = 17,19,23,29,31 ; il a utilisé des courbes modulaires $X_1(p)$.

« Torsion points on Elliptic Curves over all quadratic Fields », Duke Math . J- 53 (1986)-157-162.
(3) Fung , Stroker , Williams et Zimmer ont montré que le groupe de torsion T(E)(K) est isomorphe à l'un des 8 groupes additifs abéliens finis :

$$\mathbb{Z}/n\mathbb{Z} \text{ pour } n = 2,3,4,5,12 .$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/d\mathbb{Z} \text{ pour } d = 2,3,6 .$$

K est un corps cubique pur $K = Q(\sqrt[3]{a})$ et a non puissance $3^{ème}$ dans le corps K.
Ils ont utilisé les formes normales de Kubert E(b,c) , les propriétés de l'invariant modulaire j(E) et des valuations p-adiques v_p .
« Torsion groups of Elliptic Curves with integral j-invariant over pure cubic Fields », journal N . T . 36(1990)-12-45 .
(4) Kishi a montré que le groupe de torsion T(E)(K) est isomorphe à l'un des groupes abéliens additifs finis :

$$\mathbb{Z}/11\mathbb{Z} ; \mathbb{Z}/13\mathbb{Z} ; \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} ; \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} ; \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z} ;$$

$$\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} ; \mathbb{Z}/64\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} ; \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/32\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} .$$

K est un corps quartique cyclique imaginaire .
Il a utilisé la forme normale de Kubert E(b,c) , des valuations additives normalisées v_p et les réductions d'une Courbe Elliptique .
« On Torsion Subgroups of Elliptic Curves with integral j-invariant over imaginary cyclic quartic Fields » ; Tokyo J . Math vol 20 (1997) 315-327 .

Exemple 2 :
Considérons la Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + 1 \in Q [x , y] ; \qquad (1)$$

Calcul des invariants de E :

$$b_2 = b_4 = 0 , b_6 = 4 , b_8 = 0 , \Delta(E) = -27 \times 16 ; \qquad (2)$$

En utilisant les formules Ψ_i , nous obtenons les coordonnées d'un point 2P :

$$x_{2P} = \frac{x^4 - 8x}{(2y)^2} \text{ et } \quad y_{2P} = \frac{x^6 + 20x^3 - 8}{(2y)^3} \quad ; \qquad (3)$$

Par définition, un point de 2 –torsion satisfait la relation :

$$2P = O_E = (\infty,\infty) ; \qquad (4)$$

Les formules (3) et (4) impliquent l'ordonnée du point P :

$$y = 0 ; \qquad (5)$$

Les équations (1) et (5) impliquent trois solutions qui sont les abscisses de 3 points :

$P_1 = (-1,0)$ dans le plan IR^2, $P_2 = [\frac{1 + \sqrt{-3}}{2} , 0]$ et $P_3 = [\frac{1 - \sqrt{-3}}{2} , 0]$;dans le plan Complexe.

Ces trois points P_i , satisfont la relation $2P_i = O_E$, ce sont donc des points d'ordre 2 .

Figure 4(courbe tracée avec le logiciel Scientific Note book 5.0).

Exemple 3 :

Soit la Courbe Elliptique E d'équation :

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) \in IR[x] ; \text{ avec } e_i \neq e_j ;$$

Aux trois points d'intersection $T_i = (e_i , 0)$ avec l'axe Ox , la parallèle à l'axe Oy est la tangente à la Courbe Elliptique au point T_i . il en résulte que ces trois points d'intersection T_i sont des points de 2-torsion du groupe abélien E(Q) . La règle géométrique de 3 points colinéaires de la Courbe E implique les relations :

$T_1 + T_2 = T_3$, $T_1 + T_3 = T_2$ et $T_2 + T_3 = T_1$.

Ces 3 points et le point O_E forment le groupe de 2- torsion :

$$E[2] = \{ T_1 , T_2 , T_3 , O_E \} ;$$

Exemple 4 :

Soit la Courbe Elliptique E d'équation de Weierstrass :

$$E(n) : y^2 = x^3 - n^2x \in Q [x , y] ;$$

Cette courbe E(n) coupe l'axe Ox en trois points :

$$P_1 = (0,0)\ ,\ P_2 = (n,0) \text{ et } P_3 = (-n,0)\ .$$

Ces trois points engendrent un groupe additif abélien d'ordre 4 .

$$\{P_1\ ,\ P_2\ ,\ P_1 + P_2\ ,\ O_E\ \} \cong \mathbb{Z}\ /2\mathbb{Z} \times \mathbb{Z}\ /2\mathbb{Z}\ .$$

Ces trois points sont d'ordre 2 , ce groupe est le groupe de torsion T(E(n)) de la Courbe Elliptique .
C'est un groupe de Klein : $\{a\ ,\ b\ ,\ ab = ba\ ,\ a^2 = b^2 = (ab)^2 = e\ \}$.

Les coordonnées de points de torsion des Courbes Elliptiques E(Q) peuvent être calculées avec la :

Proposition 6 :
Soit une Courbe Elliptique E d'équation de Weierstrass :

$$\mathbf{E : y^2 = x^3 + Ax + B \in Q[x\ ,\ y]\ ;\ avec\ 4A^3 + 27B^2 \neq 0\ et\ A\ et\ B \in \mathbb{Z}\ ;}$$

Soit un point P ∈ E(Q) de torsion. Alors :
1) Les coordonnées x et y de P sont des entiers rationnels.
2) Lorsque $2P \neq O_E$, alors y^2 divise $4A^3 + 27B^2$.

Preuve :
Elle a été obtenue par [Lutz] et [Nagell].
□
Exemple 5 :
Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 - 3x + 10 \in Q[x\ ,\ y]\ ;$$

Figure 5(courbe tracée avec le logiciel Scientific Note book 5.0).

Alors : $4A^3 + 27B^2 = 3^4 \times 2^5$. Appliquons le théorème de Lutz-Nagell.

Les valeurs possibles de y^2 sont égales à :

$y^2 = 4 , 16 , 9 , 81 , 36 , 4 \times 81 = 324 , 9 \times 16 = 144 , 16 \times 81 = 1296.$

Pour $y^2 = 4$, j'obtiens l'équation diophantienne cubique $x^3 - 3x + 6 = 0$, pas de solutions rationnelles .
Pour $y^2 = 16$, j'obtiens l'équation diophantienne cubique $x^3 - 3x - 6 = 0$, pas de solutions rationnelles .
Pour $y^2 = 9$, j'obtiens l'équation diophantienne cubique $x^3 - 3x + 1 = 0$, pas de solutions rationnelles .
Pour $y^2 = 81$, j'obtiens l'équation diophantienne cubique $x^3 - 3x – 71 = 0$, pas de solutions rationnelles .
Pour $y^2 = 36$, j'obtiens l'équation diophantienne cubique $x^3 - 3x - 26 = 0$, pas de solutions rationnelles .
Pour $y^2 = 324$, j'obtiens l'équation diophantienne cubique $x^3 - 3x - 314 = 0$, pas de solutions rationnelles .
Pour $y^2 = 144$, j'obtiens l'équation diophantienne cubique $x^3 - 3x - 134 = 0$, pas de solutions rationnelles .
Pour $y^2 = 1296$, j'obtiens l'équation diophantienne cubique $x^3 - 3x – 1286 = 0$, pas de solutions rationnelles.

