N°d'ordre : 30/2009 – M / M .T

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LARECHERCHE SCIENTIFIQUE
UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE « HOUARI BOUMEDIENE »
FACULTE DE MATHEMATIQUES

Mémoire

Présenté pour l'obtention du diplôme de MAGISTER

EN : MATHEMATIQUES

Spécialité : Algèbre et Théorie des nombres

Par : **CHACHOUA Ali**

Thème

Courbes Elliptiques à Invariant Modulaire Nul

Soutenu le 02 /07/2009 devant le jury composé de :

Mr Meziane AIDER	**Professeur**	**U.S.T.H.B**	**Président**
Mr Mohamed ZITOUNI	**Professeur**	**U.S.T.H.B**	**Directeur de thèse**
Mr Mohamed N. BENKAFADAR	**Professeur**	**U.S.M de Constantine**	**Examinateur**
Melle Soraya BOUGHABA	**Maitre de Conférences**	**U.S.M de Constantine**	**Examinatrice**
Mr Mohand O. HERNANE	**Maître de Conférences**	**U.S.T.H.B**	**Examinateur**

Sommaire

Introduction…...……..…….....2

I : Notions de Géométrie Algébrique

1. Espaces Affines - Variétés Affines…… ……..…3

2. Espaces Projectifs - Variétés Projectives …… ……..…6

3. Variétés Abéliennes …… ……..….9

II : Courbes Algébriques Planes - Cubiques de Weierstrass :

1. Courbes Algébriques Planes …….……...10

2. Classification des Courbes Algébriques Planes selon leur degré ……..…….10

3. Singularités d'une Courbe Algébrique Plane……..11

4. Genre d'une Courbe Algébrique……..13

5. Cubiques de Weierstrass ……14

6. Transformations de l'équation de Weierstrass……..15

7. Invariants des Cubiques de Weierstrass…….16

8. Classification des Cubiques de Weierstrass suivant leur discriminant….. 18

9. Courbes Elliptiques ……..26

III : Groupe de Mordell-Weil d'une Courbe Elliptique :

1. Loi de groupe abélien additif sur l'ensemble E (K) …….30

2. Coordonnées des points : - P, $P_1 + P_2$, P + P = 2 P du groupe E (K) ……..32

3. Points d'ordre fini d'une Courbe Elliptique …….35

4. Formules de Cassels des coordonnées des points m P …….36

5. Sous-groupes de torsion et groupe de torsion d'une Courbe Elliptique….37

6. Isomorphismes de groupes de Mordell-Weil de Courbes Elliptiques……41

IV : Application aux Courbes Elliptiques à invariant modulaire nul :

1. Equations des Courbes Elliptiques à invariant modulaire nul……... 47

2. Courbe de Fermat $u^3 + v^3 = w^3$…….……...…48

Références……51

Introduction

Les Courbes Elliptiques sont des courbes planes de degré 3 particulières .Elles sont munies de plusieurs structures algébriques : groupes, variétés, schémas…etc. Elles sont liées à la Géométrie Algébrique, à la Théorie des Nombres, à l'Analyse Complexe.

Dans cette thèse j'étudie les Courbes Elliptiques à invariant modulaire nul.

Il y a 4 chapitres :

Dans le chapitre I , j'ai traité des notions de Géométrie Algébrique : variétés affines, projectives , abéliennes de dimension 1 munies du point à l'infini $O_E = (0 , 1 , 0)$ dans le plan projectif $IP^2 (K)$ et $O_E = (\infty , \infty)$ dans le plan affine $IA^2(K)$.

Le chapitre II concerne les Cubiques de Weierstrass qui sont des courbes algébriques planes d'équations particulières :

$$E : y^2 + a_1 x y + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in K \left[x, y\right]$$

Ces cubiques possèdent plusieurs invariants : discriminant $\Delta(E)$, invariant modulaire j (E), régulateur, rang, qui permettent leurs classifications..

Dans le chapitre III, j'ai établi la structure algébrique de groupe additif abélien de l'ensemble E (K) des points K-rationnels d'une Courbe Elliptique E sur un corps commutatif K. La loi additive est basée sur la règle géométrique : '' 3 points colinéaires ont une somme nulle ''.

Ce groupe qui est de type fini est le groupe de Mordell-Weil.

J'ai décrit aussi les isomorphismes d'un groupe E (K).

Dans le quatrième chapitre , j'ai cherché les équations de Courbes Elliptiques à invariant modulaire nul avec les 2 conditions : $c_4 = 0$ et $\Delta (E) \neq 0$ .J'ai trouvé quelques équations et j'ai présenté la courbe de Fermat $x^3 + y^3 = z^3$ qui remplit les conditions précédentes.

CHAPITRE I : Notions de Géométrie Algébrique

Selon Hartshorne [6] , la Géométrie Algébrique est l'étude des Variétés Algébriques, des Diviseurs, des Shémas, de la Cohomologie ,des Courbes , des Surfaces…etc.

Pour arriver aux Variétés Abéliennes, nous allons décrire les Espaces Affines et les Variétés Affines, les Espaces Projectifs et les Variétés Projectives.

Dans ce chapitre, nous utilisons des notions qui se trouvent dans les ouvrages ''Algebraic Geometry'' de Hartshorne [6] et ''Basic Algebraic Geometry''de Shafarevich [17].

1. Espaces Affines - Variétés affines :

1.1 L'Espace Affine $IA^n(K)$:

Soient un entier positif $n \geq 1$ et un corps commutatif K.

Définition 1 :

L'espace affine de dimension $n \geq 1$ est l'ensemble des systèmes a :

$IA^n(K) = \{ a = (a_1, \ldots, a_n) , a_i \in K , i = 1, \ldots, n \}$

Les systèmes a sont des points de l'espace affine et les a_i sont les coordonnées du point a .

Exemples d'espaces affines :

1) n=2 : IA^2 (IR) est le plan affine euclidien réel ; ses points sont les couples a = (x,y) de nombres réels.

2) n = 3 : IA^3 (IR) est l'espace affine euclidien réel de dimension 3 ; ses points sont les triplets a = (x,y,z) de nombres réels.

3) $n \geq 4$: IA^n (IR) est un hyperespace de dimension n.

A l'espace affine IA^n (K) est associé l'anneau des polynômes à n indéterminées $K[X_1,..., X_n]$ sur le corps K.

L'espace affine IA^n (K) contient les zéros de ces polynômes $f \in K[X_1,..., X_n]$.

Définition 2 :

Un ensemble algébrique d'un espace affine IA^n *(K) est l'ensemble Z(S) des zéros communs d'une famille* $S = \{f_1,..., f_r\}$ *de polynômes* $f_i \in K[X_1,..., X_n]$ *:*

$Z(S) = \{ a \in IA^n(K) ; f_i(a) = 0$ *pour tout* f_i *de* $S \}$

Les ensembles algébriques de l'espace affine $IA^n(K)$ possèdent des propriétés :

Proposition 1 :

Soient des ensembles algébriques Z (S_i) de l'espace affine IA^n (K) :

1) La réunion de deux ensembles algébriques Z (S_1) et Z (S_2) est un ensemble algébrique :Z (S_1) $\cup$ Z (S_2)

2) L'intersection d'une famille d'ensembles algébriques $\{Z(S_i), i = 1,..., s\}$ **est un ensemble algébrique :** $\bigcap_{1 \le i \le s} Z(S_i)$

3) L'ensemble vide ϕ **et l'espace affine IA^n (K) sont des ensembles algébriques.**

Preuve de 1) Soient deux ensembles algébriques

Z (S_1) = $\{a \in IA^n(K), f_i(a) = 0, f_i \in K[x_1,..., x_n]\}$ et

Z (S_2) = $\{b \in IA^n(K), g_j(b) = 0, g_j \in K[x_1,..., x_n]\}$ alors la réunion

Z (S_1) $\cup$ Z (S_2) est l'ensemble des zéros des polynômes f_i et g_j ; c'est donc un ensemble algébrique.

Preuve de 2) Soit une famille finie $\{Z(S_i), i = 1,..., s\}$ d'ensembles algébriques , alors l'intersection $\bigcap_{1 \le i \le s} Z(S_i)$ est l'ensemble des zéros communs des polynômes associés aux ensembles Z (S_1) , …, Z (S_n) ; c'est donc un ensemble algébrique.

Preuve de 3) : ϕ = Z (1) , 1 étant le polynôme constant

$f = 1 + 0\ x_1 + \ldots + 0\ x_n \in K[x_1,..., x_n]$ qui n'admet pas de zéros.

IA^n (K) = Z (0) , 0 étant le polynôme identiquement nul

$f = 0\ x_1 + \ldots + 0\ x_n \in K[x_1,..., x_n]$ qui admet comme zéros tous les points de l'espace affine IA^n (K) .

□

Exemples d'ensembles algébriques :

1) V = $\{a \in IA^2(IR),\ f(x,y) = x^2 + y^2 = 0\ \} = \{(0,0)\ \}$

2) V = $\{a \in IA^2(C),\ f(x,y) = x^2 + y^2 = 0\ \} = \{(t,it),(t,-it), t \in C\ \}$

Avec les ensembles algébriques de l'espace affine IA^n (K) , nous obtenons une topologie particulière :

Définition 3 :

La topologie de Zariski , sur un espace affine IA^n (K) , est formée par les ensembles algébriques comme fermés et leurs complémentaires comme ouverts.

L'espace affine IA^n (K) et l'ensemble vide ϕ sont les seuls sous ensembles de l'espace affine qui sont des ouverts et des fermés à la fois.

La topologie de Zariski confère à l'espace affine IA^n (K) une structure d'espace topologique.

Définition 4 :

Soit V un sous espace de l'espace topologique IA^n (K).

V est irréductible s'il n'est pas vide et s'il n'est pas la réunion de deux sous espaces disjoints fermés de IA^n (K) .

1.2 Variété Affine :

Définition 5 :

1) Tout sous ensemble fermé et irréductible d'un espace topologique IA^n (K) est une Variété algébrique affine.

2) Tout sous ensemble ouvert d'un espace topologique IA^n (K) est une Variété quasi affine.

3) Toute partie irréductible et fermée d'une Variété algébrique affine d'un espace topologique IA^n (K) est une sous Variété algébrique affine.

Exemple de Variété Affine :

Dans le plan affine IA^2 (K) , tout polynôme f (x , y) irréductible implique la courbe algébrique plane d'équation f(x,y) = 0 qui est donc une Variété Affine.

2. Espace Projectif - Variété Projective :

2.1 L'espace projectif $IP^n(K)$:

Sur l'espace affine $IA^{n+1}(K)$, nous introduisons la relation $\Re$ binaire :

$a = (a_1, \ldots, a_{n+1}) \; \Re \; b = (b_1, \ldots, b_{n+1})$ si et seulement si $a = \lambda b$ pour un certain élément non nul λ du corps K.

Cette relation satisfait les trois axiomes des relations d'équivalence : réflexivité, symétrie et transitivité.

Définition 6 :

L'espace projectif $IP^n(K)$ est l'ensemble quotient $(IA^{n+1}(K) - \{0\}) / \Re$

$IP^n(K) = \{(x_1,...,x_{n+1}), x_i \in K, (x_1,...,x_{n+1}) \neq (0,...,0)\}$.

Exemples d'espaces projectifs **:**

1) L'espace projectif $IP^1(K)$ est l'ensemble des classes des couples

$a = (a_1, a_2)$; $(a_1, a_2) \neq (0,0)$; $cl(1,1) = \{(1,1),(r,r); r \in IR^*\}$

2)L'espace projectif $IP^2(K)$ est l'ensemble des triplets

$(a_1, a_2, a_3) \in IR^3 - \{(0,0,0)\}$.

$cl(1,0,0) = \{(1,0,0),(2,0,0),(-1,0,0),...,(r,0,0); r \in IR^*\}$.

$Cl(0,1,0) = \{(0,1,0),(0,2,0),...,(0,r,0), r \in IR^*\}$, cette classe représente le point à l'infini des cubiques .

Il en résulte que les polynômes associés sont homogènes de degré d = 1,2,…

Définition 7 :

Soit $K[x_1,...,x_{n+1}]$ l'anneau des polynômes à n+1 indéterminées $x_1, \ldots, x_{n+1}$

Un polynôme $f(x_1, \ldots, x_{n+1})$ de cet anneau est :

1) homogène de degré d s'il satisfait la relation :

$$f(t x_1, \ldots, t x_{n+1}) = t^d f(x_1, \ldots, x_{n+1}) \text{ pour } t \in K .$$

2) irréductible s'il n'est pas le produit non trivial de deux polynômes f_1, f_2 de degrés ≥ 1.

Exemples :

1) Dans l'espace projectif $IP^1(IR)$, les polynômes homogènes :

$f_1(x, y) = a x + b y$ et $f_2(x, y) = a x^2 + b x y + c y^2$ sont de degré respectivement d = 1 et d = 2 .

2) Dans l'espace projectif $IP^2(IR)$, les polynômes homogènes :

$f_1(x, y, z) = a x + b y + c z$, $f_2(x, y, z) = a x^3 + b x^2 y + c x y^2 + e z^3$ et $f_3(x, y, z) = 3 x^3 y^2 + 4 x y z^3$ sont de degré respectivement d = 1 , d = 3 et d = 5 .

La topologie de Zariski appliquée à l'espace affine $IA^n(K)$ s'applique aussi à l'espace projectif $IP^n(K)$.

Définition 8 :

Un sous ensemble V d'un espace projectif $IP^n(K)$ est algébrique s'il est l'ensemble U (f) des zéros communs d'une famille de polynômes homogènes de l'anneau $K[x_1, ..., x_{n+1}]$.

Exemple :

Le sous ensemble

$V = \{ (x, y, z) \in IP^2(IR) ; f(x, y, z) = y^2 z - x^3 + x^2 z + z^3 = 0 \}$ est un ensemble algébrique.