5- Théorème de Mordell-Weil d'une Courbe Elliptique :

Selon Lang , la preuve de ce théorème comporte 2 parties , l'une est consacrée à l'ordre fini du groupe quotient E(K) / mE(K) , l'autre partie concerne le type fini du groupe abélien E(K) .

Proposition 7 :

Soit le groupe de Mordell-Weil E(K)d'une Courbe Elliptique E .Alors le groupe quotient E(K) / mE(K) est fini pour un entier $m \geq 2$.

Preuve :

Selon Lang , je choisis l'équation de Weierstrass :

$$E : y^2 = (x - e_1)(x - e_2)(x - e_3) \in K[x] .$$

Soient trois homomorphismes de groupes :

$\theta_i : E(K) \longrightarrow K^* / K^{*2}$, i = 1 , 2 , 3 .

tels que les noyaux satisfont l'intersection :

$$\bigcap_{i=1,2,3} \ker \theta_i \subset 2\,E(K) \text{ , pour carac } (K) \neq 2 , 3 .$$

Ces trois homomorphismes Θ_i sont choisis tels que :

$\theta_i (O_E) = 1$, $\theta_i (x,y) = x - e_i$ si $x \neq e_i$ et $\theta_i (e_i,0) = (e_i - e_j)(e_i - e_k)$.

Alors en utilisant certaines propriétés des groupes abéliens , les auteurs obtiennent le résultat annoncé .

□

Pour le type fini du groupe E(K) de Mordell-Weil, commençons par les fonctions hauteurs.

Définition 3 : (selon Silverman)
Une hauteur sur un groupe abélien A est une fonction h à valeurs réelles :

$$\mathbf{h : A \longrightarrow IR}$$

qui satisfait les 3 axiomes :
(h_1) à tout point P_1 de A correspond une constante $c_1(P_1, A) = c_1$ telle que :

$$\mathbf{h(P_1 + P) \leq 2h(P) + c_1 \text{ , pour tout point P de A.}}$$

(h_2) à une constante c_2 correspond un entier $m \geq 2$ tel que :

$$\mathbf{h(mP) \geq m^2 h(P) \text{ , pour tout point P de A.}}$$

(h_3) l'ensemble des points P de A de hauteur h(P) bornée est fini.

$$\mathbf{\{ P \in A ; h(P) \leq c_3 \} \text{ est un ensemble fini.}}$$

Les fonctions hauteurs sont déterminées par leur valeur aux points du groupe abélien A.
Elles permettent de démontrer la finitude du groupe A / 2A.

Proposition 8 :
Soit un groupe abélien A tel que le groupe quotient A / mA soit fini.
Alors le groupe abélien A est de type fini.

Preuve :
Le groupe abélien quotient A / mA étant fini, considérons des représentants des classes de A / mA :

$$T_1 , T_2 ,\ldots, T_s ; \qquad (1)$$

Construisons une suite infinie de points de A avec des combinaisons linéaires :

$P = m P_1 + T_{i1}$; $P_1 = mP_2 + T_{i2}$, … , $P_{n-1} = mP_n + T_{in}$. avec ij = 1, … , s. (2)

Tout combinaison linéaire $P_{j-1} = mP_j + T_{ij}$ implique:

$$mP_j = P_{j-1} - T_{ij} ; \qquad (3)$$

Appliquons au 1er membre de (3) l'axiome (h_2) et au 2ème membre de (3) l'axiome (h_1) .
Nous obtenons l'inégalité :

$$h(P_j) \leq \frac{1}{m^2} \left(2h\,(P_{j-1}) + c' \right) ; \qquad (4)$$

En appliquant cette procédure à chaque point P , P_1 , … , P_{n-1} et en ajoutant les inégalités obtenues membre à membre , nous obtenons l'inégalité :

$$h(P_n) \leq \left(\frac{2}{m^2} \right)^n h(P) + \left(\frac{1}{m^2} + \frac{2}{m^4} + \frac{4}{m^6} + \ldots + \frac{2^{n-1}}{m^{2n}} \right) c' \; ; \qquad (5)$$

L'hypothèse $m \geq 2$ et le développement limité égal à la somme : $\left(\frac{1}{m^2} + \frac{2}{m^4} + \ldots + \frac{2^{n-1}}{m^{2n}} \right)$

impliquent l'inégalité :

$$h(P_n) \leq 1 + \frac{c'}{r} \; ; \qquad (6)$$

Donc l'ensemble $\{ P_n , n \longrightarrow \infty \}$ est un ensemble de points de hauteur bornée.

Par l'axiome (h_3), cet ensemble est borné

$$\{ P_1 , \ldots, P_r \} ; \qquad (7)$$

Il en résulte que tout point P du groupe abélien A est une $\mathbb{Z}$-combinaison linéaire de la forme :

$$P = n_1 T_1 + \ldots + n_S T_S + n_{S+1} P_1 + \ldots + n_{S+r} P_r \; , n_i \in \mathbb{Z} \; ; \qquad (8)$$

Donc le groupe abélien A, admettant un nombre fini de générateurs, est de type fini.
□

Cette proposition s'applique aux groupes de Mordell-Weil des Courbes Elliptiques.

Il existe plusieurs types de hauteurs. Indiquons quelques unes :

1- la hauteur logarithmique sur une Courbe Elliptique E(Q) est la fonction :

$h_{log} : E(Q) \longrightarrow IR$

de valeur $h_{log}(P) = \log\{\max (|a| , |b|)\}$, pour $x_P = a / b$ et $h_{log}(O_E) = 0$.

2- la hauteur logarithmique relative à une fonction $f \in K(E)$ est la fonction :

$h_f : E(K) \longrightarrow IR$

de valeur $h_f (P) = h_{log}(f(P))$

3-la hauteur canonique (ou de Néron-Tate) sur une Courbe Elliptique E est la fonction :

$$\hat{h} : E(K) \longrightarrow IR$$

de valeur $\hat{h}(P) = \lim_{n \to \infty} 4^{-n} h_f(2^n P)$

Cette hauteur canonique satisfait la :

Proposition 9 :

1) La hauteur canonique $\hat{h} : E(K) \longrightarrow IR$, satisfait la loi du parallélogramme :

$$\hat{h}(P + M) + \hat{h}(P - M) = 2\hat{h}(P) + 2\hat{h}(M)$$ **pour tous points P et M de E(K).**

2)Pour tout point $P \in E(K)$ et tout entier $m \in \mathbb{Z}$:

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

3) La hauteur $\hat{h}$ induit une forme quadratique sur E(K) :

$$< , > : E(K) \times E(K) \longrightarrow IR$$

de valeur $< M , P > = \hat{h}(P + M) - \hat{h}(P) - \hat{h}(M)$.

Cette forme $< , >$ est bilinéaire.

4) $\hat{h}(P) \geq 0$ et $\hat{h}(P) = 0$ si et seulement si le point P est d'ordre fini.

Preuve :
On utilise la définition de $\hat{h}$ et les propriétés des formes quadratiques bilinéaires.
C'est un théorème de Néron – Tate.
□

Cette forme quadratique $\hat{h}$ de Néron-Tate, bilinéaire, permet d'introduire un invariant des Courbes Elliptiques.

Définition4 :

Soit une Courbe Elliptique E et un système de générateurs P_1 , ..., P_r de la partie infinie E(K) / T(E(K)) , le régulateur de E est le déterminant d'ordre r :

$$R(E) = \det(< P_i , P_j >) , 1 \leq i , j \leq r , \text{ pour } r > 0.$$

et

$$R(E) = 1 \text{ pour } r = 0, < , > = \text{forme quadratique de la proposition 10}.$$

C'est le régulateur elliptique de la Courbe Elliptique E.

La proposition 9 s'applique au groupe abélien E(K).

Proposition 10 :
Le groupe de Mordell-Weil E(K) d'une Courbe Elliptique E est de type fini.
□

La structure de ce groupe de Mordell-Weil d'une Courbe Elliptique est précisée par le :

Corollaire 1 :
Le groupe de Mordell-Weil E(K) d'une Courbe Elliptique E est isomorphe au produit de groupes abéliens :

$$E(K) \cong T(E) \times \mathbb{Z}^r$$

où T(E) est le groupe de torsion de la Courbe Elliptique E , qui est fini.
r = r(E) est un entier positif ou nul.
$\mathbb{Z}^r$ = r copies du groupe abélien additif infini $\mathbb{Z}^r$.
□

Définition5 :
L'entier naturel r = r(E) ≥ 0 de cette formule d'isomorphisme est le rang de la Courbe Elliptique E. C'est aussi le nombre de générateurs P_1 , … , P_r de la partie infinie du groupe E(K).

Le rang d'une Courbe Elliptique ne peut être obtenu à l'aide d'une formule.

CHAPITRE III
ISOGENIES DE COURBES ELLIPTIQUES.

Une Courbe Elliptique a une structure de groupe abélien de type fini, selon la théorie des groupes de courbes il existe des homomorphismes, des endomorphismes, des isomorphismes, des automorphismes et des isogénies de Courbes Elliptiques.

1. Morphismes de Courbes Elliptiques :

Définition 1:

Soit deux Courbes Elliptiques E et E', sur le même corps K, d'éléments neutres respectifs O_E et $O_{E'}$. Un morphisme de Courbes Elliptiques est un homomorphisme de groupes abéliens f :E(K) ⟶ E'(K).

1-1. Endomorphismes de Courbes Elliptiques :

La description de l'anneau des endomorphismes End(E) d'une Courbe Elliptique a été indiquée par Deuring.
Selon Deuring, l'anneau des endomorphismes d'une Courbe Elliptique est isomorphe soit à l'anneau $\mathbb{Z}$, soit à un ordre d'un corps quadratique imaginaire, soit à un ordre de l'algèbre des quaternions.
Ce dernier cas se produit lorsque carac(K) = p > 0.

L'ensemble des endomorphismes $End_K(E)$ d'une Courbe Elliptique forme un anneau intègre de caractéristique nulle, isomorphe à l'anneau $\mathbb{Z}$ ou isomorphe à un anneau contenant $\mathbb{Z}$.

Définition2:

Les Courbes Elliptiques dont l'anneau des endomorphismes $End_K(E)$ contient l'anneau $\mathbb{Z}$ sont des Courbes Elliptiques à Multiplication Complexe.

Dans le cas où la Courbe Elliptique E est à Multiplication Complexe, l'anneau End(E) est isomorphe à l'anneau des entiers d'un corps quadratique imaginaire.

1-2. Isomorphismes de Courbes Elliptiques :

Définition3:

Un isomorphisme de 2 Courbes Elliptiques est un isomorphisme f :E(K) ⟶ E'(K) de leurs groupes de Mordell-Weil.

Donc il satisfait les formules d'isomorphisme de groupes abéliens :
1) $f(O_E) = O_{E'}$.

2) $f(P_1 + P_1) = f(P_1) + f(P_2)$.

3) f est bijective.

Examinons les propriétés de ces isomorphismes :

Soit deux Courbes Elliptiques E et E', d'équations de Weierstrass :

$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in K[x,y]$ et

$E' : Y^2 + a'_1XY + a'_3Y = X^3 + a'_2X^2 + a'_4X + a'_6 \in K[X,Y]$;

Proposition1 :

Un isomorphisme de 2 Courbes Elliptiques E et E' est une application :

$$\mathbf{f : E(K) \longrightarrow E'(K)}$$

de valeur : f(x,y) = (X ,Y) ;

pour $x = u^2X + r$, $y = u^3Y + su^2X + t$ et $u \neq 0$, r, s, t $\in$ K. **(1)**

Preuve:

Les formules d'homomorphismes :

$f(P_1 + P_1) = f(P_1) + f(P_2)$ et $f(O_E) = O_{E'}$, se vérifient par le calcul.

Pour vérifier que f est bijective, nous calculons les valeurs de X et Y.

$$X = \frac{(x - r)}{u^2} \quad \text{et} \quad Y = \frac{(y - s\,u^2 X - t)}{u^3}.$$

L'hypothèse $u \neq 0$ implique la bijection.

□

La relation (1) et les calculs impliquent des relations entre les cœfficients et les invariants des deux courbes nous résumons dans le :

Corollaire1:

Soit 2 Courbes Elliptiques E et E' isomorphes. Alors:

1) Les coefficients a_1 et a'_1 sont liés par les relations :

$$\mathbf{ua'_1 = a_1 + 2s ;}$$

$$\mathbf{u^2a'_2 = a_2 - sa_1 + 3r - s^2 ;}$$

$$\mathbf{u^3a'_3 = a_3 + ra_1 + 2t ;} \qquad \mathbf{(2)}$$

$$\mathbf{u^4a'_4 = a_4 - sa_3 - (t + rs)a_1 + 2ra_2 + 3r^2 - 2st ;}$$

$$\mathbf{u^6a'_6 = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 ;}$$

2) Les invariants b_{2i} et b'_{2i} sont liés par les relations :

$$\begin{aligned} u^2 b'_2 &= b_2 + 12r; \\ u^4 b'_4 &= b_4 + rb_2 + 6r^2 ; \\ u^6 b'_6 &= b_6 + 2rb_4 + r^2 b_2 + 4r^3 ; \\ u^8 b'_8 &= b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4 ; \end{aligned} \qquad (3)$$

3) Les relations entre les invariants c_{2i} et c'_{2i} sont :

$$u^4 c'_4 = c_4 \text{ et } u^6 c'_6 = c_6 ; \qquad (4)$$

4) Les discriminants satisfont la relation :

$$u^{12}\Delta(E') = \Delta(E) ; \qquad (5)$$

5) Les invariants modulaires sont égaux :

$$j(E) = j(E') ; \qquad (6)$$

6) Les invariants différentiels satisfont la relation :

$$u^{-1}\omega(E') = \omega(E); \qquad (7)$$

Preuve :
En remplaçant x et y dans l'équation de E par les fonctions :

$x = u^2X + r$ et $y = u^3Y + su^2X + t$, nous obtenons toutes les relations du corollaire1.
□

Proposition2 :
Deux Courbes Elliptiques E et E' sur un corps K de carac(K) $p \neq 2, 3$, sont isomorphe si et seulement si leurs invariants modulaires sont égaux.