2.2 Variété Projective :

Définition 9:

1) Une Variété projective de l'espace $IP^n(K)$ est un sous ensemble algébrique irréductible de l'espace Projectif $IP^n(K)$.

2) Une Variété quasi projective est un sous ensemble ouvert d'une Variété projective.

Il existe des relations entre les coordonnées affines et les coordonnées projectives des points et des polynômes :

2.3 Passage de l'espace affine $IA^n(K)$ à l'espace projectif $IP^n(K)$:

Soit une application $u : IA^n(K) \rightarrow IA^n(K)$

$$f(x_1, \ldots, x_n) \rightarrow f\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) \text{ pour } x_{n+1} \neq 0$$

suivie de l'application : multiplication par x^d_{n+1} , où d = degré du polynôme $f(x_1, \ldots, x_n)$.

$$IA^n(K) \rightarrow IP^n(K)$$

$$f\left(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}\right) \rightarrow x^d_{n+1} f = g(x_1, \ldots, x_{n+1})$$

Exemple :

$f(x, y) = 3x^3y - 2x^2 + 4y + 5$ = polynôme affine de degré 4.

L'application $: (x, y) \rightarrow \left(\frac{x}{z}, \frac{y}{z}\right)$; $z \neq 0$, implique

$f\left(\frac{x}{z}, \frac{y}{z}\right) = 3\frac{x^3y}{z^4} - 2\frac{x^2}{z^2} + 4\frac{y}{z} + 5$, la multiplication par z^4 implique :

$z^4 f\left(\frac{x}{z}, \frac{y}{z}\right) = 3x^3y - 2x^2z^2 + 4yz^3 + 5z^4 = g(x, y, z) \in IP^2(IR)$

2.4 Passage de l'espace projectif $IP^n(K)$ à l'espace affine $IA^n(K)$:

Avec l'application : $f(x_1, \ldots, x_n, x_{n+1}) \rightarrow f(x_1, \ldots, x_n, 1)$

Exemple :

$f(x, y, z) = 2x^7y + 3x^5yz^2 - x^2y^2z^4 + 6z^8 \in IP^2(IR)$.

Pour $z = 1$ j'obtiens le polynôme affine :

$f(x, y, 1) = 2x^7y + 3x^5y - x^2y^2 + 6 = = g(x, y) \in IA^2(IR)$.

3. Variété Abélienne :

Définition 10 :

Soit X une Variété Algébrique Projective, munie d'une loi additive :

$$u : X^2 \rightarrow X : u(a, b) = a + b$$

X est une Variété Abélienne si les conditions suivantes sont satisfaites :

1) X a une structure de groupe abélien .

2) L'application u (a , b) = a + b et

l'application inverse v : X $\rightarrow$ *X : v(a) =* a^{-1} *est un morphisme de Variétés.*

Selon Shafarevich [17], les Courbes Elliptiques sont les seuls exemples de Variétés Abéliennes.

Exemple :

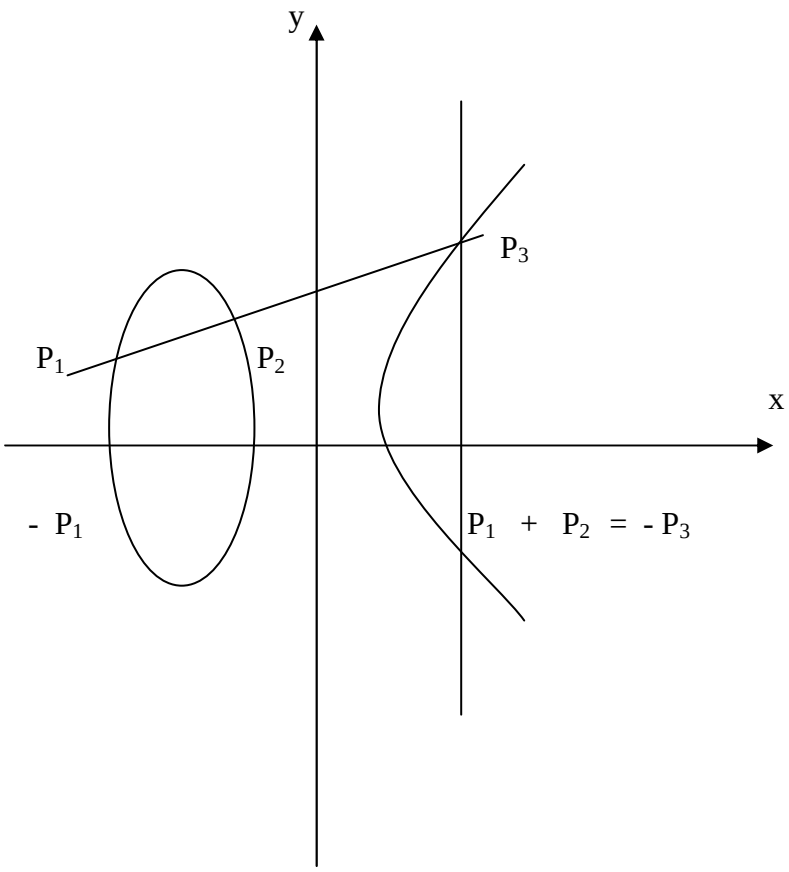
Soit X une courbe Elliptique d'élément neutre $O_X = (0, 1, 0)$.

Son équation de Weierstrass dans le plan projectif $IP^2(K)$ est :

$$y^2z + a_1 xyz + a_3 yz^2 = x^3 + a_2 x^2z + a_4 xz^2 + a_6 z^3$$

La loi de groupe additif abélien est basée sur la règle géométrique de 3 points colinéaires de la courbe X :

$$P_1 + P_2 + P_3 = O_X \qquad (1)$$



Les morphismes $u : X^2 \rightarrow X$ et $v : X \rightarrow X$

ont pour images :

$$u(P_1, P_2) = P_1 + P_2 \quad \text{et} \quad v(P_1) = -P_1$$

La somme $P_1 + P_2$ et le symétrique $-P_1$ sont obtenus par la relation (1) :

$$P_1 + P_2 = -P_3 \quad \text{et} \quad P_1 + (-P_1) = O_X$$

Chapitre II :Courbes Algébriques Planes -Cubiques de Weierstrass

En géométrie analytique l'étude des courbes algébriques et leur classification ont été initiées par Descartes et Newton. Au 19 ième siècle, avec Plucker en particulier, ces courbes furent étudiées d'un point de vue projectif.
Les cubiques de Weierstrass forment un sous ensemble particulier de l'ensemble des courbes algébriques planes.

1. Courbes algébriques planes :

Définition 1 :

Une courbe algébrique plane est l'ensemble des points $P = (x, y)$ *de l'espace euclidien réel à 2 dimensions qui satisfont l'équation affine* $f(x, y) = 0$ *où*

$$f(x, y) = \sum_{i,j \geq 0} c_{ij} x^i y^j \in IR[x, y]$$

Son degré n est égal au degré maximal $i + j$ *des monômes* $x^i y^j$.

Ces courbes algébriques C : f (x , y) = 0 sont classifiées par le degré n de f (x , y)

2. Classification des Courbes Algébriques planes selon leur degré :

Pour n = 1 , ce sont les droites : f (x , y) = a x + by + c = 0

Pour n = 2, les courbes sont des coniques qui sont les intersections d'un cône avec un plan, elles se répartissent en trois familles selon leurs équations :

1) Les cercles de centre (a , b) et de rayon r : $(x - a)^2 + (y - b)^2 = r^2$

2) Les paraboles : $y^2 = a x + b$, $a \neq 0$

3) Les hyperboles : $\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$, $a \neq 0$ et $b \neq 0$

4) Les ellipses : $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$, $a \neq 0$ et $b \neq 0$

Une courbe algébrique plane de degré 2 peut être dégénérée en un produit de 2 droites : $f(x, y) = (a_0 x + a_1 y + a_2)(a_3 x + a_4 y + a_5) = 0$.

Pour n = 3 , les courbes sont des cubiques : $f(x, y) = f_0 + f_1 + f_2 + f_3 = 0$

où les f_i sont des polynômes homogènes de degré i = 0 , 1 , 2 , 3 .

Une cubique peut être dégénérée :

- en un produit d'une conique par une droite :

$f(x, y) = (a_0 x + a_1 y + a_2)(a_3 x^2 + a_4 y^2 + a_5 x y + a_6 x + a_7 y + a_8) = 0$ ou

- en un produit de trois droites :

$f(x, y) = (a_0 x + a_1 y + a_2)(a_3 x + a_4 y + a_5)(a_6 x + a_7 y + a_8) = 0$.

Pour n = 4 les courbes sont des quartiques.

Pour n = 5 les courbes sont des quintiques…etc.

Exemples de courbes algébriques planes :

1)La courbe d'équation $x^3 - 3y + y^3 = 0$ est une cubique.

Cette courbe algébrique admet un point singulier qui est un nœud au point (0 ,0) ; la courbe admet 2 tangentes distinctes en ce point.

2)l'équation : $x^3 + 2y^2 + x^2 y^2 + x y - 5 = 0$ définit une quartique.

Une courbe algébrique admet plusieurs types de points : points ordinaires, points d'inflexion, points singuliers (nœuds, points de rebroussement).

3. Singularités d'une courbe algébrique plane :

Soit une courbe algébrique C d'équation $f(x, y) = 0$, alors les types de ses points sont décrits dans la :

Définition 2 :

Soit une courbe algébrique C d'équation $f(x, y) = 0$ et un point P sur C ; alors :

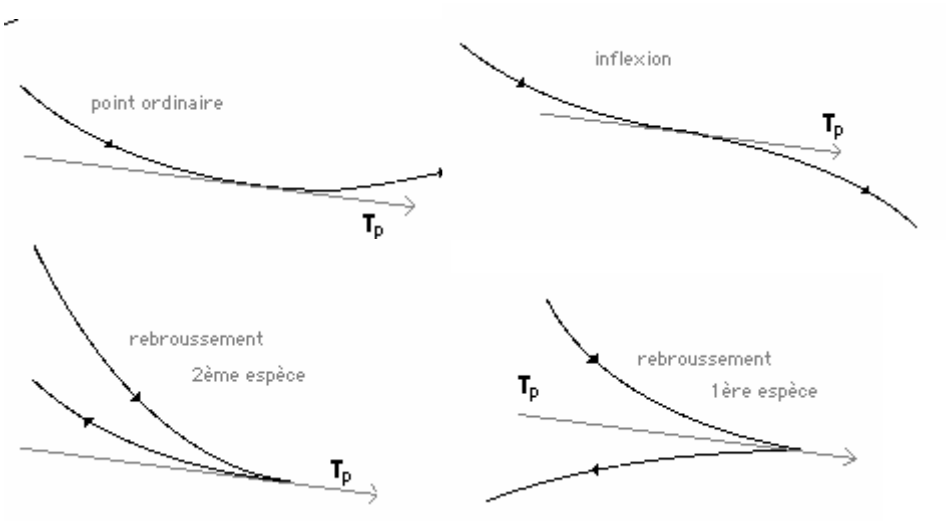
(1)P est ordinaire si C admet en ce point une tangente unique qui ne traverse pas C dans un voisinage de P

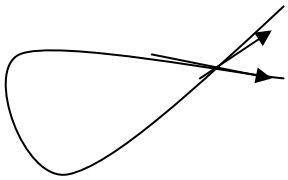
(2) P est un point d'inflexion si C admet en ce point une tangente unique qui traverse C dans un voisinage de P.

(3) P est un nœud si C admet en ce point deux tangentes distinctes.

(4) P est un point de rebroussement si C admet en ce point deux tangentes confondues.

Les 5 types de points :





Nœud

La proposition suivante permet de calculer les points singuliers :

Proposition1 :

Soit une courbe algébrique C plane d'équation f (x , y) = 0.

Alors , un point S de C est singulier si les dérivées partielles de f s'annulent en S :

$$\mathbf{f(S) = f_x'(S) = f_y'(S) = 0}$$

Une courbe algébrique C de degré n est singulière si elle admet des points singuliers ; elle est non singulière sinon.

Preuve avec la formule de Taylor :

$$F(x_0 + h, y_0 + l) = f(x_0, y_0) + h f_x' + l f_y' + \frac{h^2}{2} f''^2_x + \frac{l^2}{2} f''^2_y + \ldots.$$

□

Exemple : Soit la courbe C : $f(x, y) = x^3 - 5x^2 + y^3 = 0$

$f_x' = 3x^2 - 10x$; $f_y' = 3y^2$;

Le système $f(S) = f_x'(S) = f_y'(S) = 0$ admet la solution $S = (0, 0)$, donc S est un point singulier ; la pente des tangentes à C en ce point est calculée par les formules :

$$y^3 = -x^3 + 5x^2 ; \quad 3y^2 y' = -3x^2 + 10x \; ; \; y' = \frac{-3x^2 + 10x}{3y^2}$$

$$y = \sqrt[3]{-x^3 + 5x^2}$$

4. **Genre d'une courbe algébrique :**

Le nombre s de points singuliers S d'une courbe algébrique C permet de définir le genre g (C) de cette courbe , c'est un invariant des courbes C qui permet de les classifier.

Définition 3:

Le genre d'une courbe algébrique C de degré n qui possède s (comptés avec leurs multiplicités) points singuliers est l'entier positif ou nul :

$$g(C) = \frac{1}{2}(n-1)(n-2) - s$$

Exemples de genre pour n = 3 et 4

Les courbes algébriques de degré $n \leq 2$ ont un genre $g(C) = 0$.

Pour n = 3 , les cubiques C ayant un point singulier ont un genre égal à :

$$g(C) = \frac{1}{2}(3-1)(3-2) - 1 = 0$$

Une cubique singulière admet un point double ou triple .

Les cubiques C n'ayant pas de point singulier ont un genre égal à :

$$g(C) = \frac{1}{2}(3-1)(3-2) = 1$$

Pour n = 4 , une quartique non singulière C a un genre égal à :

$$g(C) = \frac{1}{2}(4-1)(4-2) = 3$$

Une quartique C ayant un point singulier a un genre égal à :

$$g(C) = \frac{1}{2}(4-1)(4-2)-1=2$$

Une quartique C ayant 2 points singuliers a un genre égal à :

$$g(C) = \frac{1}{2}(4-1)(4-2)-2=1$$

Parmi les courbes algébriques planes , il y a les cubiques de Weierstrass.

Nous nous intéressons à ces cubiques de Weierstrass.

5. Cubiques de Weierstrass :

Définition 4 :

Soit K un corps commutatif global, local ou fini.

Une cubique de Weierstrass est une courbe algébrique plane C , irréductible d'équation spécifique :

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

Les deux variables x et y appartiennent à une clôture algébrique K^{alg} du corps K.

Définition 5 :

L'équation (1) est l'équation de Weierstrass de la cubique C.

Les cubiques de Weierstrass se répartissent en deux classes :

Les cubiques de Weierstrass singulières et les cubiques de Weierstrass non singulières

Définition 6 :

Une Courbe Elliptique est une cubique de Weierstrass non singulière d'équation de Weierstrass :

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

La nature du corps K permet de choisir les outils mathématiques pour étudier la Courbe Elliptique.

Lorsque le corps K est un corps de nombres algébriques ;nous appliquons à la Courbe Elliptique E la Théorie des Nombres (les entiers ,les unités, les idéaux,les discriminants,la ramification,les valuations , l'analyse p-adique , les fonctions arithmétiques. .etc…).

Lorsque le corps K est le corps des nombres complexes,nous appliquons à la Courbe Elliptique E l'Analyse Complexe (les réseaux , les fonctions elliptiques,les fonctions et les formes modulaires , la série L (E , s) de Dirichlet Hasse …etc..) et la Géométrie Algébrique (les variétés,les diviseurs , la cohomologie ,les courbes algébriques projectives..etc..) .

Lorsque le corps K est un corps fini ; nous appliquons à la Courbe Elliptique E la théorie des corps finis (la cryptographie,le codage,la recherche des facteurs premiers des très grands nombres...etc..).

6. Transformations de l'équation de Weierstrass :

Avec des changements linéaires convenables des deux variables x et y , nous obtenons des transformations de l'équation de Weierstrass :

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

1) Lorsque la caractéristique du corps K est $\neq 2$,le changement linéaire de variables :

$$(x , y) \ \rightarrow (X , \ \frac{Y - a_1 X - a_3}{2}) \qquad (2)$$

permet d'éliminer les monômes en x y et en y et transforme l'équation (2) en l' équation

$$E_1 : \ Y^2 \ = X^3 + b_2 X^2 + 4 b_4 X + b_6 \in K[x, y] \qquad (3)$$

Les coefficients b_{2i} sont des polynômes '' homogènes de degré 2i ''de

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

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

2) Lorsque la caractéristique du corps K est $\neq 2 , 3$, le changement linéaire de variables :

$$(X, Y) \ \rightarrow \quad (\frac{x - 3b_2}{36}, \frac{y}{108}) \qquad (5)$$

permet d'éliminer le coefficient 4 et le monôme en X^2 et transforme l'équation (3) en l'équation :

$$E_2 : \ y^2 \ = x^3 - 27 c_4 x - 54 c_6 \in K[x, y] \qquad (6)$$

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

$$c_4 = b_2^2 - 24\, b_4 \;; \qquad c_6 = -\, b_2^3 + 36\, b_2 b_4 - 216 \quad b_6 \qquad (7)$$

Il existe d'autres modèles de cubiques de Weierstrass:

Le modèle de Tate : $E : y^2 + x\,y = x^3 + a\,x + b$ où a et b sont des séries de puissances formelles en $q = \exp(2\pi i z)$, $z \in C$, et égales à :

$$a = -\,5 \sum_{n\geq 1} n^3 q^n (1-q^n)^{-1} \quad \text{et}$$

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

Le modèle de Legendre : $E : y^2 = x\,(x-1)\,(x-\lambda) \in K[x,y]$, pour $\lambda \neq 0$, 1.

Le modèle de Deuring : $E : y^2 + a\,x\,y + y = x^3 \in K[x,y]$; $a^3 \neq 3$

La Cubique de Weierstrass utilisée en cryptographie :

$E : y^2 = x^3 + A\,x + B \in Q[x,y]$ et $4\,A^3 + 27\,B^2 \neq 0$

Les coefficients b_{2i} et c_{2i} permettent d'introduire des invariants.

7. Invariants des cubiques de Weierstrass :

Les invariants des cubiques de Weierstrass sont des fonctions des coefficients des équations de ces cubiques ; ils prennent différentes valeurs et sont utilisés dans des classifications de ces cubiques.

Toute cubique de Weierstrass possède plusieurs invariants : un discriminant, un invariant modulaire, un invariant différentiel, un rang, …etc.

Définition 7 :

Le discriminant d'une Cubique de Weierstrass E est le polynôme

'' homogène de degré 12'' égal à :

$$\Delta\,(E) = 9\, b_2 b_4 b_6 - 8\, b_4^3 - 27 b_6^2 - b_2^2 b_8 \in Z[b_2, b_4, b_6, b_8] \qquad (8)$$

et $\quad 4\, b_8 = b_2 b_6 - b_4^2$ *pour carac (K)* $\neq 2,3 \qquad (9)$

L'invariant discriminant et le coefficient c_4 permettent d'introduire l'invariant modulaire :

Définition 8 :

L' invariant modulaire d'une cubique de Weierstrass E est l'élément du corps K égal à :

$$J(E) = \frac{c_4^{\,3}}{\Delta(E)} \quad pour \ \ carac\,(K) \neq 2,3 \qquad (10)$$

La différentielle df de la fonction f : $df(x,y) = f_x' \, dx + f_y' \, dy$,

$$\text{où} \qquad f_x' = \frac{\partial f}{\partial x} \quad \text{et} \quad f_y' = \frac{\partial f}{\partial y} \qquad (11)$$

désignent les dérivées partielles d'ordre 1 de f , permet d'obtenir l'invariant différentiel de la cubique de Weierstrass d'équation (1) :

Définition 9 :

L'invariant différentiel d'une cubique de Weierstrass E est l'élément différentiel :

$$\omega(E) = \frac{dx}{f_y'} = -\frac{dy}{f_x'} \qquad (12)$$

avec : $f_x' = -3x^2 - 2a_2 x - a_4 + a_1 y$ *et* $f_y' = 2y + a_1 x + a_3$.

Exemple de calcul des invariants de la Cubique de Weierstrass :

E : $y^2 + 3xy - 2y = x^3 + x^2 - 5x + 1 \in Q[x,y]$:

Avec les formules (4) , (8) et (9) et le calcul nous trouvons :

$b_2 = 13$; $b_4 = -16$; $b_6 = 8$; $b_8 = -38$ et $\Delta(E) = 22486$ (13)

Avec les formules (7) ,(10) , le résultat (13) et le calcul nous trouvons :

$c_4 = 553$ et $j(E) = \frac{553^3}{22486}$.

Avec la formule (11) , (12) et le calcul , nous trouvons :

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

Il existe d'autres invariants d'une Courbe Elliptique : un conducteur, un régulateur, une série de Dirichlet-Hasse-Weil , etc.…

Chacun des invariants permet une classification des Cubiques de Weierstrass**.**

8. Classification des Cubiques de Weierstrass par leurs discriminants :

Le discriminant Δ (E) d'une Cubique de Weierstrass $y^2 = f(x)$ est lié au discriminant dis(f) du polynôme f(x) $\in K[x]$:

8.1 Discriminant d'un polynôme f(x) $\in K[x]$

La théorie du discriminant d'un polynôme se trouve dans « Algèbra » de Lang [10] et dans « introduction à l'Algèbre » de Kostrikin [9] , etc.…

Soit K un corps global , local ou fini.

L'équation de Weierstrass d'une cubique peut se mettre sous la forme :

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

Tout polynôme $f(x) = d_0x^n + d_1x^{n-1} + \ldots + d_n \in K[x]$ de degré n se factorise sous la forme : $f(x) = d_0(x - \alpha_1) (x - \alpha_2)\ldots(x - \alpha_n) \in K[x]$, α_i appartenant à une clôture algébrique K^{alg} de K.

Définition 10 :

Le discriminant d'un polynôme f(x) est l'élément dis(f) du corps K égal à :

$$dis(f) = d_0^{2n-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \qquad (14)$$

C'est une fonction symétrique quadratique de ses racines α_i .

Les fonctions symétriques élémentaires de ces racines sont des sommes S_i de produits de t racines , t = 1,..,n :

$$S_1 = \sum_{i=1}^{n} \alpha_i = \frac{-d_1}{d_0}, S_2 = \alpha_1\alpha_2 + \ldots + \alpha_{n-1}\alpha_n = \frac{d_2}{d_0}, \ldots, S_n = \prod_{i=1}^{n} \alpha_i = (-1)^n \frac{d_n}{d_0}$$

Exemple : $f(x) = 3x^2 - 27$; le discriminant de f (x) est égal à :

$dis(f) = 3^{(2.2-2)} (3 - (- 3))^2 = 9 . 36 = 324$

La formule (14) implique la :

Proposition 1 :

Le discriminant d'un polynôme f(x) $\in K[x]$ de degré n ≥ 2 est nul si et seulement si ce polynôme admet deux racines égales.

Preuve de « discriminant de f(x) est nul» implique « f(x) admet deux racines égales ».

La formule $dis(f) = d_0^{2n-2} \Pi (\alpha_i - \alpha_j)^2 = 0$ implique $(\alpha_i - \alpha_j) = 0$ pour un certain facteur $(\alpha_i - \alpha_j)$; il en résulte que f(x) admet au moins 2 racines égales $\alpha_i = \alpha_j$.

Preuve de « f(x) admet deux racines égales » implique le «discriminant de f(x) est nul ».

f(x) admet 2 racines égales $\alpha_i = \alpha_j$, ceci implique $dis(f) = d_0^{2n-2} \Pi (\alpha_i - \alpha_j)^2 = 0$.

□

Selon Harvey – Cohn [3],le discriminant dis(f) se calcule à l'aide d un déterminant :

Proposition 2 :

Soit un polynôme unitaire f(x) de degré n ≥ 2 ;

$$\mathbf{f(x) = x^n + d_1 x^{n-1} + ... + d_n = (x - \alpha_0) ....(x - \alpha_{n-1}) \in K[x]}$$

Les α_i sont dans une clôture algébrique K^{alg} de K ,

Alors son discriminant dis(f) est égal au déterminant symétrique d'ordre n :

$$\mathbf{dis\ (f)} = \begin{vmatrix} \sigma_0 & \sigma_1 & ..... & \sigma_{n-2} & \sigma_{n-1} \\ \sigma_1 & \sigma_2 & & & \\ & & & & \\ \sigma_{n-2} & & & & \\ \sigma_{n-1} & & ..... & & \sigma_{2n-2} \end{vmatrix}$$

Les éléments $\sigma_m = \sum_{i=1}^{n} (\alpha_i)^m$ sont des sommes de puissances des racines ; ce sont donc des fonctions symétriques non élémentaires des racines, qui sont des polynômes de l'anneau $Z[d_1,.....,d_n]$:

$\sigma_0 = n$, $\sigma_1 = - d_1$, $\sigma_2 = d_1^2 - 2 d_2$, $\sigma_3 = 3 d_1 d_2 - d_1^3 - 3 d_3$, …,

$\sigma_m = - m d_m - \sigma_1 d_{m-1} - .... - \sigma_{m-1} d_1$ et $\sigma_m = 0$ pour $m > n$

Exemple : soit le polynôme $f(x) = x^3 - x = x(x - 1)(x + 1)$,nous avons :

$d_1 = 0$, $d_2 = - 1$, $d_3 = 0$, $d_4 = 0$, $\sigma_0 = n = 3$, $\sigma_1 = - d_1 = 0$, $\sigma_2 = d_1^2 - 2 d_2 = 2$,

$\sigma_3 = 3 d_1 d_2 - d_1^3 - 3 d_3 = 0$, $\sigma_4 = - 4d_4 - \sigma_1 d_3 - \sigma_2 d_2 - \sigma_3 d_1 = - 2 (- 1) = 2$.

Nous avons alors :

$$\text{dis}(f) = \begin{vmatrix} 3 & 0 & 2 \\ 0 & 2 & 0 \\ 2 & 0 & 2 \end{vmatrix} = 3(4) + 2(-4) = 4$$

Le discriminant d'un polynôme f(x) peut être aussi calculé avec la théorie du résultant de deux polynômes :

8-2 Résultant de deux polynômes :

Le résultant est une notion qui s'applique à deux polynômes f et g d'un anneau $K[x]$; c'est un scalaire qui permet de vérifier s'ils possèdent des facteurs communs.

Il peut être calculé à partir des coefficients des 2 polynômes à l'aide d'un déterminant , il peut être aussi obtenu à partir des racines de ces polynômes.

Définition 11 :

Soit l'anneau des polynômes $K[x]$ *et 2 polynômes* $f(x) = \sum_{i=0}^{s} c_i x^{s-i}$

d'ordre s et $g(x) = \sum_{i=0}^{t} d_i x^{t-i}$ *d'ordre t .*

Le résultant des deux polynômes f et g est le déterminant d'ordre s + t :

$$\text{Res}(f, g) = \begin{vmatrix} c_0 & c_1 & \dots & \dots & \dots & c_s & & & & \\ 0 & c_0 & c_1 & \dots & \dots & \dots & c_s & & & \\ & & & & & & & & & \\ & & & & & & & & & \\ 0 & \dots & \dots & \dots & c_0 & c_1 & & & & c_s \\ d_0 & d_1 & \dots & \dots & \dots & d_t & & & & \\ & & & & & \dots & d_t & & & \\ & & & & & & \dots & d_t & & \\ & & & & & & & \dots & d_t & \\ & & & & & & & & \dots & d_t \end{vmatrix} \qquad (15)$$

La diagonale principale est formée de t coefficients c_0 de f (x) et de s coefficients d_t de g (x) .