Preuve :
Preuve de « E et E' sont isomorphes » implique « j(E) = j(E') ».
Soit 2 Courbes Elliptiques E et E' isomorphe ; alors la formule (6) implique l'égalité :

$$j(E) = j(E').$$

Preuve de « j(E) = j(E') » implique « E et E' sont isomorphes ».
Nous examinons les 3 cas :

j(E) = j(E') = 0,
j(E) = j(E') = 1728 et
j(E) = j(E') = t , $t \neq 0$ et 1728

1. Pour j(E) = j(E') = 0, nous prenons 2 équations de Weierstrass de la forme :

$$E : y^2 = x^3 + a_4x + a_6 \text{ ; avec } 4a_4^3 + 27a_6^2 \neq 0 ;$$

$$E' : y^2 = x^3 + a'_4x + a'_6 \text{ ; avec } 4a_4'^3 + 27a_6'^2 \neq 0;$$

L'invariant modulaire d'une Courbe Elliptique est égal à :

$$j(E) = \frac{4(1728a_4^3)}{4a_4^3 + 27a_6^2};$$

L'hypothèse d'égalité des invariants j(E) = j(E') implique les relations :

$$a_4 = a'_4 = 0,\ a_6 \neq 0 \quad \text{et} \quad a'_6 \neq 0 ;$$

Par les formules (2) d'isomorphisme, il existe un élément u Є K_{al}, tel que :

$$u^6a'_6 = a_6 ;$$

Cette équation admet, dans une clôture algébrique K_{al}, 6 racines :

$$u = \left(\frac{a_6}{a'_6}\right)^{1/6} ;$$

Il en résulte les isomorphismes :

$$f : E(K) \to E'(K) \quad , \quad \text{de valeur : } f(x, y) = (u^2x , u^3y)$$

2. Pour j(E) = j(E') = 1728, nous gardons les équations de Weierstrass des Courbes E et E'.

L'hypothèse sur j(E) et j(E') implique les conditions :

$$a_4 \neq 0 , a'_4 \neq 0 \text{ et } a_6 = a'_6 = 0 ;$$

Par les formules (2) d'isomorphisme, il existe un élément u Є K_{al}, tel que :

$$u^4a'_4 = a_4 ;$$

Cette équation admet 4 racines :

$$u = \left(\frac{a_4}{a'_4}\right)^{1/4} ;$$

Il en résulte les isomorphismes :

$$f : E(K) \to E'(K) \quad , \quad \text{de valeur : } f(x, y) = (u^2x , u^3y);$$

3. Pour j(E) = j(E') = t ≠ 0 , nous gardons les équations de Weiesstrass.

La formule de j(E) et l'hypothèse j(E) = j(E') = t , impliquent l'équation :

$$4a_4^3(1728 - t) = 27a_6^2 t,$$

Cette équation admet la solution :

$$a_4 = \frac{3t}{1728 - t} \quad , \quad a_6 = \frac{2t}{1728 - t};$$

L'égalité j(E) = j(E') implique la relation :

$$a_4^3 a_6'^2 = a_4'^3 a_6^2;$$

Par les formules (2) d'isomorphisme, il existe un élément non nul u tel que :

$$u^4 a_4' = a_4 \text{ et } u^6 a_6' = a_6;$$

Nous en déduisons les solutions :

$$u = \left(\frac{a_4}{a_4'}\right)^{1/4} = \left(\frac{a_6}{a_6'}\right)^{1/6};$$

Il en résulte les isomorphismes :

$$f : E(K) \to E'(K) \quad , \quad \text{de valeur : } f(x, y) = (u^2 x, u^3 y);$$

Alors la Courbe Elliptique E a pour équation de Weierstrass :

$$y^2 = x^3 + \frac{3tx}{1728 - t} + \frac{2t}{1728 - t};$$

□

Lorsque carac(K) = 2 ou 3 , les formules des invariants des Courbes Elliptiques sont modifiées.

Exemple1 :
Soit une Courbe Elliptique E_1 d'équation de Weierstrass :

$$E_1: y^2 + 2xy + y = x^3 + 3x^2 + 4x + 1 \in K[x,y] \text{ , carac(K)} \neq 2,3.$$

Courbe Elliptique isomorphe E_2 pour les valeurs u = 2, r = 1, s = 0 et t = 0.

$$E_2: y^2 + xy + \frac{3}{8}y = x^3 + \frac{3}{2}x^2 + \frac{13}{16}x + \frac{9}{64};$$

Les formules d'isomorphismes liant les invariants b_{2i} et les discriminants impliquent :

$$b'_2 = 7,\ b'_4 = 2,\ b'_6 = \frac{45}{64},\quad b'_8 = \frac{59}{256},\ \Delta(E_2) = \frac{-195}{4096} = 2^{-12}\Delta(E_1).$$

Tableau de valeurs des coordonnées de quelques points de la Courbe E_1:

x	-1	$-\frac{1}{4}$	0	$\frac{1}{6}$	2
y	Pas de racines réelles.	$-\frac{1}{4}\pm\frac{\sqrt{15}}{8}$	$-\frac{1}{2}\pm\frac{\sqrt{5}}{2}$	$-\frac{2}{3}\pm\frac{5\sqrt{114}}{36}$	$-\frac{5}{2}\pm\frac{\sqrt{141}}{2}$

La Courbe Elliptique E_1 coupe l'axe Ox en un seul point d'abscisse $x_1$obtenue avec le logiciel Maple : $x_1 \approx -0{,}31$.
Elle coupe l'axe Oy en deux points d'ordonnées $-\frac{1}{2}+\frac{\sqrt{5}}{2}$ et $-\frac{1}{2}-\frac{\sqrt{5}}{2}$.

Tableau de valeurs des coordonnées de quelques points de la Courbe E_2:

x	-1	$-\frac{1}{4}$	0	$\frac{1}{6}$	2
y	Pas de racines réelles.	$-\frac{1}{16}\pm\frac{\sqrt{5}}{16}$	$-\frac{3}{16}\pm\frac{3\sqrt{5}}{16}$	$-\frac{13}{48}\pm\frac{\sqrt{8205}}{144}$	$-\frac{19}{16}\pm\frac{\sqrt{4397}}{16}$

La Courbe Elliptique E_2 coupe l'axe Ox en un seul point d'abscisse x_2 obtenue avec le logiciel Maple : $x_2 \approx -0{,}33$.

Elle coupe l'axe Oy en deux points d'ordonnées : $\left(0, -\frac{3}{16}+\frac{3\sqrt{5}}{16}\right)$ et $\left(0, -\frac{3}{16}-\frac{3\sqrt{5}}{16}\right)$.

La Courbe Elliptique E_1 :

Figure1.

La Courbe Elliptique E_2 isomorphe à E_1 :

Figure2.

La relation j(E) = j(E') implique une relation d'équivalence dans l'ensemble des Courbes Elliptiques.
Il en résulte que les Courbes Elliptiques se répartissent en classes d'équivalences de Courbes Elliptiques isomorphes :

$$cl(E') = \{E' , E'_1 , E'_2 , \dots , E'_n\} ;$$

d'invariants modulaires égaux :

$$j(E) = j(E'_1) = j(E'_2) = \dots = j(E'_n);$$

1-3. Automorphismes d'une Courbe Elliptique:
Définition4:
Un automorphisme d'une Courbe Elliptique est un endomorphisme bijectif du groupe abélien E(K).

L'ordre du groupe des automorphismes d'une Courbe Elliptique E est un diviseur de 24, comme le montre la :

Proposition2:
Soit une Courbe Elliptique E sur un corps K, d'invariant modulaire j(E).
Alors, le groupe Aut(E) de ses automorphismes est d'ordre :

1) **2 si j(E) ≠0, 1728 et carac(K) ≠ 2 et 3.**
2) **4 si j(E) = 1728 et carac(K) ≠ 2 et 3.**
3) **6 si j(E) = 0 et carac(K) ≠ 2 et 3.**
4) **12 si j(E) = 0 = 1728 et carac(K) = 3.**
5) **24 si j(E) = 0 = 1728 et carac(K) = 2.**

Où carac(K) est la caractéristique du corps K.

Preuve :

1) Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + Ax + B \; ; \; \text{avec} \;\; 4a_4^3 + 27a_6^2 \neq 0 \; ; \qquad (1)$$

sur un corps K de caractéristique carac(K) ≠ 2 et 3.
Les formules impliquent les deux invariants de la Courbe :

$$\Delta(E) = \; -16(4a_4^3 + 27a_6^2) \neq 0 \;\; \text{et} \;\; j(E) = \frac{4.1728.a_4^3}{4a_4^3 + 27a_6^2} \neq 0{,}1728. \qquad (2)$$

Les hypothèses carac(K) ≠ 2, 3, j(E) ≠ 0,1728 et la relation (2) impliquent les conditions :

$$a_3 \neq 0 \quad \text{et} \quad a_6 \neq 0 \; ; \qquad (3)$$

Les formules d'isomorphismes (1) impliquent l'automorphisme :

$$g_u : E(K) \longrightarrow E(K)$$

$$(x,y) \longrightarrow (u^2x \, , \, u^3y)$$

pour un certain élément u non nul du corps K.
La Courbe Elliptique E' image de la Courbe Elliptique E par l'isomorphisme g_u est :

$$E' : Y^2 = X^3 + a'_4 X' + a'_6 \; ;$$

avec les relation:

$$a_4 = u^4 a'_4 \quad \text{et} \;\; a_6 = u^6 a'_6 \; ;$$

(4)

Les invariants modulaires des deux Courbes E et E' sont égaux:

$$j(E) = j(E') \; ;$$

ce qui implique l'égalité :

$$\frac{a_4^3}{4a_4^3 + 27a_6^2} = \frac{a_4'^3}{4a_4'^3 + 27a_6'^2};$$

Les formules (4) impliquent les valeurs de l'élément u : $u^4 = u^6 = 1$ par les propriétés de l'automorphisme g_u.
Il en résulte $u^2 = 1$ et les deux automorphismes :

$$(x \, , \, y) \rightarrow (x \, , \, y) \quad \text{et} \quad (x \, , \, y) \rightarrow (x \, , \, -y).$$

Donc le groupe Aut(E) est d'ordre deux.

2) Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 = x^3 + a_4x + a_6 \in K[x,y] ; \quad (1)$$

Les formules impliquent les valeurs des invariants de E :

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) \neq 0 \text{ et } j(E) = \frac{1728.4.a_4^3}{4a_4^3 + 27a_6^2} = 1728. \quad (2)$$

Les hypothèses carac(K) ≠ 2,3 et la formule (2) impliquent la condition :

$$a_6 = 0 ; \quad (3)$$

La Courbe E étant Elliptique et la formule (3) impliquent la condition :

$$a_4 \neq 0;$$

Les formules d'isomorphismes (1) impliquent l'automorphisme :

$$g_u : E(K) \longrightarrow E(K)$$

$$(x,y) \longrightarrow (u^2x , u^3y)$$

pour un certain élément u non nul du corps K.
La Courbe Elliptique E' image de la Courbe E par l'isomorphisme g_u a pour équation de Weierstrass:

$$E' : Y^2 = X^3 + a'_4 X' + a'_6 ;$$

avec les relations:

$$a_4 = u^4 a'_4 \quad \text{et} \quad a_6 = u^6 a'_6 ; \quad (4)$$

Les formules (3) et (4) impliquent : $a_4 = u^4$, $a'_4 \neq 0$ et $a_6 = a'_6 = 0$; (5)

La formule (5) implique :

$$u^4 = 1.$$

Il en résulte les quatre automorphismes :

$$(x , y) \to (x , y) \ , \ (x , y) \to (x , -y) \ , \ (x , y) \to (-x , -iy) \text{ et } (x , y) \to (-x , iy).$$

3) Soit une Courbe Elliptique E d'équation de Weierstrass ;

$$E : y^2 = x^3 + a_4x + a_6 ; \quad (1)$$

Il en résulte les invariants :

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) \neq 0 \quad \text{et} \quad j(E) = 0. \qquad (2)$$

Les hypothèses carac(K) ≠ 2,3 ; j(E) = 0 et la relation (2) impliquent les valeurs :

$$a_4 = 0 \text{ et } a_6 \neq 0. \qquad (3)$$

Les formules d'isomorphismes (1) impliquent l'automorphisme :

$$g_u : E(K) \longrightarrow E(K)$$

$$(x,y) \longrightarrow (u^2x , u^3y)$$

Pour un certain élément u non nul du corps K.
La Courbe Elliptique E' image de la Courbe E par l'isomorphisme g_u a pour équation :

$$E' : Y^2 = X^3 + a'_6 ;$$

avec la relation :

$$u^6 a'_6 = a_6 ; \qquad (4)$$

L'équation $u^6 = 1$ admet six racines : $u = \pm 1, \pm j, \pm j^2$.
Il en résulte les six automorphismes :

$$(x , y) \to (x , y) \;\; ; \;\; (x , y) \to (x , - y) \;\; ; \;\; (x , y) \to (jx , y) \;\; ; \;\; (x , y) \to (jx , - y) \;\; ; \;\; (x , y) \to (j^2 x , y) \;\; ;$$

$$(x , y) \to (j^2 x , - y) \text{ où } j = \exp\left(\frac{2i\pi}{3}\right) \text{ et } j^3 = 1.$$

4)C'est la valeur j(E) = 0 et la formule $j(E) = \dfrac{c_4^3}{\Delta(E)}$ qui justifient la forme convenable de l'équation de Weierstrass de la Courbe E :

$$E : \; y^2 = x^3 + a_4x + a_6 \;\; ;$$

Nous considérons l'isomorphisme du groupe abélien E(K) de la forme :

$$g_u : E(K) \longrightarrow E'(K)$$

$$(x,y) \longrightarrow (u^2x + r , u^3y)$$

Les relations entre a_i et a_i' impliquent les formules :

$$u^4 = \frac{a_4}{a_4'} \text{ et } r^3 + r a_4 + a_6 - u^6 a_6' = 0.$$

Pour E = E', l'automorphisme implique les valeurs:

$$a_4' = a_4 \text{ et } a_6' = a_6.$$

Il en résulte le système :

$$\begin{cases} u^4 = 1. \\ r^3 + r\,a_4 + (1 - u^2)\,a_6 = 0. \end{cases} \qquad (1)$$

Cela implique 4 x 3 = 12 paires (u , r) qui déterminent un groupe de douze automorphismes de la Courbe E. Les quatre valeurs de u sont ±1 , ±i , les trois valeurs de r sont les trois racines de l'équation dans le système (1). Les douze automorphismes de la Courbe E sont :

$$(x , y) \to (x + r_1 , y)\ ;\ (x , y) \to (x + r_2 , y)\ ;\ (x , y) \to (x + r_3 , y)\ ;\ (x , y) \to (x + r_1 , - y)\ ;$$
$$(x , y) \to (x + r_2 , - y)\ ;\ (x , y) \to (x + r_3 , - y)\ ;\ (x , y) \to (-x + r_1 , - iy)\ ;\ (x , y) \to (-x + r_2 , - iy)\ ;$$
$$(x , y) \to (-x + r_3 , - iy)\ ;\ (x , y) \to (-x + r_1 , iy)\ ;\ (x , y) \to (-x + r_2 , iy)\ ;\ (x , y) \to (-x + r_3 , iy).$$

Ce engendré par u et r , $u^3 = 1$, $r^3 = 1$, ur = 1 est le sous groupe alterné A_4 du groupe symétrique S_4. Ce sous groupe alterné est d'ordre 12.