Les termes qui manquent sont remplacés par des zéros.

Le résultant de deux polynômes f et g s'exprime aussi au moyen des racines de ces polynômes :

Proposition 3 :

Soit 2 polynômes f (x) = c_0 (x – α_1)….(x – α_s) et g(x) = d_0 (x – β_1) ..(x – β_t)

Alors leur résultant est donné par les formules :

1) Res (f , g) = $c_0^t \prod_{i=1}^{s} g(\alpha_i) = (-1)^{st} d_0^s \prod_{i=1}^{t} f(\beta_i)$ **(16)**

2) Res (f , g) = $c_0^t d_0^s \prod_{i=1}^{s} \prod_{j=1}^{t} (\alpha_i - \beta_j)$

La formule (16) de la proposition précédente implique le :

Corollaire 1 :

Le résultant Res (f , g) de deux polynômes f (x) et g(x) est nul si et seulement si ces deux polynômes ont une racine commune $\alpha_i = \beta_j$ pour certains indices i et j.

Preuve :

L' hypothèse Res (f , g) = 0 et la relation (16) impliquent α_i est racine de g(x) et $\alpha_i = \beta_j$ pour certains indices i , j , donc f(x) et g(x) ont une racine commune.

□

Examinons le cas particulier g(x) = f ' (x) = dérivée de f (x).

Proposition 4 :

Le résultant Res (f , f') d'un polynôme f(x) et de sa dérivée f ' (x) est égal à :

$$\text{Res}(f, f') = c_0^{s-1} \prod_{i=1}^{s} f'(\alpha_i) \qquad (18)$$

Ce résultant est lié au discriminant Dis(f) du polynôme f(x) par la relation :

$$\text{dis}(f) = c_0^{2s-2} \prod_{i<j} (\alpha_i - \alpha_j)^2 \quad \text{et} \quad \text{dis}(f) = (-1)^{\frac{n(n-1)}{2}} c_0^{-1} . \text{Res}(f, f') \qquad (19)$$

Exemple 1 :

Soit $f(x) = 3x^2 - 27$; $f'(x) = 6x$, la formule (18) et le calcul impliquent :

$Res(f, f') = 3^{2-1}.\ 6\ (3).6(-3) = -972$. La formule (19) et le calcul impliquent :

$dis(f) = 3^{(2.2-2)}(3 - (-3))^2 = 9.\ 36 = 324$ et $dis(f) = (-1)^{2(2-1)/2}\ 3^{-1}(-972) = 324$

calcul du résultant de f et f' par le déterminant :

$$Res(f,f') = \begin{matrix} 3 & 0 & -27 \\ 6 & 0 & 0 \\ 0 & 6 & 0 \end{matrix} = (-27).\ 6^2 = -972$$

Exemple 2 :

$f(x) = x^3 + x^2 + 3x - 5$

Alors $f'(x) = 3x^2 + 2x + 3$; le résultant est le déterminant d'ordre 3 + 2 = 5

$$Res(f, f') = \begin{vmatrix} 1 & 1 & 3 & -5 & 0 \\ 0 & 1 & 1 & 3 & -5 \\ 3 & 2 & 3 & 0 & 0 \\ 0 & 3 & 2 & 3 & 0 \\ 0 & 0 & 3 & 2 & 3 \end{vmatrix}$$

Avec les calculs j'obtiens $Res(f, f') = 702$.

Le discriminant $\Delta(E)$ d'une Cubique de Weierstrass $E : y^2 = f(x) \in K[x]$ est lié au discriminant dis(f) du polynôme f(x) .

Proposition 5 :

Soit une Cubique de Weierstrass $E : y^2 = f(x) \in K[x]$; alors les discriminants $\Delta(E)$ de E et dis(f) de f satisfont :

1) $\Delta(E) = 16\ dis(f)$ lorsque $f(x) = x^3 + Ax + B \in K[x]$

2) $\Delta(E) = 16\ dis(f)$ lorsque $f(x) = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x]$

3) $16\ \Delta(E) = dis(f)$ lorsque $f(x) = 4x^3 + b_2 x^2 + 2\ b_4 x + b_6 \in K[x]$

Preuve :

1) $\Delta (E) = 16 \, dis(f)$ lorsque $f(x) = \mathbf{x}^3 + A x + B$;

Avec le calcul de $f'(x)$ et les formules (15) et (19) nous obtenons :

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

Avec les formules (4) ,(8) et (9) et le calcul j'obtiens : $\Delta (E) = - 16 (4A^3 + 27 B^2)$

Il en résulte la relation : $\Delta (E) = 16 \, dis(f)$.

2) $\Delta (E) = 16 \, dis(f)$ lorsque $f(x) = x^3 + a_2 x^2 + a_4 x + a_6$;

Avec le calcul de $f '(x)$ et les formules (15) et (19) nous obtenons :

$dis (f) = 18 a_2 a_4 a_6 – 4 a_4^3 – 27 a_6^2 – a_2^3 a_6 + a_4^3$.

Avec les formules (4) , (8) et (9) nous obtenons :

$\Delta (E) = 16 (18 a_2 a_4 a_6 – 4 a_4^3 – 27 a_6^2 – a_2^3 a_6 + a_4^3)$

Il en résulte la relation : $\Delta (E) = 16 \, dis(f)$

3) $16 \Delta (E) = dis(f)$ $f (x) = 4 x^3 + b_2 x^2 + 2 b_4 x + b_6$;

avec le calcul de $f '(x)$ et les formules (15) et (19) nous obtenons :

$dis (f) = 16 (9 b_2 b_4 b_6 - 8 b_4^3 – 27 b_6^2 – b_2^2 b_8)$

avec les formules (8) et (9) nous obtenons :

$\Delta (E) = 9 b_2 b_4 b_6 - 8 b_4^3 – 27 b_6^2 – b_2^2 b_8$

il en résulte la relation : $16 \Delta (E) = dis(f)$

Les Cubiques de Weierstrass peuvent être classifiées par leur discriminant $\Delta(E)$ et leur invariant $c_4 (E)$:

8.3 Classifications des Cubiques de Weierstrass par leur discriminant $\Delta (E)$ et leur invariant $c_4 (E)$.

Proposition 6 :

Soit une Cubique de Weierstrass E d'invariants $\Delta (E)$ et $c_4 (E)$,

1) la Cubique est singulière si et seulement si $\Delta (E) = 0$

2) la Cubique admet un nœud si et seulement si $\Delta (E) = 0$ et $c_4 (E) \neq 0$.

3) la Cubique admet un point de rebroussement si et seulement si $\Delta (E) = 0$ et $c_4 (E) = 0$.

Preuve de 1):

- ‘‘ la Cubique est singulière’’ implique ‘‘ $\Delta (E) = 0$ ’’

Par définition les coordonnées du point singulier de la Cubique singulière satisfont le système : $f (x , y)) = f ' (x) = f ' (y) = 0$ donc f et $f '$ ont une racine commune,

Le corollaire (1) implique la valeur $Res (f , f ') = 0$,

La formule (19) et la proposition (5) impliquent $\Delta (E) = 0$.

- ‘‘ $\Delta (E) = 0$ ’’implique ‘‘ la Cubique C est singulière ’’

La valeur $\Delta (E) = 0$, la proposition (5) et la formule (19) impliquent que f et $f '$ ont une racine commune , donc il existe un point S de la Cubique qui satisfait $f (x , y)) = f ' (x) = f ' (y) = 0$; donc la Cubique est singulière .

Preuve de 2):

- ‘‘ la Cubique admet un nœud ’’ implique ‘‘ $\Delta (E) = 0$ et $c_4 (E) \neq 0$ ’’

Soit une cubique de Weierstrass $E : y^2 = x^3 - 27 c_4 x - 54 c_6 \in K [x, y]$

L’hypothèse ‘‘ la Cubique admet un nœud ’’implique qu’elle est singulière ,

donc $\Delta (E) = 0$.

En ce point la Cubique admet 2 tangentes distinctes dont les pentes sont égales à :

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

il en résulte que le polynôme $N (x)$ qui admet 2 racines distinctes a un discriminant : $dis (N (x)) = 144 c_4 \neq 0$

il en résulte : $c_4 \neq 0$

Preuve de 3) :

- ‘‘ la Cubique admet un point de rebroussement’’ implique ‘‘ $\Delta (E) = 0$ et $c_4 (E) = 0$ ’’

L’hypothèse ‘‘ la Cubique admet un point de rebroussement ’’implique qu’elle est singulière , donc $\Delta (E) = 0$

Par définition , en un point de rebroussement la Cubique admet 2 tangentes confondues .cela implique que le polynôme $N (x)$ admet une racine double donc $dis (N (x)) = 0$ et par suite $c_4 = 0$.

□

Exemple 1 : Cubique singulière qui admet un nœud

Soit la Cubique de Weierstrass

$$C_1 : y^2 = x^3 - 3x^2 + 4 \in \mathrm{IR}[x, y]$$

Avec le calcul j'obtiens les invariants :

$b_2 = -12$; $b_4 = 0$; $b_6 = 16$; $b_8 = -48$; $\Delta(C_1) = 0$ et $c_4(C_1) = 144$

$\Delta(C_1) = 0$ et $c_4(C_1) \neq 0$ et la proposition (6) impliquent que la Cubique singulière admet un nœud .

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

$F(x, y) = y^2 - x^3 + 3x^2 - 4 = 0$;

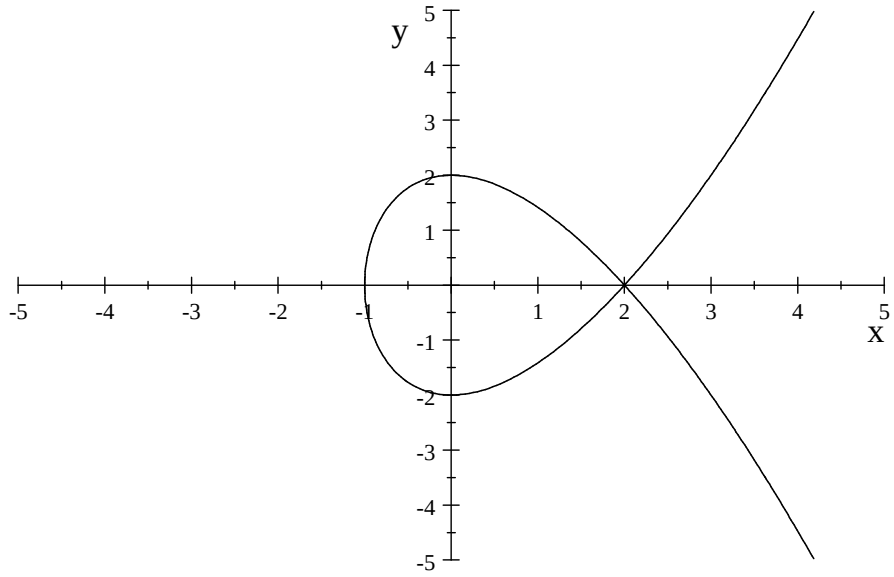
$f_x'(x, y) = -3x^2 + 6x = 0$;

$f_y'(x, y) = 2y = 0$;

J'obtiens la solution (2 , 0) .Pour construire la Cubique C_1 j'utilise le :

Tableau de valeurs des coordonnées de quelques points :

X	- 2	- 1	0	1	2	3
Y	Pas de racine réelle	0	- 2 et 2	$-\sqrt{2}$ et $\sqrt{2}$	0	-2 et 2



$C_1 : y^2 = x^3 - 3x^2 + 4$

Exemple 2 : Cubique singulière qui admet un point de rebroussement

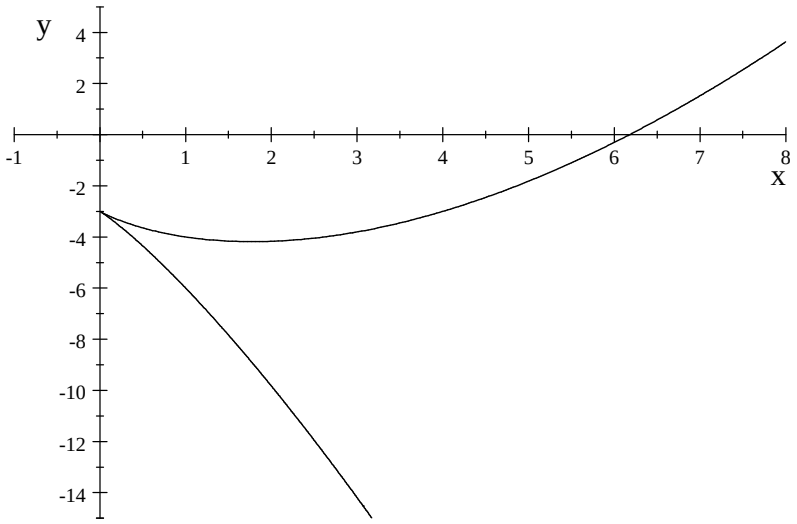
Soit la Cubique de Weierstrass d'équation :

$$C_2 : y^2 + 4xy + 6y = x^3 - 4x^2 - 12x - 9 \in \mathbb{R}[x, y]$$

Avec le calcul j'obtiens les invariants

$B_2 = 0$, $b_4 = 0$, $b_6 = 0$, $b_8 = 0$, $c_4 = 0$, $\Delta(C_1) = 0$

$\Delta(C_2) = 0$ et $c_4 = 0$ et la proposition (6) impliquent C_2 admet un point de rebroussement de coordonnées R (0 , - 3)



$$C_2 : y^2 + 4xy + 6y = x^3 - 4x^2 - 12x - 9$$

Maintenant nous allons étudier les Cubiques de Weierstrass non singulières.