5) Les hypothèses carac(K) =2 , j(E) = 0 et les formules : c_4 et $j(E) = c_4^3 / \Delta(E)$ justifient l'équation de Weierstrass de la forme :

$$E : y^2 + a_3 y + a_4 x + a_6 \in IF_q[x , y]\ ;\ q = 2^n. \qquad (1)$$

Ses invariants valent :

$$c_4 = -48 a_4 \quad ; \quad \Delta(E) = a_3^2 \neq 0.$$

Les automorphismes du groupe E(IF_q) sont :

$$\begin{aligned} g_u : E(K) &\longrightarrow E(K) \\ (x , y) &\longrightarrow (u^2 x + s^2 , u^3 y + s u^2 x + t)\ ; \end{aligned} \qquad (2)$$

Pour certains paramètres u , s et t du corps K.
Les relations entre a_i et a_i' impliquent les trois équations :

$$\begin{cases} u^3 = 1 = \dfrac{a_3}{a_3'}; \\ s^4 + a_3 s + (1 - u)\,a_4 = 0; \\ t^2 + t\,a_3 + s^6 + a_4 s^2 = 0; \end{cases} \qquad (3)$$

Tout automorphisme (2) de la Courbe E est déterminé par un triplet (u , s ,t). Les équations (3) admettent 3 solutions u, 4 solutions s et 2 solutions t. Il en résulte que le groupe *A*ut(E) est un groupe produit d'un groupe cyclique C_3 d'ordre 3 twisté par le produit d'un groupe engendré par un élément s d'ordre 4 et un groupe engendré par un élément t d'ordre 2 qui forment le groupe des quaternions d'ordre 8.

Ce groupe *A*ut(E) est donc d'ordre 3 x 8 = 24.
Il est isomorphe au groupe spécial linéaire $SL(2, IF_3)$.
□

1-4.Isogénies de Courbes Elliptiques :
Pour étudier les isogénies de Courbes Elliptiques, nous utilisons des ouvrages de Cassels[3] et de Shimura[17].
Signalons que le terme d'isogénie est utilisé pour les Variétés Abéliennes et pour les Tores Complexes.

Définition5:
Une isogénie de Courbes Elliptiques est un homomorphisme de leurs groupes de Mordell-Weil.

$$f : E_1(K) \to E_2(K);$$

qui satisfait les conditions :
1) *f* n'est pas nulle.
2) **Le noyau de *f* est un sous groupe fini du groupe $E_1(K)$.**
3) ***f*** **est surjective.**
4) $f(P_1 + P_2) = f(P_1) + f(P_2)$ et $f(O_{E_1}) = O_{E_2}$.

Cette définition est empruntée à Shimura[17].
Les Courbes E_1et E_2 sont isogènes.

Exemple :
La multiplication par un entier m sur le groupe de Mordell-Weil E(K) est une isogénie.

$$t_m : E(K) \longrightarrow E(K) \text{ ; de valeur } t_m(P) = mP.$$

Le symbole mP signifie :

mP = P + … + P, m fois P	si m > 0.
mP = (-m)(-P),	si m < 0.
$mP = O_E = (\infty , \infty)$,	si m = 0.

Une isogénie possède des invariants : un degré et une isogénie duale ;

Définition 6 :
1) Le degré d'une isogénie $f : E_1(K) \to E_2(K)$ est égal à l'ordre de son noyau.

$$\deg f = \text{card}\left\{f^{-1}(O_{E_2})\right\}$$

2)l'isogénie duale de l'isogénie *f* de degré d est l'isogénie $f^\wedge : E_2(K) \to E_1(K)$ qui satisfait les relations de composition des applications :

$f^\wedge \circ f : E_1(K) \to E_2(K)$ est la multiplication par d sur la courbe E_1.

$f \circ f^\wedge : E_2(K) \to E_1(K)$ est la multiplication par d sur la courbe E_2.

La multiplication par un entier rationnel possède des propriétés liées à la caractéristique du corps de base de la Courbe Elliptique.

Proposition3:
Soit la multiplication t_m : E(K)$\rightarrow$ E(K) par un entier rationnel m.
Alors :

1) **Le degré de cette multiplication est égal à m^2.**
2) **Si la caractéristique du corps K est nulle, alors le noyau de l'isogénie t_m est isomorphe au groupe abélien produit *IZ*/m *IZ* x *IZ*/m *IZ*.**
3) **Si la caractéristique du corps K est un entier premier p, premier à m, alors le noyau de la multiplication par p^e est isomorphe au groupe trivial $\{O_E\}$ ou bien isomorphe au groupe abélien IZ/ p^eIZ pour e = 1,2,3,…**

Preuve :Elle a été indiquée par Deuring [4].
□

Le noyau d'une isogénie et les sous groupes du groupe E(K) sont liés par la :

Proposition 4:
Soit une Courbe Elliptique E_1 sur un corps K, et un sous groupe fini F du groupe de Mordell-Weil $E_1(K)$.

Alors il existe une unique isogénie $f : E_1(K) \rightarrow E_2(K)$ de noyau $f^{-1}(O_{E_2}) = F$ pour $E_2(K)$.

Preuve :
Les isogénies de Courbes Elliptiques sur le corps des nombres rationnels Q, qui sont de degré premier N sont en nombre fini d'après Mazur [12].

Puisqu'une isogénie $f : E_1(K) \rightarrow E_2(K) = E_1(K) / F$ est liée à un sous groupe F fini du groupe $E_1(K)$, il peut y avoir plusieurs isogénies d'une Courbe Elliptique.

Par exemple, l'ensemble des multiplications par m $\in$ *IZ* a une structure d'anneau.

Proposition5:
L'ensemble M(E) des multiplications par un entier rationnel sur une Courbe Elliptique E est un anneau isomorphe à l'anneau *IZ*.

Preuve :
Considérons l'application $f : IZ \rightarrow$ M(E), de valeur f (n) = multiplication par l'entier n :

$$u_n : E(K) \rightarrow E(K), u_n(P) = nP. \qquad (1)$$

Soient 2 entiers rationnels n, n' $\in$ *IZ*.
Calculons les valeurs f (n + n'), f (0) et f (n n') pour déterminer la structure de l'ensemble M(E).
f (n + n') = $u_{n+n'}$ de valeur $u_{n+n'}(P) = (n + n')P = nP + n'P$.

Cela implique $f(n + n') = f(n) + f(n')$. (2)

$f(nn') = u_{nn'}$ de valeur $u_{nn'}(P) = (nn')P = n(n'(P))$.

Cela implique la relation $f(nn') = f(n) \circ f(n')$. (3)

$f(0) = 0$, $0P = O_E$ = élément neutre du groupe E(K). (4)

Les 3 relations (1),(2) et (3) impliquent que *f* est un isomorphisme de l'anneau *IZ* sur l'ensemble M(E).