9. Courbes Elliptiques :

Une Courbe Elliptique E est une Cubique de Weierstrass de discriminant $\Delta(E) \neq 0$. le signe de ce discriminant permet leur classification :

9.1 Classification des Courbes Elliptiques suivant le signe de leur discriminant :

Proposition 7 :

Soit une Courbe Elliptique E de discriminant $\Delta(E)$:

1) la Courbe E coupe l'axe Ox en 3 points simples si et seulement si $\Delta(E) > 0$;

2)la Courbe E coupe l'axe Ox en un seul point simple si et seulement si $\Delta(E) < 0$.

Preuve de : ‘‘ E coupe l’axe Ox en 3 points ’’ implique‘‘Δ (E) > 0 ’’

Soit une Courbe Elliptique E coupant l’axe Ox en 3 points simples $P_1 = (e_1 , 0)$, $P_2 = (e_2 , 0)$, $P_3 = (e_3 , 0)$ alors l’équation de Weierstrass de E est de la forme :

$$y^2 = (x - e_1) (x - e_2) (x - e_3) = f (x) \in R[x]$$

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

$$\text{Dis} (f) = \prod_{1 \le i, j \le 3} (e_i - e_j)^2$$

Comme les 3 racines e_i sont réelles , le produit des carrés $(e_i - e_j)^2$ est positif d’où :

$$\text{dis} (f) > 0 . \qquad (20)$$

la relation entre le discriminant Δ (E) et le discriminant du polynôme f (x) , la formule (20) et l’hypothèse $\Delta (E) \neq 0$ impliquent $\Delta (E) > 0$.

Preuve de : ‘‘E coupe l’axe Ox en un seul point simple ’’implique ‘‘Δ (E) < 0 ’’.

Soit une Courbe Elliptique E coupant l’axe Ox en un seul point P = (e , 0) qui est simple. Elle a pour équation :

$$y^2 = (x - e) (x - e_1) (x - e_2) = f (x) \in IR[x]$$

La racine e est réelle et les 2 racines e_1 et e_2 sont complexes Conjuguées $s \pm it$; $(s,t) \in IR^2$

Le discriminant de f (x) est égal à :

$$\text{Dis} (f) = - 4 t^2 ((e - s)^2 + t^2) \qquad (21)$$

Comme les 3 nombres e, s , t sont réels, il en résulte la valeur :

$$\text{Dis} (f) < 0 \qquad (22)$$

la relation entre le discriminant Δ (E) et le discriminant du polynôme f (x) , la formule (22) et l’hypothèse $\Delta (E) \neq 0$ impliquent $\Delta (E) < 0$.

□

9.2 Illustration de cette classification par des exemples :

Exemple 1 : Courbe Elliptique coupant l’axe ox en 1 point simple

Soit la Cubique de Weierstrass d’équation :

$E_1 : y^2 = x^3 + 2 x^2 + 2x + 15 \in IR[x, y]$

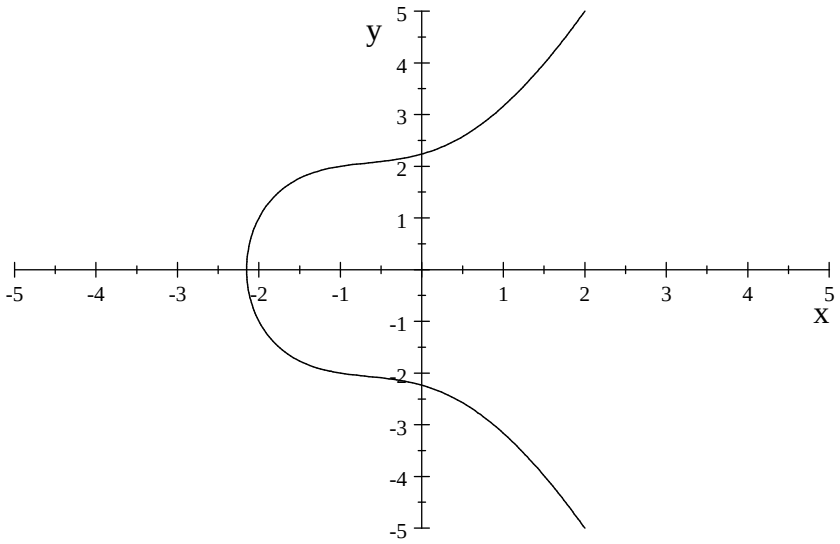
Avec le calcul j’obtiens les invariants :

$b_2 = 8$, $b_4 = 4$, $b_6 = 60$, $b_8 = 116$ et $\Delta(E_1) = -87856 < 0$

La valeur $\Delta(E_1) < 0$ implique un point simple d'intersection de la Courbe Elliptique E_1 avec l'axe O_x.

Tableau des coordonnées de quelques points de la courbe E_1

X	- 4	- 3	- 1	0
Y	Pas de racine réelle	0	$-\sqrt{15}$ et $\sqrt{15}$	$-2\sqrt{5}$ et $2\sqrt{5}$



$E_1 : y^2 = x^3 + 2x^2 + 2x + 5$

Exemple 2 : Courbe Elliptique coupant l'axe Ox en trois points simples :

Soit la Cubique de Weierstrass

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

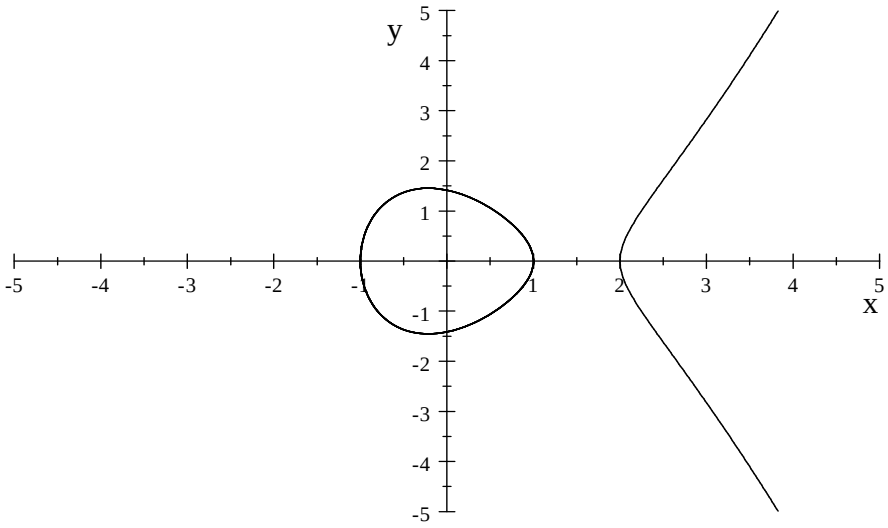
Avec le calcul j'obtiens les invariants :

$b_2 = -8$, $b_4 = -2$, $b_6 = 8$, $b_8 = -17$ et $\Delta(E_2) = 2816 > 0$

La valeur $\Delta(E_2) > 0$ implique trois points simples d'intersection de la Courbe Elliptique E_2 avec l'axe O_x.

Tableau des coordonnées de quelques points de la courbe E_2

X	- 2	- 1	0	3
Y	Pas de racine réelle	0	$-\sqrt{2}$ et $\sqrt{2}$	8



E_2 : $y^2 = x^3 - 2x^2 - x + 2$

Chapitre III : Groupe de Mordell-Weil d'une Courbe Elliptique

1. Loi de groupe abélien additif sur l'ensemble E(K) :

Soient K un corps commutatif et une Courbe Elliptique E d'équation de Weierstrass :

$$y^2 + a_1 x y + a_3 = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$$

les 2 variables x et y sont des éléments d'une clôture K^{alg} de K

Sur l'ensemble E (K) des points K-rationnels de E , auquel nous adjoignons le point $O_E = (0,1,0) \in IP^2(K)$ à l'infini sur E nous définissons une loi de groupe abélien par la :

Proposition 1 :

L'ensemble E (K) des points K-rationnels d'une Courbe Elliptique E ,admet une structure de groupe abélien additif ,d'élément neutre le point O_E ,avec :

La propriété géométrique : '' 3 points colinéaires de E ont une somme nulle '' :

$$\mathbf{P + Q + R = O_E}$$

et la loi de composition interne :

$F : E (K) \times E (K) \rightarrow E (K)$, avec $P + Q = - R$

Preuve de la proposition 1 :

1) Axiome de l'élément neutre :

La droite verticale passant par un point P de E et le point à l'infini O_E recoupe E au point P' qui est le symétrique de P par rapport à l'axe Ox ; le point $P + O_E$ recherché est le symétrique de P' , c'est donc P lui-même ; il en résulte l'élément neutre : $P + O_E = O_E + P = P$.

2) Axiome du symétrique :

Le symétrique d'un point P de E est le 2ieme point Q d'intersection de E par la parallèle à l'axe Oy qui passe par P , le 3ieme point étant O_E . il satisfait la propriété de colinéarité des 3 points : $P + Q + O_E = O_E$; il en résulte le symétrique de P : $Q = - P$

3)Axiome de commutativité :

La droite PQ passant par 2 points de E est confondue avec la droite QP ;

il en résulte la commutativité : $P + Q = Q + P$

4)Axiome d'associativité :

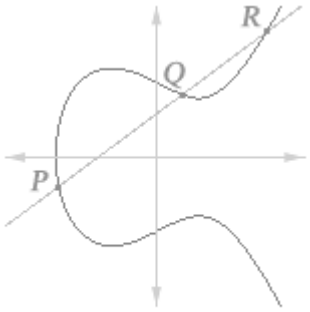
Pour vérifier cet axiome , il faut utiliser le calcul des sommes 2 à 2 des 3 points P, Q et R : $P + Q = S$; $S + R$ et $Q + R = T$ et $P + T$.

Alors , nous obtenons l'égalité : $S + R = P + T$

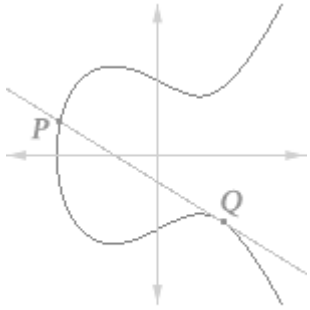
Il en résulte l'associativité : $(P + Q) + R = P + (Q + R)$

□

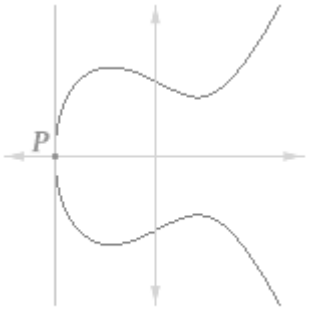
Illustration géométrique pour la loi de groupe additif dans les différents cas :



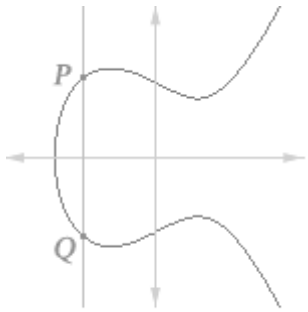
$P + Q + R = 0$



$P + Q + Q = 0$



$P + P + 0 = 0$



$P + Q + 0 = 0$

Définition 1 :

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

2. Coordonnées des points - P , $P_1 + P_2$, P + P = 2 P du groupe E(K) :

Pour obtenir les coordonnées du symétrique d'un point P , de la somme de 2 points $P_1 + P_2$ et du point 2P , il faut utiliser la propriété géométrique des 3 points colinéaires de la courbe et la théorie des intersections des courbes par les droites :

1) **Calcul des coordonnées du symétrique – P d'un point P** :

Soit un point P = (x_p , y_p) sur une Courbe Elliptique E. Le symétrique - P du point P est l'intersection de la droite parallèle à Oy passant par P par la courbe E . cette droite a pour équation :

$$x = x_p \qquad (1)$$

cela implique que P et – P ont même abscisse $x = x_p$ et des ordonnées y_P et y_{-P} qui sont les racines de l'équation du second degré en y :

$$y^2 + (a_1 x_p + a_3) y - (x_p^3 + a_2 x_p^2 + a_4 x_p + a_6) = 0 \qquad (2)$$

La somme des racines est la fonction symétrique :

$$y_P + y_{-P} = - a_1 x_p - a_3 \qquad (3)$$

Il en résulte les coordonnées du symétrique – P :

$$- P = (x_P , - y_P - a_1 x_p - a_3) \qquad (4)$$

2) **Calcul des coordonnées de la somme $P_1 + P_2$ de deux points $P_i (x_i , y_i)$ tels que $P_1 \neq \pm P_2$:**

Soit 2 points $P_1 = (x_1 , y_1)$ et $P_2 = (x_2 , y_2)$ sur la courbe elliptique E .

La sécante P_1P_2 recoupe E en un 3ieme point P_3 . D' après la propriété géométrique de trois points colinéaires P_1 , P_2 , P_3 de la courbe E : $P_1 + P_2 + P_3 = O_E$; cela implique :

$$P_1 + P_2 = - P_3$$

Comme la sécante P_1P_2 a pour équation :

$$y - y_1 = t\,(x - x_1)\ ,\ t = \frac{(y_1 - y_2)}{(x_1 - x_2)} \qquad (5)$$

cela implique que les abscisses des trois points P_1 , P_2 , P_3 sont les racines de l'équation cubique en x :

$$[(t(x - x_1) + y_1]^2 + (a_1 x + a_3)[t(x - x_1) + y_1] = x^3 + a_2 x^2 + a_4 x + a_6 \qquad (6)$$

La somme des 3 racines de cette équation cubique est une fonction symétrique élémentaire :

$$x_1 + x_2 + x_3\ \frac{-\,coefficient\ de\ x^2}{coefficient\ de\ x^3} = -a_2 + t^2 + a_1 t \qquad (7)$$

Cela implique l'abscisse x_3 du point $P_3 = (x_3 , y_3)$.

$$x_3 = t^2 + a_1 t\ - a_2 - x_1 - x_2 \qquad (8)$$

Les formules (5) et (7) et le calcul impliquent l'ordonnée y_3 du point P_3 :

$y_3 = t\,(x_3 - x_1) + y_1$ et $y_3 = t^3 + a_1 t^2 - t\,(a_2 + 2\,x_1 + x_2) + y_1$

Les coordonnées du point $M = P_1 + P_2 = -P_3$ sont obtenues avec la formule du symétrique :

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

$y_M = -t^3 - 2a_1 t^2 + t\,(2\,x_1 + x_2 - a_1^2 + a_2) + a_1 a_2 - a_3 - y_1 + a_1 (x_1 + x_2)$;

$$t = \frac{y_2 - y_1}{x_1 - x_2} \qquad \text{pour } x_1 \neq x_2$$

3) Calcul des coordonnées de la somme P + P = 2 P :

Pour déterminer la somme P + P = 2 P , nous utilisons l'équation :

$$y = y'\,(x - x_P) - y_P \qquad (9)$$

de la tangente à la courbe E au point P .

Cette tangente coupe la courbe en un point simple T ; selon la propriété géométrique des 3 points colinéaires :

$$P + P + T = O_E \qquad \text{donc} \quad 2P = -T$$

En remplaçant (9) dans l'équation de Weierstrass de E ,nous obtenons une équation en x cubique.

Nous utilisons la fonction symétrique élémentaire des racines de cette équation pour calculer l'abscisse du point T et par suite de son symétrique – T = 2P :

$X_{2P} = y_P'^2 + a_1 y' - 2x$;

$Y_{2P} = y_P'^3 - 2 a_1 y_P'^2 + (3 x_P - a_1^2 + a_2) y_P' + a_1 a_2 - a_3 - y_P + 2 a_1 x_P$;

$$y_P' = \frac{3x_P^2 + 2a_1x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}$$

Ces résultats sont rassemblés dans la :

Proposition 2 :

Soit une courbe elliptique E d'équation de Weierstrass :

$$y^2 + a_1 x y + a_3 = x^3 + a_2 x^2 + a_4 x + a_6 \in K[x, y]$$

1) Les coordonnées du symétrique – P d'un point P = (x_P , y_P) sont égales à :

$x_{(-P)} = x_P$ et $y_{(-P)} = - y_P - a_1 x_p - a_3$

2) Les coordonnées de la somme M = P_1 + P_2 , pour P_i (x_i , y_i) tels que $P_1 \neq \pm P_2$ sont égales à :

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

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

$$t = \frac{y_2 - y_1}{x_1 - x_2} \quad \text{pour } x_1 \neq x_2$$

3) Les coordonnées de la somme P + P = 2 P = (x_{2P} , y_{2P}) sont égales à :

$x_{2P} = y_P'^2 + a_1 y' - 2 x_P$;

$y_{2P} = - y_P'^3 - 2 a_1 y_P'^2 + (3 x_P - a_1^2 + a_2) y_P' + a_1 a_2 - a_3 - y_P + 2 a_1 x_P$; (4)

$$y_P' = \frac{3x_P^2 + 2a_1x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}$$

Exemple :

Soit la courbe Elliptique E : $y^2 = x^3 + 1$. et soient les 3 points $P_1 = (- 1 , 0)$, $P_2 = (0 , 1)$ et $P_3 = (2 , 3)$ de la courbe E.

Calculons les coordonnées de :

1) $M = P_1 + P_2$

Les formules de la proposition 2 donnent : $t = (1 - 0)/(0 - (-1)) = 1$;

$x_M = 1^2 + 0\, t - 0 - (-1) - 0 = 2$ *et*

$y_M = -1^3 - 2\times0\times1t^2 + 1\,(\,2\,(-1) + 0 - 0^2 + 0\,) + 0\times0 - 0 - 0 + 0\,(-1 + 0\,) = -3$

d'où M = (2 , - 3)

2) M' = 2 P_3

Les formules (4) impliquent :

$$y_P' = \frac{3x_P^{\,2} + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} = 12/6=2$$

$$x_{2P} = y_P'^{\,2} + a_1\,y_P' - 2\,x_p = 0$$

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

$y_{2P} = -8+12-3= 1$ d' où M = (0 , 1)

3) M = - P_3 (2 , 3)

D'après les formules de la proposition 2 ; nous obtenons

$x_M = 2$ et $y_M = -\,y_{P_3} - a_1\,x_{P_3} - a_3 = -3$, d' où M = (2 , - 3) .

La proposition 2 nous permet de calculer les coordonnées de tout point m P, m>2.

Ainsi 3 P = 2 P + P , 4P = 2 (2 P) , 5 P = 4 P + P , etc…

Nous verrons , par la suite , des formules obtenues par Cassels [2] et qui permettent de calculer les coordonnées des points m P , m > 1 , de Courbes Elliptiques particulières.

D'après la théorie des groupes , le groupe de Mordell-Weil E (K) possède des sous groupes abéliens et des sous groupes cycliques . Les sous groupes cycliques sont engendrés par un point P du groupe de Mordell-Weil E (K) :

$\{P, 2P = O_E\}$, $\{P, 2P, 3P = O_E\}$, …., $\{P, 2P, ..., mP = O_E\}$ pour un entier m > 1.

3. Points d'ordre fini d'une Courbe Elliptique :

Définition2 :

Soit un point P de la Courbe Elliptique E et un entier m ∈ IN .

Le point P est d'ordre m s'il satisfait la relation :

$$m\,P = O_E \qquad (1)$$

avec : *m le plus petit entier vérifiant la relation (1)*

m P = P + P +...+ P , m fois P si m > 0

0 P = O_E

Si m < 0 : *m P = (- P) + (- P) + ….+ (- P) , (- m) fois (- P)*

Les coordonnées des points 2P , 3P ,..,m P sont des fonctions rationnelles .

4-Formules de Cassels des coordonnées des points m P :

Proposition 3 :

Soit une courbe elliptique E d'équation de Weierstrass :

$$\mathbf{E : y^3 = x^3 + A\,x + B} \in \mathbf{Q}[x, y] \quad \textbf{et } \mathbf{4\,A^2 + 27\,B^3} \neq 0$$

Alors les coordonnées d'un point m P de la courbe elliptique E sont égales à :

$$\mathbf{X\,(\,m\,P\,)} = \frac{\phi_m}{\psi_m^{\,2}} \quad \textbf{et} \quad \mathbf{y\,(\,m\,P\,)} = \frac{\omega_m}{\psi_m^{\,3}}$$

ϕ_m, ω_m, ψ_m **sont des polynômes de l'anneau** $\mathbf{Z}[x, y, A, B]$ **qui vérifient les relations :**

$$\psi_{-1} = -1, \psi_0 = 0, \psi_1 = 1, \psi_2 = 2y, \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,$$
$$\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 2A^2x^2 - 4ABx - 8B^2 - A^3),$$
$$\psi_{2m} = 2\psi_m(\psi_{m+2}\psi_{m-1} - \psi_{m-2}{}^2\psi_{m+1}{}^2),$$
$$\psi_{2m+1} = \psi_{m+2}\psi_m{}^3 - \psi_{m-1}{}^3\psi_{m+1}{}^3 \; pour m \geq 2,$$
$$\phi_m = x\psi_m{}^2 - \psi_{m-1}\psi_{m+1},$$
$$\omega_m = \psi_{m+2}\psi_{m-1}{}^2 - \psi_{m-2}\psi_{m+1}{}^2$$

Preuve :

Pour m = - 1 , la formule du symétrique - P = (x , - y) implique :

$$X = \frac{x}{(-1)^2} \quad \text{et} \quad -y = \frac{y}{(-1)^3} \quad \text{donc} \quad \psi_{-1} = -1$$

Pour m = 0 , la relation 0 P = (∞, ∞) = ($\frac{x}{0}, \frac{y}{0}$) implique $\psi_0 = 0,$

Pour m = 1 , la relation 1 P = 1 (x , y) = P = (x , y) implique $\psi_1 = 1$.

Pour m ≥ 2 , nous utilisons un raisonnement par récurrence sur m .

□

Selon son discriminant , une Courbe Elliptique E a un ou trois points à coordonnées réelles sur l'axe des abscisses .En ces points , la tangente est parallèle à l'axe Oy , son 3^e point d'intersection avec la courbe est le point à l'infini.

Donc P + P = 2P = 0_E. un tel point est d'ordre 2. Puisque P = − P, l'ensemble formé du point P et du point à l'infini forme un sous-groupe du groupe des points de la courbe ; il est cyclique d'ordre 2.

Si la courbe a trois points d'ordre 2, c'est-à-dire lorsque le discriminant $\Delta (E) > 0$, l'ensemble de ces points forme , avec le point à l'infini, un groupe d'ordre 4 isomorphe à deux copies du groupe cyclique d'ordre 2, donc un groupe de Klein(disciple de Plucker)

Pour n > 2, les points à coordonnées réelles d'ordre n forment un sous-groupe cyclique d'ordre n

Les points d'ordre m sont des points de m – torsion de la Courbe Elliptique.

5 . Sous-groupes de m-torsion et groupe de torsion d'une Courbe Elliptique :

***Définition* 3 :**

Pour tout entier rationnel m , ,l'ensemble $E (K)[m] = E [m]$ *des points d'ordre m d'une Courbe Elliptique E , est le sous groupe de m – torsion de E.*

La réunion infinie des sous groupes de m – torsion de E est un groupe.

Définition 4 :

Le groupe de torsion d'une Courbe Elliptique E est l'ensemble :

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

des points de E d'ordre fini.

Pour le calcul des points de torsion , nous pouvons utiliser le :

Théorème de Nagell-Lutz :

Soit une Courbe Elliptique E définie sur Q par une équation de Weierstrass :

E : $y^2 = x^3 + a_2 x^2 + a_4 x + a_6 = f (x)$ **avec** $a_i \in ZI$ **pour i = 2 , 4 , 6 .**

Soit un point P (x , y) de m-torsion de E , $m \geq 2$ **.**

Alors :

1) Les coordonnées (x , y) de P sont des entiers rationnels.

2) L'ordonnée y de P est soit nulle , soit un diviseur du discriminant

$$D = - 4 a_2^3 a_6 + a_2^2 a_4^2 + 18 a_2 a_4 a_6 - 4 a_4^3 - 27 a_6^2$$ **du polynôme f (x)**

3) Et si $a_2 = 0$ **alors** y^2 **divise D.**

La preuve de ce théorème se trouve dans l'ouvrage de Hellegouarch [7] pages 203-204.

Exemple de calcul de points de m-torsion :

Soit la Courbe Elliptique E d'équation de Weierstrass :

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

Avec le calcul j'obtiens les invariants : $b_2 = 0$; $b_4 = 0$; $b_6 = 4$; $b_8 = 0$; $c_4 = 0$; $c_6 = -216 \times 4$; $\Delta(E) = -27$; $j(E) = 0$.

Les nombres qui sont des carrés diviseurs de 27 sont 1 et 9 d'où y = -1 , 1 , - 3 , 3 ce qui implique les points de torsion de la courbe E : $P_2 = (0, 1)$; $P_3 = (2, 3)$; $P_4 = (0, -1)$; $P_5 = (2, -3)$, $P_1 = (-1, 0)$ et du point à l'infini O_E .

La structure du groupe de torsion T (E (Q)) d'une courbe elliptique E sur le corps des nombres rationnels Q a été conjecturée par Ogg et démontrée par Mazur [14].

Proposition 4 : (théorème de Mazur)

Le groupe de torsion T (E (Q)) d'une courbe elliptique E est isomorphe à l'un des 15 groupes additifs abéliens finis : Z / nZ , $1 \leq n \leq 10$ ou $n = 12$,

$Z / 2Z \times Z / 2nZ$, $1 \leq n \leq 4$.

Preuve :

Consulter '' Rational isogénies of prime degrée '' Inv.Math.44 (1978) 129-162.

□

C'est au début du siècle dernier que le mathématicien Poincaré manifeste son intérêt au sujet des points rationnels sur une courbe et sur le nombre de générateurs. En 1922 , le mathématicien anglais Louis Mordell (1888 – 1972) prouve que pour toutes les Courbes Elliptiques , il y a un sous ensemble fini de points rationnels qui génèrent tous les autres points rationnels.

Théorème :(Mordell-Weil) :

Le groupe E (Q) est un groupe additif abélien de type fini.

La preuve du théorème requiert deux éléments : la finitude du groupe $\frac{E(Q)}{mE(Q)}$ et l'introduction d'une fonction hauteur sur le groupe abélien E (Q) .

Définition 5 :

Une fonction hauteur sur un groupe abélien A est une fonction

$$h : \quad A \rightarrow IR^{+}$$

qui satisfait les trois conditions :

h_1) pour tout point $Q \in A$ il existe une constante $c_1(A, Q) = c_1$ telle que

$$h(P+Q) \leq 2\,h(P) + c_1 \qquad \text{pour tout } P \in A$$

h_2) il existe un entier $m \geq 2$ et une constante $c_2(A)$ tels que

$$h(mP) \geq m^2\,h(P) - c_2 \qquad \text{pour tout } P \in A$$

h_3) pour tout nombre réel c_3 l'ensemble : $\{P \in A : h(P) \leq c_3\}$ est fini

Il y a plusieurs types de hauteurs , parmi elles :

La hauteur logarithmique de Weil :

$$h : E(Q) \rightarrow R^{+}$$

telle que : $h(O_E) = 0_E$ et $h(P) = \log \max(|p|,|q|)$ pour tout point $P(x, y) \neq 0_E$

et $x = \frac{p}{q}$.