Un isomorphisme conserve la structure algébrique ;
Cela implique que l'ensemble :

M(E) = { multiplications par *IZ* sur la Courbe Elliptique}est un anneau isomorphe à *IZ*.
□

2-Algorithme de Velu de construction d'équation de Weierstrass de Courbes Elliptiques isogènes :

1) Soit une Courbe Elliptique E d'équation de Weierstrass :

$$E : g(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2 x^2 - a_4x - a_6 = 0 ;$$

2) Prendre un sous groupe fini F du groupe E(K).

3) Prendre $F_2 = \{ P \in F$, d'ordre 2 $\}$.

4) Partition de $F - F_2 - \{O_E\} = R \cup -R$; donc $R \cap -R = \{ \}$ et $-R = \{ -P ; P \in R \}$.

5) Prendre la partie $S = F_2 \cup R$.

6) Calculer les dérivées partielles g'_x et g'_y.

7) L'application $\lambda : E \to E / F = E'$; $(x , y) \to (X , Y)$ d'équation :

$$\begin{cases} X = x + \sum_{p \in S} \left[\dfrac{t_P}{x - x_P} + \dfrac{u_P}{(x - x_p)^2} \right] \\ Y = y - \sum_{P \in S} \left[u_P \dfrac{2y + a_1 x + a_3}{(x - x_p)^3} + t_P \dfrac{a_1(x - x_p) + y - y_P}{(x - x_p)^2} + \dfrac{a_1 u_P - g_P^x g_P^y}{(x - x_p)^2} \right] \end{cases}$$

est une isogénie de Courbes Elliptiques.

8)Calculer les nombres :

$g_x^{'}(P)$; $g_y^{'}(P)$; $t_P = g_x^{'}(P)$ si $P \in F_2$; $t_P = 6x_P^2 + b_2 x_P + b_4$ si $P \notin F_2$.

$u_P = 4x_P^3 + b_2 x_P^2 + 2b_4 x_P + b_6$; $b_2 = 4a_2 + a_1^2$; $b_4 = a_1 a_3 + 2a_4$ et $b_6 = a_3^2 + 4a_6$.

$$t = \sum_{P \in S} t_P \; ; \omega = \sum_{P \in S} (u_P + x_P t_P).$$

9) L'équation de Weierstrass de la Courbe isogène E' = E / F est

$$E' = E / F : Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + (a_4 - 5t) X + a_6 - b_2 t - 7\omega \; ;$$

Application de l'algorithme à la Courbe Elliptique E_1 d'équation de Weierstrass :

$$E_1 : y^2 = x^3 + 5 \; ; \qquad (1)$$

Le calcul implique les invariants $\Delta(E_1) = -10800 = -2^4 \times 3^3 \times 5^2$ et $j(E_1) = 0$. (2)

Le groupe $E_1(K)$ a un sous groupe F d'ordre 3 , formé des points :

$$F = \left\{ P = (0, \sqrt{5}), 2P = (0, -\sqrt{5}), 3P = O_E = (\infty, \infty) \right\}; \qquad (3)$$

En utilisant la méthode de Velu , nous obtenons les ensembles :

$$F_2 = \{ \} \quad , \quad R = \{P\} = S. \qquad (4)$$

Avec le calcul nous obtenons les coordonnées du point (X , Y) :

$$(x, y) \rightarrow \left[X = x + \frac{20}{x^2}, Y = y - \frac{40y}{x^3} \right], \qquad (5)$$

Par le calcul nous obtenons les nombres de l'étape (8)

$$T = 0 \; , \; \omega = 20 \; ; \qquad (6)$$

Nous en déduisons l'équation de Weierstrass de la Courbe Elliptique isogène E_2 :

$$E_2 = E_1 / F : Y^2 = X^3 - 135. \qquad (7)$$

Le calcul implique les invariants :

$$\Delta(E_2) = -7873200 = -2^4 \times 3^9 \times 5^2 \text{ et } j(E_2) = 0. \qquad (8)$$

La proposition 2 et la relation $j(E_1) = j(E_2) = 0$ impliquent que les Courbes isogènes E_1 et E_2 sont isomorphes.

Application de l'algorithme à l'exemple traité par Velu :
Soit la Courbe Elliptique d'équation de Weierstrass :

$$E : y^2 + xy + y = x^3 - x^2 - 3x + 3 \in Q[x,y] ; \quad (1)$$

Le calcul implique les invariants :

$$\Delta(E) = -1664 = -2^7 \times 13 \text{ et } j(E) = \frac{(3 \times 43)^3}{-2^7 \times 13}; \quad (2)$$

Le groupe E(Q) a un sous groupe cyclique F d'ordre 7 formé des points :

P = (1,0) , 2P = (-1,-2) , 3P = (3,-6) , 4P = (3,2) , 5P = (-1,2) , 6P = (1,-2) et $7P = O_E$;

La relation $7P = O_E$ implique P = -6P , 2P = -5P , 3P = -4P ;

Il en résulte les 3 parties :

$$F_2 = \Phi \ , \ R = \{ P, 2P , 3P \} \quad \text{et} \quad S = \{ P , 2P ,3P \} \quad (3)$$

Avec le calcul nous obtenons les nombres t = 42 , $\omega = 198$. (4)

Il en résulte l'équation de Weierstrass de la Courbe Elliptique isogène :

$$E' = E / F : Y^2 + XY + Y = X^3 - X^2 - 213X - 1257. \quad (5)$$

Le calcul implique les invariants de la Courbe isogène E' :

$$\Delta(E') = -125497034 = -2 \times 62748517 \quad \text{et} \quad j(E') = \frac{(3 \times 3403)^3}{-2 \times 62748517}; \quad (6)$$

Application de l'algorithme à la Courbe Elliptique E d'équation de Weierstrass :

$$E : y^2 + y = x^3 - x^2 \in Q[x,y] ; \quad (1)$$

Le calcul implique les invariants :

$$\Delta(E) = -11 \text{ et } j(E) = \frac{-2^{12}}{11}; \quad (2)$$

Le groupe E(Q) a un sous groupe cyclique F d'ordre 5 formé des points :

P = (0,0) , 2P = (1,-1) , 3P = (1,0) , 4P = (0,-1) , 5P = (∞,∞).

La relation 5P = (∞,∞) implique P = -4P , 2P = -3P.

Il en résulte les 3 parties du groupe E(Q) :

$$F_2 = \Phi \ , \ R = \{ P, 2P \} \quad \text{et} \quad S = \{ P , 2P \} \quad (3)$$

Avec le calcul nous obtenons les nombres t = 2 , ω = 4. (4)

et la Courbe Elliptique isogène E' d'équation de Weierstrass :

$$E' = E / F : y^2 + y = x^3 - x^2 - 10x - 20 ; \quad (5)$$

Le calcul implique les invariants :

$$\Delta(E') = -11^5 \text{ et } j(E') = \frac{-2^{12} \times 31^3}{11^5}; \quad (6)$$

Citons des équations classiques d'isogénies que l'on trouve dans[20].

Soient deux Courbes Elliptiques sur un corps K de caractéristique ≠ 2 ;

$$E_1 : y^2 = x^3 + ax^2 + bx ; \quad (1)$$

$$E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X ; b \neq 0 \text{ et } a^2 - 4b \neq 0. \quad (2)$$

Alors les deux applications f , g :

$$f : E_1 \to E_2$$
$$(x, y) \to \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right) \quad (3)$$

$$g : E_2 \to E_1$$
$$(X, Y) \to \left(\frac{Y^2}{4X^2}, \frac{Y(a^2 - 4b - X^2}{8X^2} \right) \quad (4)$$

Sont des isogénies.