Preuve du théorème de Mordell-Weil :

Soient le groupe de Mordell-Weil $E(Q)$ et un entier m tel que

le groupe quotient $\frac{E(Q)}{mE(Q)}$ soit fini.

Soit un point $P \in E(Q)$ à coordonnées rationnelles sur la courbe E et soient des représentants $R_1 , R_2 ,\ldots, R_r$ des classes du groupe quotient $\frac{E(Q)}{mE(Q)}$

Nous construisons une suite infinie de points $P_1 , P_2 , \ldots , P_n ,..$ à partir du point P :

$P = mP_1 + R_{i_1}; P_1 = mP_2 + R_{i_2}; P_j = mP_{j+1} + R_{i_{j+1}}; P_{n-1} = mP_n + R_{i_n}$ avec

$1 \leq i_1, i_2, \ldots, i_n \leq r$

La relation $P_{j-1} = mP_j + R_{i_j}$ implique $\qquad mP_j = P_{j-1} - R_{i_j} \qquad (1)$

En appliquant l'axiome (h_2) au premier membre de l'égalité (1) et l'axiome (h_1) à son second membre , nous obtenons l'inégalité :

$$h(P_j) \leq \frac{2}{m^2}(h(P_{j-1} - R_{i_j}) + c_j^{'}) \qquad (2)$$

Nous additionnons membre à membre les inégalités (2) pour j = 1 , . . . , n , nous obtenons l'inégalité : $h(P_n) \leq (\frac{2}{m^2})^n h(P) + (\frac{2}{m^2} + \frac{2^2}{m^4} + ... + \frac{2^n}{m^{2n}})c^{'}$ (3)

La série de terme général $u^t = \frac{2^t}{m^{2t}}$ du deuxième membre de l'inégalité (3) a pour somme $\frac{1}{1-\frac{2}{m^2}}$ pour $m \geq 2$ et comme $\lim (\frac{2}{m^2})^n = 0$ pour n assez grand , nous en déduisons que h (P) est borné et que , par l'axiome (3) , l'ensemble $\{P_1, P_2, ..., P_k\}$ des points P_i est fini.

Donc tout point P du groupe abélien E (Q) est une combinaison Z – linéaire

$P = n_1 R_1 + n_2 R_2 + \ldots + n_r R_r + n_{r+1} P_1 + n_{r+2} P_2 + \ldots + n_{r+k} P_k$; $n_i \in Z$

par conséquent le groupe abélien E (Q) est de type fini.

□

La structure algébrique de ce groupe abélien est précisée par la :

Proposition 5 :

Le groupe abélien E (K) de Mordell-Weil est isomorphe à un produit de groupes abéliens :

$E(K) \cong T(E) \times Z^r$ ou T (E) = le groupe de torsion qui est fini et Z^r = r copies du groupe additif infini Z.

Cette décomposition du groupe E (K) permet de définir un invariant des Courbes Elliptiques :

Définition 6 : (rang d'une courbe elliptique)

L'entier r = r (E) ≥ 0 de la formule de la proposition (7) est le rang de la Courbe Elliptique E , il est égal au nombre de points linéairement indépendants qui engendrent la partie infinie du groupe de Mordell-Weil.

6. Isomorphismes de Courbes Elliptiques :

Plusieurs spécialistes des Courbes Elliptiques, parmi eux Sylverman [19], Mazur [14], Cassels [2], Shimura [18] , Lang [13] , Shafarevish [17] , Tate [20] ont publié des articles sur les morphismes de groupes abéliens E (K) de Mordell-Weil des Courbes Elliptiques.

Ces morphismes peuvent être des isomorphismes, des endomorphismes ou des automorphismes .Les morphismes spécifiques aux Courbes Elliptiques sont des isogénies et des twists.

Proposition 6 :

Soit une courbe elliptique E d'équation de Weierstrass :

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

de groupe de Mordell-Weil E(K) Alors l'application μ : E (K) $\rightarrow$ E'(K)

de valeur : μ (x , y) = ($u^2 X + r$, $u^3 Y + s u^2 X + t$) (2)

avec $u \neq 0$ et r , s t $\in$ K ,

est un isomorphisme du groupe E (K) dans le groupe E'(K) .

Preuve :

La transformée de la courbe elliptique E par μ est la courbe E' d'équation de Weierstrass :

E' : $Y^2 + a_1' X Y + a_3' = X^3 + a_2' X^2 + a_4' X + a_6' \in K[X,Y]$ (3)

1) Les relations de morphisme de groupes : $\mu (P_1 + P_2) = \mu (P_1) + \mu (P_2)$ et $\mu (O_E) = O_E$ sont vérifiées avec le calcul .

2) Le système ($x = u^2 X + r$, $y = u^3 Y + s u^2 X + t$) admet une solution unique :

($X = \frac{x - r}{u^2}$, $Y = \frac{y - sx - sr + t}{u^3}$) pour $u \neq 0$, donc le morphisme μ est bijectif .

□

L'isomorphisme entre deux Courbes Elliptiques implique des relations entre leurs invariants :

2. Relations entre coefficients et invariants de deux Courbes Elliptiques isomorphes E et E' :

Corollaire : Avec les mêmes hypothèses de la proposition précédente alors :

1) les coefficients a_i , b_i , c_i , a_i' , b_i' , c_i' satisfont les relations :

$u\, a_1' = a_1 + 2\, s$; $u^2\, a_2' = a_2 - s\, a_1 + 3\, r - s^2$; $u^3\, a_3' = a_3 + r\, a_1 + 2\, t$

$u^4\, a_4' = a_4 - s\, a_3 + 2\, r\, a_2 - (t + r\, s)\, a_1 + 3\, r^2 - 2\, s\, t$; (isom 1)

$u^6\, a_6' = a_6 + r\, a_4 + r^2\, a_2 + r^3 - t\, a_3 - t^2 - r\, t\, a_1$

$u^2\, b_2' = b_2 + 12\, r$; $u^4\, b_4' = b_4 + r\, b_2 + 6\, r^2$;

$u^6\, b_6' = b_6^2 + 2\, r\, b_4 + r^2\, b_2 + 4\, r^3$; (isom 2)

$u^8\, b_8' = b_8 + 3\, r\, b_6 + 3\, r^2\, b_4 + r^3\, b_2 + 3\, r^4$

$u^4\, c_4' = c_4$; $u^6\, c_6' = c_6$ (isom 3)

2) Les invariants de E et E' satisfont les relations :

$u^{12}\, \Delta (E') = \Delta (E)$, $j (E') = j (E)$, $\omega (E') = u\, \omega (E)$ (isom 4)

Preuve :

En remplaçant ,dans l'équation de Weierstrass de E la variable x par $u^2\, X + r$ et la variable y par $u^3\, Y + s\, u^2\, X + t$, nous obtenons les relations (isom 1) , puis par transformation d'équations et le calcul des invariants nous obtenons les relations (isom 2) ,(isom 3),(isom 4) .

□

Dans les relations (isom 4) , nous constatons que les invariants modulaires de E et de E' sont égaux .ce qui permet de classifier les Courbes Elliptiques isomorphes .

Proposition 7 :

Deux Courbes Elliptiques E et E' définies sur un même corps commutatif K sont isomorphes si et seulement si leurs invariants modulaires sont égaux

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

Preuve de « E et E' isomorphes « implique « j (E) = j (E') «

Soient deux Courbes Elliptiques E / K et E' / K isomorphes ; alors le corollaire précédent implique l'égalité j (E) = j (E') .

Preuve de « j (E) = j (E') « implique « E et E' isomorphes «

Soient deux Courbes Elliptiques E et E' ayant des invariants modulaires égaux

$$j(E) = j(E') \qquad (1)$$

d'équations de Weierstrass :

E : $y^2 = x^3 + A x + B$ et E' : $Y^2 = X^3 + A' x + B'$

avec les conditions :

$$4A^3 + 27B^2 \neq 0 \quad \text{et} \quad 4A'^3 + 27B'^2 \neq 0 \qquad (2)$$

La formule de l'invariant modulaire et l'hypothèse (1) impliquent l'égalité :

$$A^3 B'^2 = A'^3 B^2 ; \qquad (3)$$

Nous cherchons un isomorphisme entre E et E' de la forme :

$$(x , y) \rightarrow (u^2 x , u^3 y) \qquad (4)$$

Où $u \neq 0$, u appartenant à une clôture algébrique K^{alg} du corps K.

Les formules d'isomorphismes impliquent les relations entre les coefficients :

$$u^4 A' = A ; \; u^6 B' = B ; \; u^{12} \Delta(E') = \Delta(E) \qquad (5)$$

La formule(3) implique 3 cas possibles pour les valeurs de A et B :

$A = 0$ et $B \neq 0$, $A \neq 0$ et $B = 0$ ou $A B \neq 0$ (6)

Le cas $A = B = 0$ ne vérifie pas la condition (2) .

1) Lorsque $A = 0$ et $B \neq 0$ les formules (5) impliquent la valeur de u :

$$U^6 B' = B \quad \text{soit} \quad u = (B / B')^{\frac{1}{6}} \qquad (7)$$

Dans la clôture algébrique K^{alg} , la formule (6) implique 6 racines sixièmes de B/B'.

Chaque racine $u \neq 1$ implique un isomorphisme, dont la formule est donnée par la relation (4) .

2) Lorsque $B = 0$ et $A \neq 0$, les formules (5) impliquent la valeur de u :

$u^4 A' = A$ soit $u = (A / A')^{\frac{1}{4}}$; (8)

Dans la clôture algébrique K^{alg} , il y a 4 racines quatrièmes de (A / A')

Chaque racine $u \neq 1$ implique un isomorphisme, dont la formule est donnée par la relation (4) .

3) Lorsque $A B \neq 0$, les formules (5) impliquent les valeurs de u :

$$u = \left(\frac{B}{B'}\right)^{\frac{1}{6}} = \left(\frac{A}{A'}\right)^{\frac{1}{4}} \quad ; \qquad (9)$$

Il en résulte la relation entre les coefficients A, B, A', B' :

$A^3 B'^2 = A'^3 B^2$, (relation (3) vérifiée) .

Chaque valeur de u implique un isomorphisme dont la formule est donnée par la relation (4)

Exemple de Courbes Elliptiques isomorphes :

Soit une courbe Elliptiques E d'équation de Weierstrass :

$E : y^2 + 4xy + 6y = x^3 + 3x^2 - 12x - 15 \in Q[x, y]$

L'application : f : $E(Q) \rightarrow E'(Q)$ de valeur

f (x , y) = (4 X – 1 , 8 Y – 8 X + 3) avec u = 2 ; r – 1 ; s = - 2 et t = 3

est un isomorphisme de courbes elliptiques .

Cet isomorphisme transforme la courbe elliptique E en la courbe E' d'équation :

$$E' : y^2 + y = x^3 + x^2 - \frac{11}{16}x - \frac{1}{4} \in Q[x, y]$$

Avec le calcul j'obtiens les invariants de :

1) La courbe E :

$b_2 = 28$; $b_4 = 0$; $b_6 = -24$; $b_8 = -168$, $\Delta(E) = 64 \times 3 \times 5 \times 121$

$$c_4 = 28^2 \quad ; \; j(E) = \frac{28^6}{64 \times 3 \times 5 \times 121} = \frac{14^6}{15 \times 121}$$

2) La courbe E' : $b_2' = 4$; $b_4' = \frac{-11}{8}$; $b_6' = 0$, $b_8' = \frac{121}{256}$

$$\Delta(E') = 2^{-6} \times 3 \times 5 \times 121 \qquad c_4' = 33 \qquad ; \qquad j(E') = \frac{14^6}{15 \times 121}$$

La relation j (E) = j (E ') et la proposition 2 impliquent que les courbes E et E ' sont isomorphes.

Cette propriété de l'invariant modulaire définit une relation d'équivalence qui quotiente l'ensemble des Courbes Elliptiques en classes d'équivalence de Courbes Elliptiques :

Cl (E_1) = $\{E_1, E_{1,2}, ..., E_{1,n}\}$ où j (E_1) = j ($E_{1,1}$) = … = j ($E_{1,n}$)

Cl (E_2) = $\{E_2, E_{2,1}, ..., E_{2,n}\}$ où j (E_2) = j ($E_{2,1}$) = … = j ($E_{2,n}$) etc..

Toutes ces classes sont disjointes lorsque les invariants modulaires sont différents..

Proposition 8 :

Tout nombre μ du corps K est l'invariant modulaire d'une courbe elliptique E.

Preuve :

Soit une courbe elliptique E d'équation de Weierstrass :

$E : y^2 = x^3 + A x + B \in K[x, y]$ avec $4 A^3 + 27 B^2 \neq 0$ (1)

les formules impliquent les invariants : :

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

et $j (E) = 4 \times 1728 A^3 / (4 A^3 + 27 B^2)$ (3)

Nous avons 3 cas à examiner :

1) $\mu = 0$:

L'hypothèse j (E) = 0 et les relations (2) et (3) impliquent A = 0 et B $\neq$ 0 d'où l'équation (1) devient $E : y^2 = x^3 + B$, avec B $\neq$ 0 (4)

2) $\mu = 1728$:

L'hypothèse j (E) = 1728 et les relations (2) et (3) impliquent B = 0 et A $\neq$ 0 d'où l'équation (1) devient : $E : y^2 = x^3 + A x$ avec A $\neq$ 0 (5)

3) $\mu \neq 0, 1728$:

L'hypothèse j (E) $\neq$ 0 , 1728 et les relations (2) et (3) impliquent :

$4 \times 1728 A^3 = (4 A^3 + 27 B^2) \mu$. (6)

La relation (6) donne l'équation :

$4 A^3 (1728 - \mu) = 27 \mu B^2$ (7)

Posons : $A = 3\mu / (1728 - \mu)$ (8)

alors la relation (7) devient :

$B^2 = 4\mu^2 / (1728 - \mu)^2$ (9)

La relation (9) implique la valeur :

$B = \pm 2\mu / (1728 - \mu)$ (10)

Les relations (1) ,(8) et (9) impliquent l'équation générale des Courbes Elliptiques d'invariant modulaire $j(E) = \mu$ où $\mu \neq 0$, 1728 :

$$E : y^2 = x^3 + \frac{3\mu}{1728-\mu}x \pm \frac{2\mu}{1728-\mu}$$

.

Chapitre IV: Application aux Courbes Elliptiques à invariant modulaire nul

Les Courbes Elliptiques à invariant modulaire nul forment une famille particulière de Courbes dans l'ensemble des Courbes Elliptiques .

1. Equations de Courbes Elliptiques à invariant modulaire nul :

Soit une cubique de Weierstrass E d'équation :

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

K étant un corps global , local ou fini..

L'hypothèse $j(E) = 0$ implique les 2 relations $c_4 = 0$ et $\Delta(E) \neq 0$

Soit $c_4 = b_2^2 - 24 b_4 = 0$.

J'examine 5 familles de Courbes Elliptiques et la courbe de Fermat .

1) Famille de Courbes Elliptiques d'équation :

$$E : y^2 = x^3 + a_2 x^2 + a_4 x$$

Avec le calcul , j'obtiens les invariants :

$c_4 = 16 (a_2^2 - 3 a_4)$ et $\Delta(E) = 16 a_4^2 (a_2^2 - 4a_4)$; $j(E) = c_4^3 / \Delta(E)$.

Avec les valeurs: $a_2 = 3$ et $a_4 = 3$, j'obtiens une Courbe Elliptique d'équation

$E_1 : y^2 = x^3 + 3x^2 + 3x$; $c_4 = 0$; $\Delta(E) = - 432$ et $j(E_1) = 0$.

2) Famille de Courbes Elliptiques d'équation :

$$E : y^2 = x^3 + a_6$$

$c_4 = 0$; $\Delta(E) = -16 \times 27 a_6^2$, avec $a_6 \neq 0$; $j(E) = 0$.

3) Famille de Courbes Elliptiques d'équation :

$$E : y^2 + a_3 y = x^3 + a_4 x + a_6$$

Avec les calculs j'obtiens $c_4 = - 48 a_4$; $\Delta(E) = - 64 a_4^3 - 27 (a_3^2 + 4a_6)^2$

Avec les valeurs : $a_4 = 0$ et $a_3^2 + 4 a_6 \neq 0$, j'obtiens la famille de Courbes Elliptiques d'équation : $E : y^2 + a_3 y = x^3 + a_6$; $c_4 = 0$;

$\Delta(E) = - 27 (a_3^2 + 4 a_6)^2$ et $j(E) = 0$.

4) Famille de Courbes Elliptiques d'équation :

$$E : \quad y^2 + a_1 x y + a_3 y = x^3 \in K[x, y]$$

Avec les calculs j'obtiens : $c_4 = a_1^4 - 24 a_1 a_3$; $\Delta(E) = a_3^3 (a_1^3 - 27 a_3)$

Avec les valeurs : $a_1 = 0$ et $a_3 \neq 0$, j'obtiens la famille de Courbes Elliptiques d'équation :

$$E : y^2 + a_3 y = x^3 \quad ; c_4 = 0 \quad ; \Delta(E) = -27 a_3^4 \text{ et } j(E) = 0 .$$

5) Famille de Courbes Elliptiques d'équation :

$$E : y^2 + a_3 y = x^3 + a_4 x$$

Avec les calculs j'obtiens : $c_4 = -48 a_4$; $\Delta(E) = -(27 a_3^4 + 64 a_4^3)$

Avec les valeurs : $a_4 = 0$ et $a_3 \neq 0$, j'obtiens la famille de Courbes Elliptiques d'équation :

$$E : y^2 + a_3 y = x^3 \quad ; c_4 = 0 \quad ; \Delta(E) = -27 a_3^4 \text{ et } j(E) = 0 .$$

2. La Courbe de Fermat : $u^3 + v^3 = w^3$

La conjecture de Fermat de 1664 selon laquelle l'équation diophantienne :
$x^n + y^n = z^n$ n'admet pour $n \geq 3$ que les solutions triviales (0 , 0 , 0) , (0 , 1 , 1) et (1 , 0 , 1) , a été démontrée en 1994 par Wiles au moyen de la théorie des Courbes Elliptiques et de la représentation des groupes finis .

La courbe plane : $u^3 + v^3 = w^3$ est devenue la courbe de Fermat. C'est une Courbe Elliptique à invariant modulaire nul .Elle a été étudiée par plusieurs auteurs , parmi eux :

1) John T. Tate [20]

Soit la cubique de Fermat : $u^3 + v^3 = w^3$,.

Il utilise le changement de variable rationnel :

$x = 3w / (u + v)$ et $y = (9 (u + v) + 1) / 2$

il obtient la cubique de Weierstrass :

$$E_1 : y^2 - y = x^3 - 7 .$$

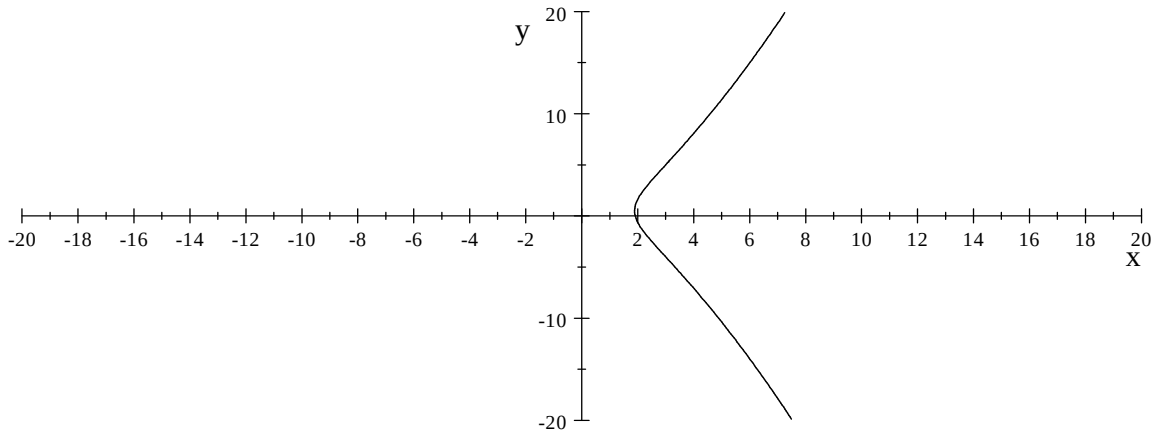
Cette cubique a un discriminant $\Delta (E_1) = -3^9$ et un invariant modulaire $j(E_1) = 0$.

L'inégalité $\Delta (E_1) < 0$ implique que cette Courbe coupe l'axe réel Ox en un seul point.

Pour tracer cette courbe nous calculons les coordonnées de quelques points :

x	1	$\sqrt[3]{7}$	2	3
y	Pas de y réel	0 et 1	$\frac{1\pm\sqrt{5}}{2}$	- 4 et 5

Il en résulte que cette Courbe coupe l'axe Ox au point ($\sqrt[3]{7}$, 0).



2) Robin Hartshorne [6]

La courbe de Fermat est non singulière sur tout corps K de carac (K) $\neq$ 3 .

Avec le changement de variable $x = z - z/3$, l'équation de Fermat

$x^3 + y^3 = z^3$ devient $E_2 : z^2 - z/3 = y^3 - 1/27$ (1)

Le changement de variable $z = Y$ et $y = X$ transforme (1) en :

$E_2 : Y^2 - Y/3 = X^3 - 1/27$ (2)

Avec le calcul nous obtenons les invariants de (2)

$\Delta (E_2) = - 1/27$ et $j (E_2) = 0$.

3) Knapp [10]

L'auteur pose dans l'équation de Fermat $\frac{u}{v} = \frac{3x}{y}$ et $\frac{u}{w} = \frac{y-9}{y}$.

Il obtient la cubique de Weierstrass :

$E_3 : y^2 - 9y = x^3 - 27$.

Le calcul des invariants implique : $\Delta(E_3) = -27^3$ et $j(E_3) = 0$

Les égalités des 3 invariants modulaires $j(E_1) = j(E_2) = j(E_3) = 0$ impliquent que les 3 courbes Elliptiques obtenues par les trois auteurs sont isomorphes .

Conclusion et Perspectives :

Il me reste beaucoup à faire dans la poursuite de ma recherche pour connaître la théorie des Courbes Elliptiques et ses applications (cryptographie , codage…) , les isogénies , les twists , les groupes de Chatelêt-Weil , les groupes de Selmer , les groupes de Shafarevich-Tate , la série L (E , s) de Dirichlet etc…

REFERENCES:

[1] E.ARTIN: « Algebraic Number and Algebraic Functions » -Gordon and Breach – sciences Publishers; New York; (1960).

[2] J.W. CASSELS: « Diophantine Equations with Special Reference to Elliptic Curves »- Journal London Mathematical Society - 41 (1966) 193-291.

[3] M.DEURING : Die Typen der Multiplikat : renringe Elliptisscher Funktionen Korper , " Abh . Math . Seminaire."

[4] Harvey COHN : «A classical invitation to Algebraic Numbers and Class Fields» -Springer Verlag -(1978)

[5] FULTON: « Algebraic Curves »- Benjamin- New York (1969).

[6] Robin HARTSHORNE: « Algebraic Geometry »- Graduate Texts in Mathematics 52-Springer (1983) Classification: 14 A 10 – 14 Fxx – 14Hxx – 14 Jxx.

[7] Yves HELLEGOUARCH : Invitations aux Mathématiques de Fermat Wiles . 2^{ieme} Ed.Masson – Paris (1999)

[8] D.HUSEMOLLER: « Elliptic Curves » -G.T.M 111 Springer (1987).

[9] Shokichi IYANAGA: « The Theory of Numbers » -North Holland Pub. Company-Amsterdam (1975).

[10] A.W. KNAPP : " Elliptic Curves – Mathematical Notes 40 , Princeton University Press (1992)

[11] NEAL KOBLITZ: (1) « Introduction to Elliptic Curves and Modular Forms » -2^{eme} edition GTM97. Springer (1984)

(2) « A course in Number Theory and Cryptography » - 2^{eme} edition GTM 114-Springer

[12] A.I.KOSTRIKIN: « Introduction à l'Algèbre » - Ed. Mir- Moscou- 2^{eme} edition (1986).

[13] Serge LANG: (1) « Algebra » - 2^{eme} edition, Addison Wesley Publishing Company, Inc, Reading, Massachusetts, New York (1984).

(2) « Elliptic Curves – Diophantine Analysis » - Springer Verlag (1978) - Classification AMS = 10 B 45 – 10 F 99 -14 G 25 – 14 H 25.

(3) « Algebraic Number Theory » - Addition – Wesley (1970).

(4) « Cyclotomic Fields »- GTM 59 – Springer.

[14] Barry MAZUR: (1) "Modular curves and the Eisenstein ideal» - IHES Publ. Math. 47. (1977), 33-186.
(2) « Rational points on Modular Curves » - LNM. n 601 (1977) 107 – 147.

[15] A. NERON: « Quasi Fonctions et Hauteurs sur les Variétés Abéliennes » - Annals of Mathematics 82 (1965), 249-331.

[16] Jean Pierre SERRE: « Géométrie Algébrique et Géométrie Analytique » - Ann. Inst. Fourier 6 (1956) – 1 – 42.

[17] I.R.SHAFAREVICH: (1) « Basic Algebraic Geometry » - Springer Verlag (1977).
(2) « Algebraic I»- Mir (1986)-Springer (1987).Classification AMS = 12 – xx, 20 – xx.

[18] Goro SHIMURA: « Introduction to the Arithmetic Theory of Automorphic Functions » - Princeton University Press -(1971).

[19] Joseph H. SILVERMAN: (1) « The Arithmetic of Elliptic Curves »- GTM 106 – Springer (1986). Classification AMS = 1401, 14G 99, 14H 05, 14 K 15.

[20] John TATE: « The Arithmetic of Elliptic Curves »- Invention- Mathematique 23 (1974) 179-206.

[21] André WEIL : (1) « Sur un théorème de Mordell »- Bull. Sci. Math. 54 (1930).
(2) « Courbes Algébriques et Variétés Abéliennes « Herman , Paris (1974)

[22] Edwin WEISS : « Algebraic Number Theory » - Mc Graw – Hill – New York (1964)

[23] Andrew WILES. : Modular Elliptic Curves and Fermat's last Theorem. Annalen of Math.N°142 (1995) 443-451**.**

[24] D.B ZAGIER : « Large integral points on elliptic curves» -Math. Comp. 48 (1987), 425-436.

[25] M. ZITOUNI : Géométrie Arithmétique et Algorithmique des Courbes Elliptiques Ed.O.P.U. Alger (2007)

REMERCIEMENTS

Toute ma gratitude et ma reconnaissance vont à toutes les personnes qui ont contribué et m'ont encouragé à élaborer ce travail de thèse de magister.
Je commencerai par remercier mon directeur de thèse le Professeur Mohamed ZITOUNI pour m'avoir dirigé , orienté et conseillé tout le long de la durée de ce travail .
J'ai l'honneur d'avoir comme président du jury le Professeur Meziane AIDER que je remercie également .
Je tiens aussi à remercier le Professeur Mohamed N. BENKAFADAR et Melle Soraya BOUGHABA Maître de Conférences de l'université de constantine pour avoir accepté d'être membres du jury comme examinateurs.
Je remercie aussi le Docteur Mohand Ouamar Hernane , Maître de Conférences à l'USTHB d'avoir accepté de faire partie du jury comme examinateur.

À la mémoire de mon père

À ma mère

À mes sœurs et frères