Les changements de variables sont des fonctions rationnelles.les 2 applications ont des composées qui satisfont :
La composée $f \circ g : E_2 \to E_2$ est la multiplication par 2 sur $E_2(Q)$, c'est une isogénie de degré 4. (5)
La composée $g \circ f : E_1 \to E_1$ est la multiplication par 2 sur $E_1(Q)$, c'est une isogénie de degré 4. (6)
Les relations (5) et (6) impliquent que g est l'isogénie duale de l'isogénie *f* .
Le calcul implique les invariants de la Courbe Elliptique E_1 :

$$\Delta(E_1) = 16b^2(a^2 - 4b), c_4(E_1) = 16(a^2 - 3b) \text{ et } j(E_1) = \frac{16^2(a^2 - 3b)^3}{b^2(a^2 - 4b)}; \quad (7)$$

Les invariants de la Courbe Elliptique E_2 sont égaux à :

$$\Delta(E_2) = 64 \times 4b(a^2 - 4b)^2, c_4(E_2) = 16a^2 + 192b \text{ et } j(E_2) = \frac{(16a^2 + 192b)^3}{64 \times 4b(a^2 - 4b)^2}; \quad \textbf{(8)}$$

Application pour a =5, b = -8.

$$E_1 : y^2 = x^3 + 5x^2 - 8x \ ; \qquad (1)$$

$$E_2 : Y^2 = X^3 - 10X^2 + 57X \ ; \qquad (2)$$

Les isogénies de degré 2 sont les 2 morphismes :

$$\begin{aligned} & f : E_1 \to E_2 \\ & (x, y) \to \left(\frac{y^2}{x^2}, \frac{y(-8 - x^2)}{x^2} \right) \end{aligned} \qquad \textbf{(3)}$$

$$\begin{aligned} & g : E_2 \to E_1 \\ & (X, Y) \to \left(\frac{Y^2}{4X^2}, \frac{Y(57 - X^2)}{8X^2} \right) \end{aligned} \qquad \textbf{(4)}$$

Le calcul implique les invariants de la Courbe Elliptique E_1 :

$$\Delta(E_1) = 2^{10} \text{ x } 57, \ c_4(E_1) = 2^4 \text{ x } 7^2 \text{ et } j(E_1) = \frac{2^2 \text{ x } 7^6}{57}; \qquad (5)$$

Les invariants de la Courbe Elliptique E_2 sont égaux à :

$$\Delta(E_2) = 2^{11} \text{ x } 3^2 \text{ x } 361, \ c_4(E_2) = -2^4 \text{ x } 71 \text{ et } j(E_2) = \frac{-2 \text{ x } (71)^3}{3^2 \text{ x } 361}; \qquad (6)$$

En conclusion, je me propose de chercher d'autres formules d'isogénies dans des travaux de recherches ultérieures.
Pour cela je considérerai la structure analytique complexe d'une Courbe Elliptique associée à un tore complexe C / L.
Une autre voie consiste à prendre la structure de Variété abélienne de dimension un.
La théorie des Courbes Elliptiques comporte plusieurs aspects algébriques, analytiques, géométriques et algorithmiques.
Elle a des applications pour la factorisation des entiers très grands (plus de 500chifres), pour la codage et la cryptographies.

REFERENCES

🕮 **[1] ARTIN - E:**
«Algebraic Number and Algebraic Functions » Gordon and Brea Sciences Publishers - New York; (1960).

🕮 **[2] BOREVICH et SHAFAREVICH:**
(1) « Basic Algebraic Geometry »,Springer Verlag (1977).
(2) « Algebraic I», Moscou (1986)-Springer (1987).

🕮 **[3] CASSELS - JWS:**
« Diophantine Equations with Special Reference to Elliptic Curves » Journal London Mathematical Society 41 (1966) 193-291.

🕮 **[4] DEURING - M:** « Algebren » ; Springer Verlag, New York (1968).

🕮 **[5] HARTSHORNE - R:**
« Algebraic Geometry », GTM 52-Springer (1983).
Graduate texte in Mathematics n° 52 (1980)

🕮 **[6] HASSE - H:**
« Number theory » - Springer (1980)

🕮 **[7] HUSEMOLLER :**
« Elliptic Curves » - G.T.M -111 (1987).

🕮 **[8] IYANAGA - S :**
« The Theory of Numbers – North Holland Pub. Company- Amsterdam (1975)

🕮 **[9] KOSTRIKIN – A -I:**
« Introduction à l'algèbre » Ed. Mir- Moscou- 2eme edition (1986).

🕮 **[10] KUBERT :**
« Universal Bounds on the Torsion of Elliptic Curves » Journal London Mathematical Society 33 (1976) 193 – 237

🕮 **[11] LANG - S:**
(1) « Algebra » 2eme édition, Addison Wesley Publishing Company, Inc, Reading, Massachusetts, New York (1984).
(2) « Elliptic Curves – Diophantine Analysis » Springer Verlag (1978) -
(3) « Algebraic Number Theory », Addition – Wesley (1970).
(4) « Cyclotomic Fields », GTM 59 – Springer.

🕮 **[12] MAZUR - B:**
(1) « Rational isogenies of prime degre » Invent. Math. 44 (1978), 129-162.
(2) « Rational points on Modular Curves LNM. n° 601 (1977) 107 -147

🕮 **[13] NERON - A:**
« Quasi Fonctions et Hauteurs sur les Variétés Abéliennes », Annals of Mathematics 82 (1965), 249-331.

🕮 **[14] RUBIN - K:**
« Elliptic Curves with Complex Multiplication and the Conjecture of Birch Swinnerton »,
– Dyer – Inv. Math. 64 (1981) 455 – 470.

🕮 **[15] SERRE – J-P:**
« Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », Inventions Mathématiques 15 (1972), 259-331.

🕮 **[16] SHAFAREVICH:**
(1) «Basic Algebraic Geometry»,–Springer Verlag (1977).
(2) «Algebra I» - Moscou (1986) – Springer (1987).
Classification AMS = 12 – xx , 20 – xx.

🕮 **[17] SHIMURA -G:**
«Introduction to the Arithmetic Theory of Automorphic Function », Princeton University Press (1971).

🕮 **[18] SILVERMAN – J-H:**
(1) « The Arithmetic of Elliptic Curves », GTM 106 – Springer (1986). Classification AMS = 1401, 14G 99, 14H 05, 14 K 15.
(2) « Lower Bound for the canonical height on Elliptic Curves », Duke Math. J .48 (1981). 633-648
(3) « The Difference between the Weil Height and the Canonical Height on Elliptic Curves », Math. Comp. 35 (1990) 723-743.

🕮 **[19] TATE - J:**
« The Arithmetic of Elliptic Curves », Inv Math 23 (1974) 179-206.

🕮 **[20] VELU - J:**
« Isogénies entre Courbes Elliptiques », C.R.A.S. Paris (1971) 238-241.

🕮 **[21] WEIL - A:**
(1) « Sur un théorème de Mordell », Bull. Sci. Math. 54 (1930).
(2) « L'arithmétique sur les Courbes Elliptiques »,
acta Math 52 (1928)281-315

🕮 **[22] WEISS – E-D:**
« Algebraic Number Theory », Mc Graw – Hill. New York (1964).

🕮 **[23] ZITOUNI - M:**
« Courbes Elliptiques ; Géométrie - Arithmétique - Algorithmique (2007).